The Sedona Conference Journal®

Volume 25 ❖ 2024 ❖ Number One

Articles

The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control" . . . . The Sedona Conference

TAR 1 Reference Model: An Established Framework Unifying Traditional and GenAI Approaches to Technology-Assisted Review . . . . Tara Emory, Jeremy Pickens & Wilzette Louis

The Ubiquitous Role of the Specific "Intent to Deprive" Requirement of Amended Rule 37(e)(2)(B) . . . . Thomas Y. Allman

U.S. Biometric Systems Privacy Primer . . . . The Sedona Conference

The Sedona Conference Commentary on Privilege Logs . . . . The Sedona Conference

Evaluating the FTC's Authority to Enforce the GLBA's Provisions Regarding the Security and Privacy of Consumer Financial Information: Lessons from Recent Case Law . . . . Douglas H. Meal & Sharilyn N. Clark

Testing the Limits of the IP Legal Regimes: The Unique Challenges of Artificial Intelligence . . . . Jim W. Ko & Hon. Paul R. Michel

The Sedona Conference®

Antitrust Law, Complex Litigation, Intellectual Property Rights,
and Data Security and Privacy Law

The Sedona Conference Journal®

Volume 25

■

2024

Number 1

The Sedona Conference

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual or semi-annual basis, containing selections from the preceding year's conferences and Working Group efforts. A PDF copy of The Journal is available on a complimentary basis and can be downloaded from the Publications page on The Sedona Conference website: www.thesedonaconference.org. Check our website for further information about our conferences, Working Groups, and publications.

Comments (strongly encouraged) and requests to reproduce all or portions
of this issue should be directed to:
The Sedona Conference,
301 East Bethany Home Road, Suite C-297, Phoenix, AZ 85012 or
info@sedonaconference.org or call 1-602-258-4910.

The Sedona Conference Journal® cover designed by MargoBDesignLLC at www.margobdesign.com.

Cite items in this volume to "25 Sedona Conf. J. _____ (2024)."

Publisher's Note

Welcome to Volume 25, Number 1, of *The Sedona Conference Journal* (ISSN 1530-4981), published by The Sedona Conference (TSC), a nonpartisan and nonprofit 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of complex civil litigation, intellectual property rights, international data transfers, and data security and privacy law. The mission of TSC is to move the law forward in a reasoned and just way through the creation and publication of nonpartisan consensus commentaries and advanced legal education for the bench and bar.

TSC employs three main strategies to achieve its mission. First, it conducts limited-attendance conferences of the nation's leading jurists, lawyers, academics, and experts to examine cutting-edge issues of law and policy. Second, Working Groups in TSC's Working Group Series pursue in-depth study of these legal issues and develop consensus-based nonpartisan commentaries of immediate and practical benefit to the bench and bar. Finally, TSC disseminates the learning developed in the conferences and by the Working Groups through accredited continuing legal education programs under The Sedona Conference Institute banner, various International Programmes on global legal issues, and webinars on a variety of topics. *The Sedona Conference Journal* supports all these activities.

Volume 25, Number 1, of the *Journal* represents the sweep of TSC's ongoing activities. It contains two nonpartisan consensus commentaries from The Sedona Conference Working Group One on Electronic Document Retention and Production and one nonpartisan consensus commentary from the Working Group Eleven on Data Security and Privacy Liability. This volume also contains four articles written specifically for the *Journal* on timely, cutting-edge legal topics: one on the application of Artificial Intelligence to the essential task of document review in civil litigation, one on the "intent to deprive" element of sanctions for the failure to produce electronic discovery, one reviewing recent case law on the Federal Trade Commission's authority to enforce provisions of the Gramm-Leach-Bliley Act, and a groundbreaking article on the challenges Artificial Intelligence presents to established Intellectual Property Law, with some perhaps controversial proposals for reshaping IP law going forward. That article, coming out of a recent TSC Conference, will lead to the formation in 2025 of a new Working Group Thirteen on Artificial Intelligence and the Law, and in turn the publication of future consensus-based commentaries and the production of continuing legal education programs. This is the Sedona virtuous circle, and we invite you to participate.

I would like to thank the editors of the Working Group commentaries published in this volume of the *Journal,* as well as the authors of the individual articles. In addition, I would like to acknowledge the informal peer reviewers who volunteered their time and talents to make sure this volume of the *Journal* meets the highest professional standards: Phillip Favro of Innovative Driven, Brian E. Ferguson of Winston & Strawn LLP, Prof. Daniel W. Linna of Northwestern Pritzker School of Law, and Matthew D. Powers of Tensegrity Law Group. None of the articles necessarily reflect their personal views or those of their respective organizations.

Finally, this volume of the *Journal* notes with sadness the passing of Craig Weinlein, TSC's Executive Director of ten years and the "editor in chief" of the *Journal* during that time. His kindness, patience, and attention to detail will be sorely missed as we strive to carry on the mission of TSC.

For more information about The Sedona Conference and its activities, please visit our website at www.thesedonaconference.org

Kenneth J. Withers
Executive Director
The Sedona Conference
August 2024

The Sedona Conference gratefully acknowledges the contributions of its Working Group Series annual sponsors (www.thesedonaconference.org/sponsors), event sponsors, members, and participants whose volunteer efforts and financial support make participation in The Sedona Conference and its activities a thought-provoking and inspiring experience.

In Memoriam: Craig W. Weinlein

Volume 25 of *The Sedona Conference Journal* is dedicated to the memory of Craig W. Weinlein, executive director of The Sedona Conference from 2014 until his death at the age of 68 on June 9, 2024.

Craig succeeded founder Richard Braman as Sedona's executive director in 2014, but his involvement dated back to the organization's very beginnings, serving on the faculty of Sedona's first Conference on Patent Litigation in 2000.

He was deeply committed to the organization's mission of moving the law forward in a reasoned and just way and was soon one of its preeminent advocates. He became a member of The Sedona Conference Advisory Board in 2004 and joined its Board of Directors in 2009. He was chair of the Board of Directors at the time of his death.

Under Craig's leadership, The Sedona Conference stabilized its finances and staff and expanded its substantive scope. He guided the organization through the Covid crisis, and it emerged even stronger, something few nonprofits could claim. As the calendar turned to 2024, he was laying the groundwork for new initiatives into the intersection of Artificial Intelligence and the Law.

His leadership will be sorely missed, but he left behind a strong and prosperous organization, and the Sedona community will carry on in his absence.

Prior to becoming Sedona's executive director, Craig was a partner with Carrington, Colemen, Sloman & Blumenthal, LLP in Dallas, Texas. He joined the firm in 1981, shortly after earning his LL.M. from Columbia University, and remained in its employ for 33 years, practicing primarily in the area of complex litigation, with a concentration on intellectual property cases. He served 10 years as chair of Carrington's Intellectual Property Practice Group.

While in private practice, he tried dozens of cases and argued numerous appeals in federal and state court. He is counsel of record in 29 reported court decisions.

While Craig will be remembered as an influential leader in the legal profession, his co-workers at The Sedona Conference remember him for his generosity, kindness, sense of humor, and even temperament. He was as much a father figure as he was a boss, with a deep well of patience and understanding and always willing to listen with a sympathetic ear.

Craig was a prolific author. His book *The Art of Witness Preparation*, published in 2012, was a unique contribution to the scholarship on complex litigation by providing guidance on preparing witnesses to testify effectively and persuasively in civil litigation. Unlike most literature devoted to trial advocacy, the book focused on the witness's performance in the courtroom rather than the lawyer's, addressing an often neglected angle for civil trial attorneys.

His diverse catalogue of publication credits also includes articles in T*he American Journalism Review*, *The Journal of Arts Management and Law*, *The American Symphony Orchestra League's Principles of Orchestra Management*, and *The Journal of Air Law and Commerce*.

Craig's authorship provided a hint of his many varied interests. He played drums in a Phoenix-area band, Guitarras Latinas, was an accomplished photographer, an avid fly fisherman, a superb cook, and had a history of involvement in musical theater dating back to his youth.

His parents, Alphonso and Estelle Weinlein, ran a dance studio in Poughkeepsie, N.Y., and Craig was a proficient enough dancer to perform twice on the Ed Sullivan Show and appear on stage, according to The Poughkeepsie Journal, with the likes of Don Ameche, Carol Lawrence, Robert Goulet, and Ethel Merman, among others. Child actress Pia Zadora was a onetime dance partner.

For all his devotion to The Sedona Conference, it was at best second fiddle to Craig's true pride and joy, his family: Christine, his wife of 44 years; daughter Megan Au; son Christopher; and grandsons Bryson and Preston Au.

On behalf of all whose lives he touched, The Sedona Conference expresses its deepest gratitude to Craig W. Weinlein.

Journal Editorial Board

The Sedona Conference Advisory Board

Judicial Advisory Board

Table of Contents

Publisher's Note i

In Memoriam: Craig W. Weinlein iii

Journal Editorial Board v

The Sedona Conference Advisory Board vi

The Sedona Conference Judicial Advisory Board vii

The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control"

The Sedona Conference 1

TAR 1 Reference Model: An Established Framework Unifying Traditional and GenAI Approaches to Technology-Assisted Review

Tara Emory, Jeremy Pickens & Wilzette Louis 109

The Ubiquitous Role of the Specific "Intent to Deprive" Requirement of Amended Rule 37(e)(2)(B)

Thomas Y. Allman 137

The Sedona Conference U.S. Biometric Systems Privacy Primer

The Sedona Conference 163

The Sedona Conference Commentary on Privilege Logs

The Sedona Conference 221

Evaluating the FTC's Authority to Enforce the GLBA's Provisions Regarding the Security and Privacy of Consumer Financial Information: Lessons from Recent Case Law

Douglas H. Meal & Sharilyn N. Clark 343

Testing the Limits of the IP Legal Regimes: The Unique Challenges of Artificial Intelligence

Jim. W. Ko & Hon. Paul R. Michel 389

THE SEDONA CONFERENCE COMMENTARY ON RULE 34 AND RULE 45 "POSSESSION, CUSTODY, OR CONTROL"

A Project of The Sedona Conference Working Group on Electronic Document Retention & Production (WG1)

Author: The Sedona Conference
Editor-in-Chief & Steering Committee Liaison: Paul D. Weiner
Judicial Participant: The Honorable Kristen L. Mix

Drafting Team:

Victor L. Cardenas Jr.
Alitia Faccone
Susan Barrett Harty
Mark Kindy
Edwin Lee
Lauren E. Schwartzreich
Ronni D. Solomon
Martin T. Tully
Cheryl Vollweiler
Kelly M. Warner
W. Lawrence Wescott II
James S. Zucker

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

2024 COVER MEMORANDUM

In 2016, consistent with its mission to move the law forward in a reasoned and just way and to provide thought leadership on this issue, The Sedona Conference published its *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* 17 SEDONA CONF. J. 467 (2016). The *Commentary* analyzed the different tests federal circuits have applied to determine whether a litigant or subpoenaed non-party has "possession, custody, or control" of documents or data under Rules 34 and 45, and identified a split of authority between circuits that apply a "practical ability" standard, circuits that apply a "legal right" standard, those that have applied a "legal right plus notification" standard, and even some circuits where district courts have applied both the "practical ability" and "legal right" tests. The Sedona Conference's 2016 recommendations on this issue are summarized in the Abstract to the *Commentary*.

In January 2023, the Steering Committee of Working Group 1 appointed a Brainstorming Group to consider and make recommendations to the WG1 Steering Committee whether an update of the 2016 *Commentary* would be beneficial.

The Brainstorming Group held extensive meetings from January 2023 until April 2023, during which it conducted detailed legal research on federal and state cases that have addressed the issues of Rule 34 and Rule 45 "possession, custody or control" since the original *Commentary* was published, and dialogued about whether updates in technology like cloud computing and ephemeral messaging or developments in other areas of the law such as privacy and international laws or regulations warranted updating the 2016 *Commentary*.

The Brainstorming Group led a session at the 2023 WG1 Midyear Meeting in Portland, Ore., on April 27, 2023, entitled, *What's the Verdict: Updating The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* where it presented an outline of the issues under consideration by the Brainstorming Group and dialogued with WG1 members in attendance on those issues.

After the meeting, the Brainstorming Group reconvened to consider the dialogue from the Midyear Meeting.

Conclusion

The Brainstorming Group reached consensus that Sedona need not update the original 2016 *Commentary* because the guidance is still valid, and there is still consensus in WG1 regarding the recommendations in the original *Commentary*.

The WG1 Steering Committee, by consensus, adopted that recommendation.

The Sedona Conference, therefore, is updating the cover of the *Commentary* to reaffirm its recommendations, consistent with Sedona's mission of moving the law forward in a reasoned and just way. The contents of the *Commentary* otherwise remain unchanged.

The Sedona Conference acknowledges the efforts of brainstorming group leaders Ashley Picker Dubin and Paul Weiner in bringing this project to completion. We also thank brainstorming group members Elliot Bienenfeld, Jack Bisceglia, Vince Carnevale, Jessica Tseng Hasen, Leeanne Mancari, Jason Moore, David Nolte, Kristen Orr, Jon Polenberg, Kyle Pozan, and Caleb Sweeney and steering committee liaisons Tessa Jacob, Kaleigh Boyd, and Sandra Metallo-Barragan for their dedication and contributions to this project.

January 2024

PREFACE

Welcome to the final, July 2016, version of The Sedona Conference *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). The Sedona Conference is a 501(c)(3) research and educational institute that exists to allow leading jurists, lawyers, experts, academics, and others, at the cutting edge of issues in the areas of antitrust law, complex litigation, and intellectual property rights, to come together in conferences and mini-think tanks called Working Groups to engage in true dialogue, not debate, in an effort to move the law forward in a reasoned and just way.

The public comment version of The Sedona Conference *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control"* was published in April 2015 after two years of dialogue, review, and revision, including discussion at two of our WG1 midyear meetings. The public comment period closed June 15, 2015, and was cited six months later by the United States District Court in *Matthew Enterprise, Inc. v. Chrysler Group LLC*, No. 12-cv-04236, 2015 WL 8482256 (N.D. Cal. Dec. 10, 2015). The editors reviewed the public comments received and, where appropriate, incorporated those into this final version. I thank once again all of the drafting team members for their dedication and contribution to this project. Team members that participated and deserve recognition for their work are: Victor L. Cardenas Jr., Alitia Faccone, Susan Barrett Harty, Mark Kindy, Edwin Lee, Lauren E. Schwartzreich, Ronni D. Solomon, Martin T. Tully, Cheryl Vollweiler, Kelly M. Warner, W. Lawrence Wescott II, and James S. Zucker. The Sedona Conference also thanks The Honorable Kristen L. Mix for her participation as a Judicial Observer. Finally, The Sedona Conference thanks Paul D. Weiner for serving as both the Editor-in-Chief and Steering Committee Liaison.

We hope our efforts will be of immediate and practical assistance to judges, parties in litigation and their lawyers, and database management professionals. We continue to welcome comments for consideration in future updates. If you wish to submit feedback, please email us at comments@sedonaconference.org. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be.

Craig Weinlein
Executive Director
The Sedona Conference
July 2016

TABLE OF CONTENTS

I. Abstract 10

II. The Sedona Conference Principles on Possession, Custody, or Control 12

III. Background 14

A. Rules 34 and 45 Impose Important Obligations on Parties Deemed to Control Documents and ESI and the Law Prescribes Consequences for not Meeting Those Obligations 14

B. Interpretation of Rule 34 and Rule 45 Possession, Custody, or Control is Inconsistent across Federal Circuits, Leading to Irreconcilable Standards 17

1. The Three Standards for Rule 34 and Rule 45 Possession, Custody, or Control 17

2. Variances in Application of the Three Standards..27

C. A Deeper Look at the Practical Ability Standard Demonstrates that it Produces Potentially Unfair Results 34

1. The Practical Ability Standard may Compromise the Ability of Parties with Cross-Border Operations to Comply with Their Legal Obligations, and Gives Short Shrift to Corporate Formalities of Legally Distinct Entities 35

2. The Practical Ability Standard may Compel an Entity to Produce Documents and ESI in Violation of an Existing Contract...........................41

3. The Practical Ability Standard Often Fails to Recognize Distinctions between Separate Sister Corporations 41

4. The Practical Ability Standard may Compel Individuals to Produce Documents and ESI in the Possession of Companies they Own but that are not Parties to a Case 44

5. The Practical Ability Standard may Compel Corporate Parties to Produce Documents and ESI in the Possession of Former or Current Employees or Employers even if the Employers have no Legal Right to Demand or Obtain such Documents and ESI 45

6. The Practical Ability Standard may Compel Service Providers to Produce Information Owned by Clients and Customers even if the Service Provider has no Legal Right to Demand or Obtain such Documents and ESI 49

7. Effect of "Control" Issues on Third-Party Discovery..53

D. How new Technologies may Influence the Rule 34 Possession, Custody, or Control Analysis 55

1. Cloud Computing 55

2. Social Media..58

3. The "Bring your Own Device to Work" Movement 60

4. Changing Locations/Jurisdictions 62

IV. The Sedona Conference Principles on Possession, Custody, or Control—with Commentary..........................63

Principle 1: A responding party will be deemed to be in Rule 34 or Rule 45 "possession, custody, or control" of Documents and ESI when that party has actual possession or the legal right to obtain and produce the Documents and ESI on demand. 63

A. Interpretation of Possession, Custody, or Control for Purposes of Rules 34 and 45 Should be Consistent across Federal Circuits 63

B. A Framework for a More Objective Definition of "Control" 64

C. The Legal Right Standard is a Better Test...................71

D. Illustrations of what Should and Should Not Constitute Rule 34 "Control" Under a Consistent Standard...79

Principle 2: The party opposing the preservation or production of specifically requested Documents and ESI claimed to be outside its control, generally bears the burden of proving that it does not have actual possession or the legal right to obtain the requested Documents and ESI...81

Whether "Control" Exists must be Answered, in the First Instance, by the Responding Party 81

Principle 3(a): When a challenge is raised about whether a responding party has Rule 34 or Rule 45 "possession, custody, or control" over Documents and ESI, the Court should apply modified "business judgment rule" factors that, if met, would allow certain, rebuttable presumptions in favor of the responding party..86

Principle 3(b): In order to overcome the presumptions of the modified business judgment rule, the requesting party bears the burden to show that the responding party's decisions concerning the location, format, media, hosting, and access to Documents and ESI lacked a good faith basis and were not reasonably related to the responding party's legitimate business interests. 86

A. Rule 34 Application of the Business Judgment Rule...86

B. Appropriate Modifications of the Business Judgment Rule for Rule 34 and Rule 45 Analysis of Possession, Custody, or Control..............................93

C. The (Re)Emergence of Information Governance 98

Principle 4: Rule 34 and Rule 45 notions of "possession, custody, or control" should never be construed to override conflicting state or federal privacy or other statutory obligations, including foreign data protection laws...99

A. Examples of Overriding Statutory Restrictions 100

B. International Law must also be Considered 103

Principle 5: If a party responding to a specifically tailored request for Documents or ESI (either prior to or during litigation), does not have actual possession or the legal right to obtain the Documents or ESI that are specifically requested by their adversary because they are in the "possession, custody, or control" of a third party, it should, in a reasonably timely manner, so notify the requesting party to enable the requesting party to obtain the Documents or ESI from the third party. If the responding party so notifies the requesting party, absent extraordinary circumstances, the responding party should not be sanctioned or otherwise held liable for the third party's failure to preserve the Documents or ESI. 105

I. ABSTRACT

Rule 26(a) of the Federal Rules of Civil Procedure allows for the discovery of "documents, electronically stored information, and tangible things" in the responding party's "possession, custody, or control." Similarly, Rule 34(a) and Rule 45(a) obligate a party responding to a document request or subpoena to produce "documents, electronically stored information, and tangible things" in that party's "possession, custody, or control." Yet, the Rules are silent on what the phrase "possession, custody, or control" means. Therefore, parties must look to case law for a definition. Unfortunately, the case law across circuits (and often within circuits themselves) is unclear and, at times, inconsistent as to what is meant by "possession, custody, or control," resulting in a lack of reliable legal—and practical—guidance. The inconsistent interpretation and application of Rules 34 and 45 in this context are especially problematic because parties remain absolutely responsible for preserving and producing information within their "possession, custody, or control" and face material consequences, including sanctions, for their failure to do so.

Furthermore, in today's digital world, the determination of whether and when information should be considered to be in a responding party's "possession, custody, or control" has become more complex. New technologies and organizational initiatives have further blurred the legal and operational lines of who actually "controls" data for purposes of preservation and production, and have multiplied the practical problems associated with preserving and producing data that a party does not directly control. The proliferation, use, and transfer of vast quantities of digital information, deciding how and where to store that information, and increasingly complex business relationships aimed at addressing the creation and storage of information, have all spawned multiple issues that have profoundly

affected the issue of "possession, custody, or control" under the discovery rules.

This Commentary is intended to provide practical, uniform, and defensible guidelines regarding when a responding party should be deemed to have "possession, custody, or control" of documents and all forms of electronically stored information (hereafter, collectively referred to as "Documents and ESI") subject to Rule 34 and Rule 45 requests for production. A secondary, corollary purpose of this Commentary is to advocate abolishing use of the common-law "Practical Ability Test" for purposes of determining Rule 34 and Rule 45 "control" of Documents and ESI. Simply stated, this common-law test has led to inequitable situations in which courts have held that a party has Rule 34 "control" of Documents and ESI even though the party did not have the *actual ability* to obtain the Documents and ESI. Therefore, this Commentary recommends that courts should interpret and enforce Rule 34 "possession, custody, or control" obligations in ways that do not lead to sanctions for unintended and uncontrollable circumstances. To support that recommendation, this Commentary also looks to several well-established legal doctrines upon which to model the contemporary scope of a party's duty to identify, preserve, and collect Documents and ESI, such as reliance upon a modified version of the business judgment rule. Helping resolve the disparity among circuits to bring a uniform, national standard to this important area of the law is consistent with Sedona's mission of moving the law forward in a just and reasoned way.

II. THE SEDONA CONFERENCE PRINCIPLES ON POSSESSION, CUSTODY, OR CONTROL

Principle 1: A responding party will be deemed to be in Rule 34 or Rule 45 "possession, custody, or control" of Documents and ESI when that party has actual possession or the legal right to obtain and produce the Documents and ESI on demand.

Principle 2: The party opposing the preservation or production of specifically requested Documents and ESI claimed to be outside its control, generally bears the burden of proving that it does not have actual possession or the legal right to obtain the requested Documents and ESI.

Principle 3(a): When a challenge is raised about whether a responding party has Rule 34 or Rule 45 "possession, custody, or control" over Documents and ESI, the Court should apply modified "business judgment rule" factors that, if met, would allow certain, rebuttable presumptions in favor of the responding party.

Principle 3(b): In order to overcome the presumptions of the modified business judgment rule, the requesting party bears the burden to show that the responding party's decisions concerning the location, format, media, hosting, and access to Documents and ESI lacked a good faith basis and were not reasonably related to the responding party's legitimate business interests.

Principle 4: Rule 34 and Rule 45 notions of "possession, custody, or control" should never be construed to override conflicting state or federal privacy or other statutory obligations, including foreign data protection laws.

Principle 5: If a party responding to a specifically tailored request for Documents or ESI (either prior to or during litigation) does not have actual possession or the legal right to obtain the Documents or ESI that are specifically requested by their adversary because they are in the "possession, custody, or control" of a third party, it should, in a reasonably timely manner, so notify the requesting party to enable the requesting party to obtain the Documents or ESI from the third party. If the responding party so notifies the requesting party, absent extraordinary circumstances, the responding party should not be sanctioned or otherwise held liable for the third party's failure to preserve the Documents or ESI.

III. BACKGROUND

A. Rules 34 and 45 Impose Important Obligations on Parties Deemed to Control Documents and ESI and the Law Prescribes Consequences for not Meeting Those Obligations

If a responding party has possession, custody, or control of relevant[1] Documents and ESI, it has a duty to preserve[2] and produce[3] them in discovery. If a party fails to do so, it may be sanctioned.[4] This outcome makes sense if a party has physical possession or actual custody of its own Documents and ESI; for example, Documents and ESI stored on its servers on the company's premises or a computer that an individual owns. The preservation and production requirement also makes sense if a party enters into a direct contractual relationship with another to handle its Documents and ESI, such as when a party outsources all of its payroll functions to a third party and retains the legal right to obtain Documents and ESI on demand and/or can set the terms and conditions on which it may retrieve those Documents and ESI, or when an individual signs up with an ISP (internet service provider) for his/her personal email account. In those circumstances, the Rule 34 and Rule 45 terms "possession" and "custody" are fairly straightforward and do not present a problem. Indeed, when Rules 34 and 45 were amended in 2006 to specifically include "electronically stored information," it was far easier to enforce these Rules along bright lines without

[1] *See* FED. R. CIV. P. 26(b) (setting forth the scope and limits of discovery, including that: discovery must be proportional to the needs of the case; discovery of ESI must be limited from sources that are not reasonably accessible due to undue burden or cost; and privileged matters are not subject to discovery).

[2] Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217–18 (S.D.N.Y. 2003).

[3] *See* FED. R. CIV. P. 34(a).

[4] Metropolitan Opera Ass'n v. Local 100, 212 F.R.D. 178 (S.D.N.Y. 2003).

the further need to specifically define possession, custody, or control.[5]

However, in today's dynamic and ever-expanding digital information landscape, potential unfairness develops when an overly expansive definition of "control" is applied. Simply put, in today's digital world, the relationship between *a party in litigation* and the individual or entity that *actually possesses* potentially relevant Documents and ESI has become far more complex and multi-faceted.[6] In many instances, Documents and ESI are

[5] While the Federal Rules of Civil Procedure were amended in December 2015, those amendments did not specifically address the issues of Rule 34 and 45 "possession, custody, or control." The December 2015 amendments did, however, recognize that the data explosion that created the need for rule amendments in 2006 to specifically address "electronically stored information" has continued unabated, thus supporting the need for additional rule amendments in 2015:

> [T]he explosion of ESI in recent years has presented new and unprecedented challenges in civil litigation. . . . [T]he remarkable growth of ESI will continue and even accelerate. One industry expert reported to the Committee that there will be some 26 billion devices on the Internet in six years – more than three for every person on earth.

See Memorandum from Chair of the Advisory Committee on Federal Rules of Civil Procedure Judge David G. Campbell to Chair of the Standing Committee on Rules of Practice and Procedure Judge Jeffrey Sutton, p. B-15 (Sept. 2014), http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjV9c7KrfrMAhWq5IMKHVVHDQEQFggcMAA&url=http%3A%2F%2Fwww.uscourts.gov%2Ffile%2F18218%2Fdownload&usg=AFQjCNEiQyk8P6qPY5YW1PgfM-spZBn4Vg&bvm=bv.122676328,d.amc [hereinafter Advisory Committee Report].

[6] The drafters of the 2015 federal rule amendments specifically took note of how new technologies were impacting litigation:

> Significant amounts of ESI will be created and stored not only by sophisticated entities with large IT departments, but also by unsophisticated persons whose lives are recorded on their phones, tablets, cars, social media pages, and tools not even

in the possession or custody of non-parties to a lawsuit, creating scenarios more difficult for courts and parties to navigate. Some everyday examples of these challenges include the following:

- If a service provider has no legal right to obtain information from one of its customers, should it be required to preserve, search, and produce the customer's information that it does not have in litigation on the threat of sanctions for failure to do so?
- If a subsidiary corporation that is a separate legal entity from its parent corporation has no legal right to obtain Documents and ESI from its parent, should the subsidiary be required to preserve, search, and produce Documents and ESI from its parent in litigation on the threat of sanctions for failure to do so?
- Should the same obligations exist if that same parent corporation is also located in a foreign jurisdiction where it is subject to data privacy or blocking statutes that do not contain exceptions for American litigation?
- If an employer has neither the actual ability nor legal right to obtain Documents and ESI from its employee's personal devices—because doing so may violate important public policy interests and statutes (including social media password protection laws that have been enacted in many states) or for other reasons—should the

presently foreseen. Most of this information will be stored somewhere on remote servers, often referred to as the "cloud," complicating the preservation task.

See Advisory Committee Report, *supra* note 5.

> employer be required to preserve, search, and produce that information in litigation on the threat of sanctions for failure to do so?

The crux of the matter is that Rules 34 and 45 require the responding party to produce Documents and ESI within a party's possession, custody, or control, yet, nowhere in the Federal Rules are the terms possession, custody, or control defined.[7] As a result, different circuits across the country have created an inconsistent body of case law and standards about what constitutes "control" over data.[8]

B. Interpretation of Rule 34 and Rule 45 Possession, Custody, or Control is Inconsistent across Federal Circuits, Leading to Irreconcilable Standards

1. The Three Standards for Rule 34 and Rule 45 Possession, Custody, or Control

The federal circuits have taken differing approaches to what constitutes possession, custody, or control under Rules 34 or 45. This has led to a lack of clarity for lawyers and litigants that must manage discovery or advise clients regarding the production of Documents and ESI in multiple jurisdictions.[9] This is especially problematic given that in today's digital world, borders

[7] FED. R. CIV. P. 34(a), 45(a).

[8] *See, e.g.*, Goodman v. Praxair Servs., Inc., 632 F. Supp. 2d 494, 514 (D. Md. 2009) ("What is meant by [Rule 34] 'control' . . . has yet to be fully defined.").

[9] As discussed below, one of the primary drivers of the 2015 amendments to Rule 37(e) was to "provide a uniform standard in federal courts." *See* FED. R. CIV. P. 37(e)(2), Committee Note (Dec. 15, 2015). *See also* Advisory Committee Report, *supra* note 5, at B-14, B-17 ("Resolving the circuit split with a more uniform approach . . . has been recognized by the Committee as a worthwhile goal. . . . [The] primary purpose of [amended Rule 37(e)] is to eliminate the circuit split on [a key aspect of the rules].").

have broken down and many businesses and individuals live their lives and conduct business nationwide.

As a general matter, the case law in this area has coalesced into three broad interpretations of when the producing party will be deemed to have Rule 34 "control" over Documents and ESI in the hands of a third party. The result is to impose an obligation on the litigant to preserve, collect, search, and produce the Documents and ESI in the hands of the third party, even though the producing party does not actually possess or have actual custody of the Documents and ESI at issue. These three interpretations are:

- **Legal Right Standard:** When a party has the legal right to obtain the Documents and ESI (the "Legal Right Standard");
- **Legal Right Plus Notification:** When a party has the legal right to obtain the Documents and ESI. Plus, if the party does not have the legal right to obtain the Documents and ESI that have been specifically requested by its adversary but is aware that such evidence is in the hands of a third party, it must so notify its adversary (the "Legal Right Plus Notification Standard"); and
- **Practical Ability Standard:** When a party does not have the legal right to obtain the Documents and ESI but has the "practical ability" to do so (the "Practical Ability Standard" or "Practical Ability Test").

The Legal Right Standard requires a party to preserve, collect, search, and produce Documents and ESI which the party has a legal right to obtain. The Legal Right Standard has been followed by some federal courts in the Third, Fifth, Sixth, Seventh, Eighth, Ninth, Tenth, and Eleventh Circuits.[10] [11]

[10] *See, e.g.,* **3rd Circuit:** Brewer v. Quaker State Oil Ref. Co., 72 F.3d 326, 334 (3d Cir. 1995); **5th Circuit:** Wiwa v. Royal Dutch Petroleum Co., 392 F.3d 812, 821 (5th Cir. 2004) (finding plaintiff's subpoena requesting all documents to which the defendant had "access" overly broad, and limiting the scope of documents requested pursuant to Fed. R. Civ. P. 34(a) to those over which the defendant had "control"); **6th Circuit:** *In re* Bankers Trust Co., 61 F.3d 465, 469 (6th Cir. 1995) (explaining that a party has possession, custody, or control only when the party has the legal right to obtain the documents upon demand); *accord* Flagg v. City of Detroit, 252 F.R.D. 346, 353 (E.D. Mich. 2008) ("documents are deemed to be within the 'control' of a party if it 'has the legal right to obtain the documents on demand'"); Pasley v. Caruso, No. 10-cv-11805, 2013 WL 2149136, at *5 (E.D. Mich. May 16, 2013) (concluding that the Sixth Circuit had not adopted the "expansive notion of control" constituting the Practical Ability Test); **7th Circuit:** Chaveriat v. Williams Pipe Line Co., 11 F.3d 1420, 1427 (7th Cir. 1993) (affirming party's failure to produce documents not in its possession and to which it had no legal right); United States v. Approximately $7,400 in U.S. Currency, 274 F.R.D. 646, 647 (E.D. Wis. 2011) (holding that a party is obligated to produce records when it has a legal right to obtain those records even if it does not have actual possession); DeGeer v. Gillis, 755 F. Supp. 2d 909, 924 (N.D. Ill. 2010) (same, in Rule 45 context); **8th Circuit:** Beyer v. Medico Ins. Grp., No. CIV. 08-5058, 2009 WL 736759, at *5 (D.S.D. Mar. 17, 2009) ("The rule that has developed is that if a party 'has the legal right to obtain the document,' then the document is within that party's 'control' and, thus, subject to production under Rule 34."); United States v. Three Bank Accounts Described as: Bank Account # 9142908 at First Bank & Trust, Brookings, S. Dakota, No. CIV. 05-4145-KES, 2008 WL 915199, at *7 (D.S.D. Apr. 2, 2008) ("To the extent the government's subpoena asks for documents from Mr. Dockstader which he does not have in his possession or custody, and as to which he has no legal right to obtain the document, Mr. Dockstader's objection is sustained."); New All. & Grain Co. v. Anderson Commodities, Inc., No. 8:12CV197, 2013 WL 1869832, at *8 (D. Neb. May 2, 2013) (concluding that defendants had gone "above and beyond their obligation under the Federal Rules of Civil Procedure" by requesting and obtaining documents that they did not have the "right or authority" to demand); **9th Circuit:** 7-UP Bottling Co. v. Archer Daniels Midland Co. *(In re* Citric Acid Litig.), 191 F.3d 1090 (9th Cir. 1999), *cert. denied sub nom.* Gangi Bros. Packing Co. v. Cargill, Inc., 529 U.S. 1037 (2000); **10th Circuit:** Am.

The Legal Right Plus Notification Standard similarly requires that a party preserve, collect, search, and produce Documents and ESI which it has a legal right to obtain, but also requires that the party must notify its adversary about potentially relevant Documents and ESI held by third parties.[12] The obligation to notify the adversary about evidence in the hands of third parties can be traced to products liability litigation, in which the

Maplan Corp. v. Heilmayr, 203 F.R.D. 499, 502 (D. Kan. 2001) (rejecting the Practical Ability Test and explaining that "[a]s it is undisputed that defendant does not have actual possession of the VET documents, he can be required to produce only those documents that he has 'legal right' to obtain on demand"); *accord* Noaimi v. Zaid, 283 F.R.D. 639, 641 (D. Kan. 2012) (same); Kickapoo Tribe of Indians of Kickapoo Reservation in Kansas v. Nemaha Brown Watershed Joint District No. 7, 294 F.R.D. 610 (D. Kan. 2013) (holding that plaintiff had not met its burden of proving defendant had necessary control because it "ha[d] not shown that the District has the legal right to obtain the documents requested on demand from former District Board members, staff, or employees"); **11th Circuit:** Searock v. Stripling, 736 F.2d 650, 653 (11th Cir. 1984) ("Under Fed. R. Civ. P. 34, control is the test with regard to the production of documents. Control is defined not only as possession, but as the legal right to obtain the documents requested upon demand.").

[11] Note that some courts in the 11th Circuit have also applied the Practical Ability Standard. *See, e.g.*, Anz Advanced Techs. v. Bush Hog, LLC, No. CIV.A. 09-00228-KD-N, 2011 WL 814663, at *9 (S.D. Ala. Jan. 26, 2011), report and recommendation adopted *sub nom*. Anz Advanced Techs., LLC v. Bush Hog, LLC, No. CIV.A. 09-00228-KD-N, 2011 WL 814612 (S.D. Ala. Mar. 3, 2011) ("'[C]ontrol' has been 'construed broadly by the courts' to include not just a legal right, but also a 'practical ability to obtain the materials' on demand."). In one public comment, it was noted that the decision in the 11th Circuit Case of *Searock v. Stripling*, 736 F.2d 650, 653 (11th Cir. 1984), that followed the Legal Right Standard, "has been ignored by some district courts in the Circuit."

[12] *See, e.g.*, Silvestri v. Gen. Motors Corp., 271 F.3d 583, 591 (4th Cir. 2001) ("If a party cannot fulfill this duty to preserve because he does not own or control the evidence, he still has an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence.").

defendant manufacturer would be unable to inspect the product, or otherwise assert defenses based on plaintiffs' "misuse, alteration or poor maintenance" of the product.[13] The Legal

[13] Anderson v. Schwartz, 179 Misc. 2d 1001, 1003, 687 N.Y.S.2d 232, 237 (Sup. Ct. 1999).

Right Plus Notification Standard has been followed by some federal courts in the First, Fourth, Sixth,[14] and Tenth Circuits.[15]

[14] Note that some courts in the 6th Circuit have applied both the Legal Right and Legal Right Plus Notification Standard, thus:

- [Legal Right]: *In re* Bankers Trust Co., 61 F.3d 465, 469 (6th Cir. 1995) (holding that a party has possession, custody, or control only when the party has the legal right to obtain the documents upon demand); Pasley v. Caruso, No. 10-cv-11805, 2013 WL 2149136, at *5 (E.D. Mich. May 16, 2013) (holding that the Sixth Circuit had not adopted the "expansive notion of control" constituting the Practical Ability Test).
- [Legal Right Plus Notification]: Lexington Ins. Co. v. Tubbs, No. 06–2847–STA, 2009 WL 1586862, at *3 (W.D. Tenn. June 3, 2009) (holding "federal law of spoliation governs cases filed in federal court" and "[e]ven where a party does not own or control the evidence, the party still has a duty 'to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence'" (citing Silvestri v. Gen. Motors Corp., 271 F.3d 583, 591 (4th Cir. 1991) and sanctioning plaintiff for failure to preserve evidence)). *Cf.* Adkins v. Wolever, 692 F.3d 499, 505 (6th Cir. 2012) (reasoning that the "cases from around the country" plaintiff cites, including *Silvestri,* for the proposition that a spoliation sanction is proper "even though [defendant] was not personally responsible for the destruction of evidence . . . are not binding precedent requiring the district court to impose a spoliation sanction in this instance. [Courts] owe substantial deference to the professional judgment of prison administrators." (citing Beard v. Banks, 548 U.S. 521, 522 (2006) and holding "[t]he ultimate determination of culpability is within the district court's discretion so long as it is not a clearly erroneous interpretation of the facts")).

[15] *See, e.g.,* **1st Circuit:** Perez v. Hyundai Motor Co., 440 F. Supp. 2d 57, 61 (D.P.R. 2009) (citing *Silvestri*, 271 F.3d at 591, as the spoliation of evidence standard):

> The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation . . . . If a party cannot fulfill

The Practical Ability Standard requires a party to preserve, collect, search, and produce Documents and ESI *irrespective of that party's legal entitlement or actual physical possession of the documents* if a party has the "practical ability" (what that means is discussed in greater detail below) to obtain the Documents or ESI.[16] The Practical Ability Standard is followed by some federal

> this duty to preserve because he does not own or control the evidence, he still has an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence.

4th Circuit: Silvestri v. Gen. Motors Corp., 271 F.3d 583, 591 (4th Cir. 1991); **6th Circuit:** Lexington Ins. Co. v. Tubbs, No. 06–2847–STA, 2009 WL 1586862, at *3 (W.D. Tenn. June 3, 2009); *compare* Adkins v. Wolever, 692 F.3d 499, 505 (6th Cir. 2012); **10th Circuit:** Chavez v. Hatterman, No. CIV.06–cv–02525–WYD–MEH, 2009 WL 807440, at *2 (D. Colo. Jan. 20, 2009) (noting the *Silvestri* standard, but finding that plaintiff was not aware of relevancy of data at the time it should have been preserved).

[16] *In re* NTL, Inc. Securities Litigation, 244 F.R.D. 179, 195 (S.D.N.Y. 2007), *aff'd sub nom*. Gordon Partners v. Blumenthal, No. 02 CIV 7377LAK, 2007 WL 1518632 (S.D.N.Y. May 17, 2007).

courts in the Second, Fourth,[17] Eighth,[18] Tenth,[19] Eleventh,[20] and District of Columbia Circuits.[21]

[17] Note that courts in the 4th Circuit have applied both the Practical Ability Standard and Legal Right Plus Notification Standard:

- [Practical Ability]: Digital Vending Services International, Inc. v. The University of Phoenix, No. 2:09cv555, 2013 WL 311820, at *6 (E.D. Va. Oct. 3, 2013) (ability to control is defined as "when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action") (internal citation omitted); Grayson v. Cathcart, No. 2:07-00593-DCN, 2013 WL 1401617, at *3 (D.S.C. Apr. 8, 2013) ("Control does not require legal ownership or actual physical possession of documents at issue; rather 'documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action.'"); Ayers v. Sheetz, Inc., No.: 3:11-cv-00434, 2012 WL 5331555, at *1 (S.D.W. Va. Oct. 26, 2012) ("Control may be inferred, even when a party does not have possession or ownership of the evidence, 'when that party has the right, authority, or practical ability to obtain [the evidence] from a non-party to the action.'").
- [Legal Right Plus Notification]: King v. American Power Conversion Corp., 181 F. App'x 373, 377–87 (4th Cir. May 17, 2006) ("Accordingly, the Kings failed to discharge their duty to afford American Power sufficient notice. 'If a party cannot fulfill this duty to preserve [evidence] . . . , he still has an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence.'") (quoting Silvestri v. Gen. Motors Corp., 271 F.3d 583, 591 (4th Cir. 2001)); Ayers v. Sheetz, Inc., No. 3:11-CV-00434, 2012 WL 5183561, at *2 (S.D.W. Va. Oct. 18, 2012), *aff'd*, No. 3:11-CV-00434, 2012 WL 5331555 (S.D.W. Va. Oct. 26, 2012) ("This duty [to preserve] requires the party to 'identify, locate, and maintain information that is relevant to specific, predictable, and identifiable litigation' and to 'notify the opposing party of evidence in the hands of third parties."') (internal citation omitted).

[18] Note that courts in the 8th Circuit have applied both the Practical Ability Standard and the Legal Right Standard:

- [Practical Ability]: Prokosch v. Catalina Lighting, Inc., 193 F.R.D. 633, 636 (D. Minn. 2000) ("Therefore, under Rule 34, control does not require that the party have legal ownership or actual physical possession of the documents at issue; rather, documents are considered to be under a party's control when that party has the right, authority, or practical ability, to obtain the documents from a non-party to the action.") (citation and quotations omitted); Handi-Craft v. Action Trading, S.A., No. 4:02 CV 1731 LMB, 2003 WL 26098543, at *6 (E.D. Mo. Nov. 25, 2003) ("Thus, the appropriate test is not of legal entitlement, but of control or practical ability to obtain the documents.").
- [Legal Right]: Beyer v. Medico Ins. Group, No. CIV. 08-5058, 2009 WL 736759, at *5 (D.S.D. Mar. 17, 2009) ("The rule that has developed is that if a party 'has the legal right to obtain the document' then the document is within that party's 'control' and, thus, subject to production under Rule 34.") (internal citation omitted); United States v. Three Bank Accounts Described as: Bank Account # 9142908 at First Bank & Trust, Brookings, S. Dakota, No. CIV. 05-4145-KES, 2008 WL 915199, at *7 (D.S.D. Apr. 2, 2008) ("To the extent the government's subpoena asks for documents from Mr. Dockstader which he does not have in his possession or custody, and as to which he has no legal right to obtain the document, Mr. Dockstader's objection is sustained."); New All. & Grain Co. v. Anderson Commodities, Inc., No. 8:12CV197, 2013 WL 1869832, at *5 (D. Neb. May 2, 2013) (concluding that defendants had gone "above and beyond their obligation under the Federal Rules of Civil Procedure" by requesting and obtaining documents that they did not have the "right or authority" to demand).

19. Note that courts in the 10th Circuit have applied both the Practical Ability Standard, Legal Right Standard, and Legal Right Plus Notification Standard, thus:

- [Practical Ability]: Tomlinson v. El Paso Corp., 245 F.R.D. 474, 476 (D. Colo. 2007) ("Control 'comprehends not only possession, but also the right, authority, or ability to obtain the documents.'"); Ice Corp. v. Hamilton Sundstrand Corp., 245 F.R.D. 513, 517 (D. Kan. 2007) ("Production of documents not in a party's possession is required if a party has the *practical ability* to obtain the documents from another, irrespective of legal entitlements to the documents.") (internal quotation omitted).

- [Legal Right]: Am. Maplan Corp. v. Heilmayr, 203 F.R.D. 499, 501–02 (D. Kan. 2001) (rejecting the Practical Ability Test and explaining that, "[a]s it is undisputed that defendant does not have actual possession of the VET documents, he can be required to produce only those documents that he has 'legal right' to obtain on demand"); *accord* Noaimi v. Zaid, 283 F.R.D. 639, 641 (D. Kan. 2012) (criticizing Ice Corporation v. Hamilton Sundstrand Corp., 245 F.R.D. 513 (D. Kan. 2007) and reaching the same conclusion); Kickapoo Tribe of Indians of Kickapoo Reservation in Kansas v. Nemaha Brown Watershed Joint Dist. No. 7, 294 F.R.D. 610, 614 (D. Kan. 2013) (holding that plaintiff had not met its burden of proving defendant had necessary control because it "ha[d] not shown that the District has the legal right to obtain the documents requested on demand from former District Board members, staff, or employees").
- [Legal Right Plus Notification]: Chavez v. Hatterman, No. 06–cv–02525–WYD–MEH, 2009 WL 807440, at *2 (Jan. 20, 2009) (noting the *Silvestri* standard, but finding that plaintiff was not aware of relevancy of data at the time it should have been preserved).

20. Anz Advanced Techs. v. Bush Hog, LLC, No. CIV.A. 09-00228-KD-N, 2011 WL 814663, at *9 (S.D. Ala. Jan. 26, 2011) ("'[C]ontrol' has been 'construed broadly by the courts' to include not just a legal right, but also a 'practical ability to obtain the materials' on demand.").

21. *See, e.g.*, **2nd Circuit:** Shcherbakovskiy v. Da Capo Al Fine, Ltd., 490 F.3d 130, 138 (2d Cir. 2007) ("If a party has access and the practical ability to possess documents not available to the party seeking them, production may be required."); GenOn Mid-Atl v. Stone & Webster, 282 F.R.D. 346, 354 (S.D.N.Y. 2012), *aff'd sub nom*. GenOn Mid-Atl., LLC v. Stone & Webster, Inc., No. 11 CV 1299 HB, 2012 WL 1849101 (S.D.N.Y. May 21, 2012); **4th Circuit:** Digital Vending Services International, Inc. v. The University of Phoenix, No. 2:09cv555, 2013 WL 311820 at *6 (E.D. Va. Oct. 3, 2013); Grayson v. Cathcart, No. 2:07-00593-DCN, 2013 WL 1401617 at *3 (D.S.C. Apr. 8, 2013); Ayers v. Sheetz, Inc., No. 3:11-CV-00434, 2012 WL 5183561, at *2 (S.D.W. Va. Oct. 18, 2012); **8th Circuit:** Prokosch v. Catalina Lighting, Inc., 193 F.R.D. 633, 636 (D. Minn. 2000):

2. Variances in Application of the Three Standards

The different rules and corresponding circuit splits are set forth in the charts below, which also reflect that federal courts in some circuits have applied more than one standard.

> Therefore, under Rule 34, control does not require that the party have legal ownership or actual physical possession of the documents at issue; rather, documents are considered to be under a party's control when that party has the right, authority, or practical ability, to obtain the documents from a non-party to the action.

(citation and quotations omitted); Handi-Craft v. Action Trading, S.A., No. 4:02 CV 1731 LMB, 2003 WL 26098543, at *6 (E.D. Mo. Nov. 25, 2003) ("Thus, the appropriate test is not of legal entitlement, but of control or practical ability to obtain the documents."); **10th Circuit:** Tomlinson v. El Paso Corp., 245 F.R.D. 474, 475 (D. Colo. 2007) ("Therefore, Rule 34(a) enables a party seeking discovery to require production of documents beyond the actual possession of the opposing party if such party has retained any right or ability to influence the person in whose possession the documents lie."); **11th Circuit:** Anz Advanced Techs. v. Bush Hog, LLC, No. CIV.A. 09-00228-KD-N, 2011 WL 814663, at *9 (S.D. Ala. Jan. 26, 2011); *cf. also* Searock v. Stripling, 736 F.2d 650, 654 (11th Cir. 1984) (despite espousing the Legal Right Standard, stating "[w]e do not, however, completely rest our holding on this factor of 'control.' We find instead that the primary dispositive issue is whether [the defendant] made a good faith effort to obtain the documents over which he may have indicated he had 'control' in whatever sense, and whether after making such a good faith effort he was unable to obtain and thus produce them."); **District of Columbia Circuit:** Bush v. Ruth's Chris Steak House, Inc., 286 F.R.D. 1, 5 (D.D.C. 2012) ("Control does not require that the party have legal ownership or actual physical possession of the documents at issue, but rather 'the right, authority or practical ability to obtain the documents from a non-party to the action.'").

CATEGORY	**CIRCUIT**											
	1	2	3	4	5	6	7	8	9	10	11	D.C.
Legal Right			X		X	X	X	X	X	X	X	
Legal Right Plus Notification	X			X		X				X		
Practical Ability		X		X				X		X	X	X

To further complicate matters, even within these general categories there are differences in the ways in which federal courts within the circuits define and apply the standards:[22]

LEGAL RIGHT STANDARD	
CIRCUIT	**STANDARD**
3rd Circuit	"within the party's control"[23]

[22] *See* Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 540 (D. Md. 2010).

[23] Gerling Int'l Ins. Co. v. C.I.R., 839 F.2d 131, 140 (3d Cir. 1988) (The Third Circuit defines "control" as the "legal right to obtain documents on demand.") (internal quotation omitted); Sanofi-Aventis v. Sandoz, Inc., 272 F.R.D. 391, 395 (D.N.J. 2011) ("The control test articulated by the Third Circuit in *Gerling International* 'focuses on the relationship between the two parties.'"); Power Integrations, Inc. v. Fairchild Semiconductor Int'l Inc., 233 F.R.D. 143, 146 (D. Del. 2005) ("Control is defined as the legal right to obtain the documents required on demand."). *But see* Barton v. RCI, LLC, No. CIV.A. 10-3657 PGS, 2013 WL 1338235, at *6 (D.N.J. Apr. 1, 2013) (noting "[i]f the producing party has the legal right or practical ability to obtain the documents, then it is deemed to have 'control' . . . even if the documents are actually in the possession of a non-party") (internal citation omitted).

LEGAL RIGHT STANDARD	
CIRCUIT	**STANDARD**
5th Circuit	"the legal right to obtain the documents upon demand"[24]
6th Circuit	"the legal right to obtain the documents upon demand"[25]
7th Circuit	"control or custody of a document or thing"[26]

[24] Enron Corp. Savings Plan v. Hewitt Associates, LLC, 258 F.R.D. 149, 164 (S.D. Tex. 2009) ("Under Rule 34 documents are deemed within the possession, custody, or control of a party and subject to a request for production if the party has actual possession, custody, or control or has the legal right to obtain the documents on demand."). *But see* Piazza's Seafood World, L.L.C. v. Odom, No. CIV.A. 07-413-BAJ-CN, 2011 WL 3664437, at *3 n.6 (M.D. La. Aug. 19, 2011), *adhered to on reconsideration*, No. CIV.A. 07-413-BAJ-CN, 2011 WL 4565436 (M.D. La. Sept. 29, 2011) ("Federal courts have consistently held that documents are deemed to be within the 'possession, custody, or control' of a party for purposes of Rule 34 if the party has 'actual possession, custody, or control, or has the legal right to obtain the documents on demand or has the practical ability to obtain the documents from a non-party to the action.'"). *See also* Wood Group Pressure Control, L.P. v. B&B Oilfield Services, Inc., Civ. No. 06-3002 SECTION: "N" (4), 2007 U.S. Dist. LEXIS 83708 at *43–44 n.15 (E.D. La. 2007) ("Courts have extended the affirmative duty to preserve evidence to instances when that evidence is not directly within the party's custody or control so long as the party has access to or indirect control over such evidence.").

[25] *In re* Bankers Trust Co., 61 F.3d 465, 469 (6th Cir. 1995) (holding that a party has possession, custody, or control only when the party has the legal right to obtain the documents upon demand); Pasley v. Caruso, No. 10-cv-11805, 2013 WL 2149136, at *5 (E.D. Mich. May 26, 2013) (holding that the Sixth Circuit had not adopted the "expansive notion of control" constituting the Practical Ability Test).

[26] Chaveriat v. Williams Pipe Line Co., 11 F.3d 1420, 1427 (7th Cir. 1993) (affirming party's failure to produce documents not in its possession and to which it had no legal right); United States v. Approximately $7,400 in U.S. Currency, 274 F.R.D. 646, 647 (E.D. Wis. 2011) (holding that a party is obligated to produce records when it has a legal right to obtain those records

LEGAL RIGHT STANDARD	
CIRCUIT	**STANDARD**
8th Circuit	"if a party 'has the legal right to obtain the document,' then the document is within that party's 'control' and, thus, subject to production under Rule 34"[27]
9th Circuit	"the legal right to obtain the documents upon demand"[28]
10th Circuit	"legal right to obtain the documents on demand"[29]
11th Circuit	"Under Fed. R. Civ. P. 34 . . . Control is defined not only as possession, but as the legal right to obtain the documents requested upon demand."[30]

even if it does not have actual possession); DeGeer v. Gillis, 755 F. Supp. 2d 909, 924 (N.D. Ill. 2010) (same, in Rule 45 context); McBryar v. Int'l Union of United Auto. Aerospace & Agr. Implement Workers of Am., 160 F.R.D. 691, 694 (S.D. Ind. 1993).

[27] *See* Beyer v. Medico Ins. Group, No. CIV. 08-5058, 2009 WL 736759, at *5 (D.S.D. Mar. 17, 2009).

[28] Dugan v. Lloyds TSB Bank, PLC, No. 12CV02549WHANJV, 2013 WL 4758055, at *2 (N.D. Cal. Sept. 4, 2013) ("In the Ninth Circuit, 'control' is defined as 'the legal right to obtain documents upon demand.'"); Ubiquiti Networks, Inc. v. Kozumi USA Corp., No.12-cv-2582 CW JSC, 2013 WL 1767960, at *1 (N.D. Cal. Apr. 15, 2013) (same).

[29] Noaimi v. Zaid, 283 F.R.D. 639, 641 (D. Kan. 2012).

[30] Searock v. Stripling, 736 F.2d 650, 654 (11th Cir. 1984).

LEGAL RIGHT PLUS NOTIFICATION STANDARD	
CIRCUIT	**STANDARD**
1st Circuit	"owns and controls" and duty to notify opposing party of evidence in the hands of third parties[31]

[31] *In re* New Eng. Compounding Pharm., Inc., No. 13-cv-2419, 2013 U.S. Dist. LEXIS 161652 (D. Mass. Nov. 13, 2013) (Respondent recipients of Rule 45 subpoenas were required to produce responsive documents in their "possession custody or control," and "[t]o the extent that a respondent does not have responsive documents within its possession, custody, or control, it may simply state so."); Correia v. Town of Framingham, No. CIV. 12-10828-NMG, 2013 WL 952332, at *3 (D. Mass. Mar. 8, 2013) (defendant police officer was found to have "control" under Rule 34 over his employment personnel file in the possession of the state, because pursuant to state law he could obtain his personnel file upon demand, whereas information maintained in "other sorts of employee files . . . that are maintained separately from a 'personnel file'" were not under the officer's control); Bringuier v. AVCO Corp., No. CIV. 09-2140 ADC, 2011 WL 6372456, at *1 (D.P.R. Dec. 20, 2011) (defendant investment corporation did not have "right, authority, or ability to obtain [plane wreckage] upon demand" where it denied having possession, custody, or control over the wreckage and disclosed in correspondence with plaintiffs' counsel that the wreckage was in the possession, custody, and control of a claims supervisor under an insurance policy held by the owner of the aircraft—defendant was also insured by the same insurance carrier but under a different policy—and plaintiffs failed to rebut the assertion that defendant had no control); Rosie D. v. Romney, 256 F. Supp. 2d 115, 119 (D. Mass. 2003) (explaining that "control" under Rule 34 exists where a party has a "legal right to obtain documents," and "control" may be established by the existence of a principal–agent relationship or a legal right pursuant to a contractual provision and finding that defendant had the right to control and obtain the documents that were in the possession of various third party subcontractors because undisputed language in contracts with similar subcontractors allowed the defendant to examine and copy the same kind of documents at issue; and rejecting defendants' argument that plaintiffs should subpoena the third parties for the documents they seek).

LEGAL RIGHT PLUS NOTIFICATION STANDARD	
CIRCUIT	**STANDARD**
4th Circuit	“‘owns and controls’ and duty to notify opposing party of evidence in the hands of third parties”[32]
6th Circuit	“Even where a party does not own or control the evidence, the party still has a duty ‘to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence.’”[33]
10th Circuit	possession, but if relinquished ownership or custody, must contact new custodian to preserve[34]

PRACTICAL ABILITY STANDARD	
CIRCUIT	**STANDARD**
2nd Circuit	“right, authority or practical ability to obtain the documents at issue”[35]
4th Circuit	“right, authority or practical ability to obtain documents from non-party to the action”[36]

[32] Ayers v. Sheetz, Inc., No. 3:11-CV-00434, 2012 WL 5183561, at *2 (S.D.W. Va. Oct. 18, 2012).

[33] Lexington Ins. Co. v. Tubbs, No. 06–2847–STA, 2009 WL 1586862, at *3 (W.D. Tenn. June 3, 2009).

[34] Chavez v. Hatterman, No. CIV.A06-cv-02525-WYD-MEH, 2009 WL 807440, at *2 (D. Colo. Jan. 20, 2009).

[35] Alexander Interactive, Inc. v. Adorama, Inc., No. 12 CIV. 6608 PKC JCF, 2014 WL 61472, at *1 (S.D.N.Y. Jan. 6, 2014).

[36] Digital Vending Services International, Inc. v. The University of Phoenix, No. 2:09cv555, 2013 WL 311820, at *6 (E.D. Va. Oct. 3, 2013).

PRACTICAL ABILITY STANDARD	
CIRCUIT	**STANDARD**
8th Circuit	"right, authority or practical ability to obtain documents from non-party to the action"[37]
10th Circuit	"any right or ability to influence the person in whose possession the documents lie"[38]
11th Circuit	"practical ability to obtain the materials on demand"[39]
D.C. Circuit	"the right, authority or practical ability to obtain the documents from a non-party to the action"[40]

[37] New All. & Grain Co. v. Anderson Commodities, Inc., No. 8:12CV197, 2013 WL 1869832, at *3 (D. Neb. May 2, 2013) ("A party does not need to have legal ownership or actual possession of documents, 'rather documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action.'"); E*Trade Securities LLC v. Deutsche Bank AG, Civil No. 02-3711 RHK/AJB, 2005 U.S. Dist. LEXIS 3038, at *8 n.2 (D. Minn. Jan. 31, 2005) ("[C]ourts have sometimes interpreted Rule 34 to require production if the party has practical ability to obtain the documents from another, irrespective of his legal entitlement to the documents."); Prokosch v. Catalina Lighting, Inc., 193 F.R.D. 633, 636 (D. Minn. 2000) (quoting Bank of New York v. Meridien BIAO Bank Tanzania, Ltd., 171 F.R.D. 135, 146 (S.D.N.Y. 1997)).

[38] Tomlinson v. El Paso Corp., 245 F.R.D. 474, 477 (D. Colo. 2007); Ice Corp. v. Hamilton Sundstrand Corp., 245 F.R.D. 513, 521 (D. Kan. 2007).

[39] ANZ Advanced Techs. v. Bush Hog, LLC, No. CIV.A. 09-00228-KD-N, 2011 WL 814663, at *9 (S.D. Ala. Jan. 26, 2011) ("'[C]ontrol' has been 'construed broadly by the courts' to include not just a legal right, but also a 'practical ability to obtain the materials' on demand.").

[40] Bush v. Ruth's Chris Steak House, Inc., 286 F.R.D. 1, 5 (D.D.C. 2012) ("Control does not require that the party have legal ownership or actual physical possession of the documents at issue, but rather 'the right, authority or practical ability to obtain the documents from a non-party to the action.'").

The varying standards and the often inconsistent definition and application of these standards have left parties and courts with conflicting guidance to consider when making defensible discovery decisions.

C. A Deeper Look at the Practical Ability Standard Demonstrates that it Produces Potentially Unfair Results

Most courts applying the Practical Ability Standard rely on the following assumption: Rule 34 "control" does not require a party to have *legal ownership* or *actual physical possession* of any Documents and ESI at issue.[41] Instead, "documents are considered to be under a party's control when that party has the right, authority, or *practical ability* to obtain the documents from a non-party to the action."[42] Some courts have expanded the meaning of "practical ability" to mean the possibility that a party could potentially obtain the documents on demand.[43] In contrast, under the Legal Right Standard, the *possibility* of obtaining the Documents and ESI without the concomitant *legal right* to do so would be insufficient to establish Rule 34 "control."[44]

[41] *See, e.g.*, Golden Trade, S.r.L. v. Lee Apparel Co., 143 F.R.D. 514, 525 (S.D.N.Y. 1992) (The courts have "interpreted Rule 34 to require production if the party has the practical ability to obtain the documents from another, irrespective of his legal entitlement to the documents.").

[42] Goodman v. Praxair Servs., 632 F. Supp. 2d 494, 515 (D. Md. 2009) (quoting *In re* NTL, Inc. Secs. Litig., 244 F.R.D. 179, 195 (S.D.N.Y. 2007)).

[43] *See* Steele Software Sys. Corp. v. DataQuick Info. Sys. Inc., 237 F.R.D. 561 (D. Md. 2006) ("control has been construed broadly by the courts as the legal right, authority, or practical ability to obtain the materials sought on demand") (internal quotation omitted); S.E.C. v. Credit Bancorp, Ltd., 194 F.R.D. 469, 471 (S.D.N.Y. 2000) ("control" construed to include the "practical ability to obtain the materials sought upon demand").

[44] *See* Chaveriat v. Williams Pipe Line Co., 11 F.3d 1420, 1427 (7th Cir. 1993) (noting that even though a third party in possession of the documents likely would have provided the documents to plaintiffs upon plaintiffs' request, as this third party did at a later date, and that plaintiffs could have

Highlighted below are select areas where application of the Practical Ability Standard has led to unfair results.[45] We also note that the lack of a precise, commonly-accepted definition of "practical ability" results in an unfair lack of predictability with respect to how the Practical Ability Standard will be applied in a given case.

1. The Practical Ability Standard may Compromise the Ability of Parties with Cross-Border Operations to Comply with Their Legal Obligations, and Gives Short Shrift to Corporate Formalities of Legally Distinct Entities

Courts have applied the Practical Ability Standard to require parties with cross-border obligations to produce Documents and ESI from related entities with foreign operations, even when such production causes the entity to violate foreign data privacy laws. For example, one court ordered a domestic parent corporation to produce those documents it could obtain from its foreign subsidiary by 'picking up the telephone' or, in the alternative, to file an affidavit attesting to why it could not access those documents.[46] In this regard, the inequity of the Practical

purchased the documents, such factors did not establish control; and explaining that "the fact that a party could obtain a document if it tried hard enough and maybe if it didn't try hard at all does not mean that the document is in its possession, custody, or control; in fact it means the opposite").

[45] Our research has revealed 206 cases that have either applied or referenced the Rule 34 "practical ability" test. To download an easy-to-use, sortable spreadsheet of these cases, *see* The Sedona Conference, *"Compendium of Practical Ability Cases: A Resource for Understanding the Sedona Conference Commentary on Rule 34 and 45 Possession, Custody, or Control,"* THE SEDONA CONFERENCE (July 2016), https://s3.amazonaws.com/IGG/publications/Sedona+Practical+Ability+Cases+080516.xlsx.

[46] S2 Automation LLC v. Micron Tech., Inc., No. CIV 11-0884 JB/WDS, 2012 WL 3656454, at *12 (D.N.M. Aug. 9, 2012) ("It may be that S2

Ability Standard is perhaps felt most acutely by organizations that are subject to international privacy laws that operate to legally preclude discovery and/or movement of private data across the border and into the United States.[47] The consequences

Automation does not have the legal or practical right to obtain documents from S2 Israel. If that is the case, it must file an affidavit from a corporate official to that effect."). *See also In re* Ski Train Fire of Nov. 11, 2000 Kaprun Austria, No. MDL 1428(SAS)THK, 2006 WL 1328259, at *78 (S.D.N.Y. May 16, 2006) (applying Practical Ability Standard to hold parent company based in Germany must produce documents from wholly owned, non-party subsidiary company based in Austria: "Although the evidence demonstrates that Siemens [Germany] cannot legally compel Siemens Austria to produce its documents, there is evidence which strongly suggests that, as a practical matter, Siemens [Germany] can secure documents from Siemens Austria. . . . [Thus] the Court concludes that the only reasonable conclusion to draw is that if Siemens [Germany] needed the assistance or cooperation of Siemens Austria in a matter of concern to the company, it would receive such assistance, be it in the form of providing documents in Siemen's Austria's custody, or otherwise."); Orthoarm, Inc. v. Forestadent USA, Inc., No. 4:06-CV-730, 2007 WL 1796214, at *2 (E.D. Mo., June 19, 2007) (applying Practical Ability Standard, U.S. subsidiary ordered to produce documents from German parent because both companies had "interlocking management structures," and subsidiary had produced other parent documents without claiming no control, "thereby demonstrating the ability to obtain documents from the parent company upon request"). *But see,* Pitney Bowes, Inc. v. Kern Int'l., Inc., 239 F.R.D. 62 (D. Conn. 2006) (applying Practical Ability Standard but finding no control where plaintiff failed to offer evidence that the documents in the possession of defendant's foreign parent were necessary for the defendant's business or were routinely provided to it in the course of business and denying motion to compel).

[47] *See, e.g.*, *In re* Flag Telecom Holdings, Ltd. Sec. Litig., 236 F.R.D. 177, 181 (S.D.N.Y. 2006) (applying Practical Ability Standard to hold individual defendant was obligated to obtain documents from his former employer because he "is a senior executive of [his former employer], a former party [that is 'one of India's largest private sector enterprises' that had been dismissed with prejudice] to the litigation, and certainly has the practical ability to obtain the documents sought by plaintiffs' Request," and rejecting defendants' argument that plaintiffs themselves should seek production from the non-

party former employer located in India via the procedures set forth in the Hague Convention: "Mccormack is a party who has control over the corporation's documents irrespective of their location . . . therefore . . . plaintiffs are not required to proceed under the Hague Convention"); Ssangyong Corp. v. Vida Shoes Int'l, Inc., No. 03 CIV.5014 KMW DFE, 2004 WL 1125659, at *12–13 (S.D.N.Y. May 20, 2004) (applying Practical Ability Standard and ordering production of documents where New York branch of Hong Kong bank resisted subpoena of documents located in Hong Kong headquarters, court finds control and, as part of a comity analysis, observes that Hong Kong's interest in bank secrecy was not strong (the court characterized arguments that the bank faced the possibility of a Hong Kong injunction, a Hong Kong judgment for civil liability to accountholders, and potential criminal sanctions if it violated the injunction, as "quite remote on the facts of this case"), that "a strict confidentiality" order would reduce any hardship on the bank and its accountholders, that the documents sought via the subpoena were "very important" to the litigation, and that plaintiff who served subpoena had made a strong *prima facie* showing of bad faith by the accountholders (who may have participated in the fraud at issue in the underlying case)). *But see* Tiffany (NJ) LLC v. Qi Andrew, 276 F.R.D. 143, 151 (S.D.N.Y. 2011), *aff'd sub nom*. Tiffany (NJ) LLC v. Andrew, No. 10 CIV. 9471 WHP, 2011 WL 11562419 (S.D.N.Y. Nov. 14, 2011) (finding control where subpoenas were issued to New York branches of Chinese banks, despite the fact that branches were on separate computer systems from the Chinese offices that held the documents, but refusing to compel production pending exhaustion of Hague Convention based upon a comity analysis due to "true conflict" between United States and Chinese law (which prohibited production)); Tiffany (NJ) LLC v. Andrew, No. 10 CIV. 9471 RA HBP, 2012 WL 5451259, at *2 (S.D.N.Y. Nov. 7, 2012) (Following production of certain information from Chinese banks under the Hague Convention, the court subsequently declined to enforce the subpoena asking for production of additional information, noting "the centerpiece of plaintiffs' futility argument last year was . . . the People's Republic of China would either not respond at all to a request pursuant to the Hague Convention or would take an inordinate amount of time to do so. Experience has now proven both arguments to be unfounded."). *Accord In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d. 466, 472 (S.D.N.Y. 2014) (denying motion to quash search warrant directed to Microsoft to produce the contents of one of its customer's emails where that information is stored on a server located in Dublin, Ireland, reasoning that the Stored Communications Act, passed as for violating international laws can be severe.[48] Even so, the relatively broad discovery permitted by U.S. federal courts is in tension with international restrictions on data movement.[49]

Similarly, courts applying the Practical Ability Standard have given short shrift to corporate structures that apply to legally distinct entities.[50]

part of the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701–2712, does not implicate principles of extraterritoriality, and "it has long been the law that a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information," (citing Tiffany (NJ) LLC v. Qi Andrew, 276 F.R.D. 143, 147–48 (S.D.N.Y. 2011) ("If the party subpoenaed has the practical ability to obtain the documents, the actual physical location of the documents—even if overseas—is immaterial"))), *rev'd*, __ F.3d.___, No. 14-2985 (2nd Cir. July 14, 2016) (holding the Stored Communications Act "neither explicitly nor implicitly [] envisions the application of its Warrant provisions overseas," without reaching the issues of Rule 34 control, and rejecting the government's arguments to treat the SCA Warrant as equivalent to a subpoena and that "'similar to a subpoena, [an SCA warrant] require[es] the recipient to deliver records, physical objects, and other materials to the government' no matter where those documents are located, so long as they are subject to the recipient's custody or control," that relied upon "a collection of court rulings construing properly served subpoenas as imposing that broad obligation to produce without regard to a document's location").

[48] See The Sedona Conference, Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery, THE SEDONA CONFERENCE, at 20–22 (Aug. 2008), https://thesedonaconference.org/publications (describing criminal conviction for violation of French statute prohibiting disclosure of information required in foreign judicial proceedings).

[49] *Id.* at 23–26 (noting U.S. courts have held that they were not bound to use Hague Convention procedures over the Federal Rules of Civil Procedure).

[50] *See, e.g.*, *In re* Ski Train Fire of Nov. 11, 2000 Kaprun Austria, No. MDL 1428(SAS)THK, 2006 WL 1328259, at *1, 6 (S.D.N.Y. May 16, 2006) (After court dismissed Siemens Austria as a party to the case "because it has insufficient jurisdictional contacts with this District," court applied the Practical

However, courts in Legal Right Standard jurisdictions have given greater deference to international considerations, as well as corporate formalities that apply to legally distinct entities, especially when considering affiliate/"control" issues.[51] Toward

Ability Standard and held Siemens Germany—the parent company of Siemens Austria—must produce documents in the possession of Siemens Austria—even though the court did not have jurisdiction over Siemens Austria—because "the test for determining whether a corporate entity is the alter ego or a 'mere department' of another, are distinct from the issue of whether a parent has legal or practical access to its subsidiary's documents," and rejected defendant's argument that Siemens Germany and Siemens Austria are "distinct entities and that Siemens [Germany] does not have legal control over Siemens Austria," despite the court's prior findings when dismissing Siemens Austria "that the two companies do not operate as a single entity and that they observe all of the legal formalities of a distinct company."); Dietrich v. Bauer, No. 95 CIV. 7051 (RWS), 2000 WL 1171132, at *3 (S.D.N.Y. Aug. 16, 2000), *on reconsideration in part*, 198 F.R.D. 397 (S.D.N.Y. 2001) (Court finds Hague Convention procedures not required and New York branch of U.S. division was required to produce documents pursuant to Rule 45 subpoena in the possession of a branch of U.K. division, because parent company incorporated in Ireland exercised sufficient control over its wholly owned subsidiary, reasoning: "[c]ontrol has been construed broadly by the courts as the legal right, authority, or practical ability to obtain the materials sought upon demand. This Principle applies where discovery is sought from one corporation regarding materials which are in the physical possession of another, affiliated corporation." (internal quotation omitted); The court also rejected the argument that the "[c]ourt does not have personal jurisdiction over the corporate entity which has actual possession of the documents sought, namely, AIB Group (UK) . . . [because] personal jurisdiction and 'control' of documents are distinct issues in that court can compel discovery of documents in 'control' of a party although in 'possession' of person over whom there is no personal jurisdiction.").

[51] For example, in United States v. Deloitte & Touche USA LLP, 623 F. Supp. 2d 39, 41 (D.D.C. 2009), aff'd in part and vacated in part on other grounds, remanded sub nom. United States v. Deloitte LLP, 610 F.3d 129 (D.C. Cir. 2010), a civil tax refund case, the government moved to compel production of documents in response to a subpoena aimed at the opposing party's (Chemtech) auditing firm (Deloitte), even though the documents

this end, courts in Legal Right Standard jurisdictions have rejected the Practical Ability Standard, denying a motion to compel a U.S. corporation to produce documents in the possession of its German parent, explaining that ordering discovery from an entity beyond its jurisdiction would be "a futile gesture."[52] In rejecting the plaintiff's request to apply the Practical Ability Standard, that court also reasoned: "[c]ontrol must be firmly placed in reality, not in an esoteric concept such as 'inherent relationship.'"[53]

Likewise, one court in a Legal Right Standard jurisdiction specifically rejected a requesting party's suggestion to "go beyond 'corporate formalities'" via the application of the Practical Ability Standard to order a U.S. subsidiary to produce

were in the possession of the firm's so-called affiliate in Switzerland. The court rejected the government's argument that the auditing firm had sufficient control over its Swiss affiliate and denied the government's motion to compel. Though both Deloitte USA and Deloitte Switzerland were members of a Swiss verein, the government failed to establish that Deloitte U.S.A. had "the legal right, authority or ability to obtain the documents on demand" from Deloitte Switzerland/the affiliate. The court also rejected the government's argument to use the Practical Ability Standard and order production based upon the "close working relationship" in connection with Deloitte Switzerland's audit work for Chemtech, reasoning:

> [c]lose cooperation on a specific project does not, per se, establish an ability, let alone a legal right or authority, on Deloitte USA's part to acquire documents maintained solely by a legally distinct entity. In fact, upon Deloitte USA's request for the documents, Deloitte Switzerland refused to produce them absent an order from a Swiss court.

Id. (citations omitted).

[52] Ehrlich v. BMW of N. Am., LLC, No. CV 10-1151-ABC PJWX, 2011 WL 3489105, at *1 (C.D. Cal. May 2, 2011).

[53] *Id.* (citing U.S. v. Int'l Union of Petroleum and Indus. Workers, FFL-CIO, 870 F.2d 1450, 1453–54 (9th Cir. 1989)).

documents in the possession of its parent company, a Korean corporation with a principal place of business in Seoul, reasoning:

> the separate and distinct corporate identities of a parent and its subsidiary are not readily disregarded, except in rare circumstances justifying the application of the alter ego doctrine to pierce the corporate veil of the subsidiary.[54]

2. The Practical Ability Standard may Compel an Entity to Produce Documents and ESI in Violation of an Existing Contract

Courts in Practical Ability jurisdictions have ordered parties to produce documents even though that production would require the party to breach an existing contract with a non-party to the case that expressly prohibits the use of the non-party's documents for unauthorized purposes or disclosure. In this instance, the court reasoned that a discovery order requiring a party to violate the terms of its contractual agreement trumped "most other commitments."[55]

3. The Practical Ability Standard Often Fails to Recognize Distinctions between Separate Sister Corporations

Courts have applied the Practical Ability Standard to obligate sister corporations to obtain documents from each other when each has ties to a common parent corporation,

[54] Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc., 233 F.R.D. 143 (D. Del. 2005) (rejecting Practical Ability Standard and quashing subpoena to subsidiary seeking documents in possession of Korea-based parent corporation and noting that party seeking production could pursue a subpoena through Hague Convention procedures).

[55] S.E.C. v. Strauss, No. 09 CIV. 4150 RMB/HBP, 2009 WL 3459204, at *1 (S.D.N.Y. Oct. 28, 2009).

notwithstanding the fact that the entities may lack a sufficient relationship to warrant the imposition. Courts applying the Practical Ability Standard frequently bypass a thorough corporate veil analysis and order production of documents in the possession and custody of non-party sister entities. For example, one court relied on the Practical Ability Standard to order production of documents in the possession and custody of a non-party sister entity.[56] In that instance, the court did not consider or apply an "alter-ego" or veil-piercing analysis and, without discussion or analysis, simply concluded "as between the parties, Defendant has a 'practical ability' to obtain the information Plaintiffs seek on demand."[57] In contrast, courts that apply the Legal Right Standard analysis provide for a narrower scope of discovery among sister entities.[58]

[56] Wells v. FedEx Ground Package Sys., Inc., No. 4:10-CV-02080-JAR, 2012 WL 4513860, at *1 (E.D. Mo. Oct. 1, 2012).

[57] *Id.* at *4–5. *See also In re* Ski Train Fire of Nov. 11, 2000 Kaprun Austria, No. MDL 1428(SAS)THK, 2006 WL 1328259 (S.D.N.Y. May 16, 2006); Dietrich v. Bauer, No. 95 CIV. 7051 (RWS), 2000 WL 1171132, at *3 (S.D.N.Y. Aug. 16, 2000).

[58] For example, in *In re Citric Acid*, the court applied a Legal Right analysis and denied discovery of information in the possession and custody of a foreign co-member of an international accounting organization. *In re* Citric Acid Litig., 191 F.3d 1090 (9th Cir. 1999). Similarly, in a civil tax refund case, the court denied the government's motion to compel the production of documents in the possession and custody of the party's Swiss affiliate because it was not clear that the party had the legal right, authority, or ability to demand and obtain the documents. United States v. Deloitte & Touche USA LLP, 623 F. Supp. 2d 39 (D.D.C. 2009). *Cf. also*, Ehrlich v. BMW of N. Am., LLC, No. CV 10-1151-ABC PJWX, 2011 WL 3489105, at *1 (C.D. Cal. May 2, 2011); Gerling Int'l Ins. Co. v. C.I.R., 839 F.2d 131, 140 (3d Cir. 1988) (The two corporate entities at issue had a common president who also was the chairman of the board of directors of one of the corporations (Universale) and a minority stockholder in the other (GIIS). The court declined to find that GIIS had sufficient control over Universale to require production of its books and records: "Where the litigating corporation is the subsidiary and the parent

Other courts have combined the Practical Ability Standard and the Legal Right Standard with elements of a veil-piercing analysis to reach a more equitable determination of whether Rule 34 "control" existed concerning discovery sought from related sister entities.[59]

possesses the records, control has been found to exist where the "alter ego" doctrine warranted piercing the corporate veil. . . . The few cases involving sister corporations under common control follow the same pattern as the cases involving a litigating subsidiary. The requisite control has been found only where the sister corporation was found to be the alter ego of the litigating entity. In this case, the Tax Court seems to have regarded GIIC and Universale as sister corporations under common control. It did so, however, only on the basis of an improper presumption that Gerling controlled Universale and a tacit assumption that Gerling controlled GIIC despite his minority stockholder status. Moreover, even if these corporations had been properly presumed or assumed to be under common control, there was no finding, and no record to support a finding, that their corporate entities had been disregarded by themselves or Gerling in the course of their businesses or that GIIC had acted for the benefit of Universale either in the transactions giving rise to the alleged tax liability or in conducting this litigation. In such circumstances, we conclude that there was no foundation for the Tax Court's conclusion that GIIC had sufficient control over Universale to require production of its books and records in the United States." *Id*. at 141–42.)

[59] *See, e.g.*, Handi-Craft Co. v. Action Trading, S.A., No. 4:02 CV 1731 LMB, 2003 WL 26098543 (E.D. Mo. Nov. 25, 2003) (ordered discovery after considering commonality of ownership, intermingling of directors, officers, employees, documents exchanged in the normal course of business and the involvement of non-party entity in the litigation). *See also* Uniden Am. Corp. v. Ericsson Inc., 181 F.R.D. 302, 305–07 (M.D.N.C. 1998) (ordering party to produce documents in custody of non-party sister corporation after applying "control" factors and noting that to determine Rule 34 control, courts consider (i) "legal right" to obtain documents; (ii) "actual ability" to obtain documents; (iii) existence of "alter ego" relationship; (iv) amount of parent's ownership in subsidiary and control factors, including (a) commonality of ownership, (b) exchange or intermingling of directors, officers, or employees of the two corporations, (c) exchange of documents between the corporations in the ordinary course of business, (d) any benefit or involvement by the non-party corporation in the transaction, and (e) involvement of the non-party

Additionally, in certain cases construing the relationship among a corporate family for purposes of adjudicating Rule 34 "control," the court's decision has turned on whether a party had access for business purposes to documents in the possession and custody of a corporate sister. For example, one court denied discovery sought from a non-party sister entity because the party upon whom discovery was propounded did not have access to the information in the normal course of business.[60]

4. The Practical Ability Standard may Compel Individuals to Produce Documents and ESI in the Possession of Companies they Own but that are not Parties to a Case

Ownership in a company, regardless of the percentage of ownership or involvement in that company's day-to-day business, has been found to be sufficient to establish a "practical ability" to obtain Documents and ESI from the company, even where the company is not a party to the case. For example, courts have applied the Practical Ability Standard to order individuals to obtain and produce information in the possession and custody of non-party companies where the individuals are partial owners. In one case, the court compelled production from a joint-venture ("JV") entity of which the individual owned 49% on the basis of contract, and based upon testimony that the JV

corporation in the litigation. The court stated that Rule 34 control for discovery among members of corporate families is broader than "control" for the purpose of determining liability); E.I. DuPont de Nemours & Co. v. Kolon Indus., Inc., 286 F.R.D. 288 (E.D. Va. 2012) (construing Rule 34 control based in part on assessment of corporate veil factors); *cf.* Doe Run Peru S.R.L. v. Trafigura AG, No. 3:11mc77, 2011 U.S. Dist. LEXIS 154559 (D. Conn. Aug. 23, 2011) (denying discovery because affiliate relationship and arms-length transactions failed to establish practical ability to obtain documents).

[60] *See, e.g.,* S.E.C. v. Credit Bancorp, Ltd., 194 F.R.D. 469 (S.D.N.Y. 2000) (denying discovery request because party did not have regular business access to information in possession and custody of non-party sister entity).

entity had provided documents upon request 90% of the time.[61] Likewise, another court cited the Second Circuit's broad standard of "control" and ordered an individual to obtain and produce documents in the possession and custody of a subsidiary in which the individual was a 50% owner.[62] Courts applying the Legal Right Standard to similar factual scenarios reached the opposite conclusion.[63]

5. The Practical Ability Standard may Compel Corporate Parties to Produce Documents and ESI in the Possession of Former or Current Employees or Employers even if the Employers have no Legal Right to Demand or Obtain such Documents and ESI

Courts have applied the Practical Ability Standard to find that employers have Rule 34 "control" over documents in the possession of former employees. For example, a court ordered defendants, including former corporate officers and directors, to produce documents in the possession of the former corporate secretary, even though the former secretary had not worked for

[61] Kamatani v. Benq Corp., No. CIV.A. 2:03-CV-437, 2005 WL 2455825, at *1 (E.D. Tex. Oct. 4, 2005).

[62] Am. Rock Salt Co. v. Norfolk S. Corp., 228 F.R.D. 426 (W.D.N.Y. 2005), *objection denied by, stay denied by*, 371 F. Supp. 2d 358 (W.D.N.Y. 2005).

[63] Noaimi v. Zaid, 283 F.R.D. 639 (D. Kan. 2012) (denying a discovery request seeking corporate documents in the possession and custody of a corporation because the individual's 20% ownership interest failed to establish 'control' under the Legal Right Standard applied in Kansas); Am. Maplan Corp. v. Heilmayr, 203 F.R.D. 499 (D. Kan. 2001) (reversing magistrate judge's grant of motion to compel defendant to produce corporate documents in the possession of a third-party corporation for which defendant was president and a minority shareholder, finding that although defendant might have the practical ability to obtain the documents he did not have legal authority and the third party retained the right to confidentiality of the documents sought).

the defendants in five years, and to submit an affidavit detailing their efforts.[64] However, applying a Legal Right Standard, at least one court reached the opposite conclusion and denied a motion to compel production of documents in the possession and custody of non-party former directors.[65] Likewise, a court applying a Legal Right Standard denied plaintiffs' Motion to Compel text messages sent or received by a corporate-defendant's employees' personal cell phones because the corporate defendant did not issue the cell phones to the employees, the employees did not use the cell phones for any work-related purpose, and the corporate-defendant otherwise did not have any legal right to obtain employee text messages on demand.[66] Moreover, while no court has squarely held that the Practical Ability Standard can compel corporate parties to produce documents and ESI in the possession of current employees, the Practical Ability Standard could arguably put employers in the awkward position of asking for the personal documents and ESI

[64] Scovin v. Great W. Life & Annuity Ins. Co., No. 3:02CV1161, 2006 U.S. Dist. LEXIS 71386 (D. Conn. Sept. 29, 2006). *See also In re* Folding Carton Antitrust Litig., 76 F.R.D. 420, 423 (N.D. Ill. 1977) (suggesting that an employer may have control over documents in the possession of a former employee if that individual is still receiving economic benefits from the employer).

[65] Miniace v. Pac. Maritime Ass'n, No. C 04-03506 SI. 2006 WL 335389 (N.D. Cal. Feb. 13, 2006) (applying Legal Right Standard and, on that basis, denying production of documents in custody of former directors). *Accord In re* Lululemon Athletica Inc., 220 Litig., No. CV-9039-VCP, 2015 WL 1957196, at *4–7 (Del. Ch. Apr. 30, 2015) (finding it unwarranted to search the personal email accounts of a company's non-employee directors for documents responsive to discovery requests).

[66] Cotton v. Costco Wholesale Corp., No. 12-2731-JW, 2013 WL 3819974, at *1 (D. Kan. July 24, 2013); *see also* Matthew Enter., Inc. v. Chrysler Grp. LLC, No. 12-cv-04236, 2015 WL 8482256 (N.D. Cal. Dec. 10, 2015) (applying the Legal Right Standard, denying motion filed against corporate party to compel production from employees' personal email accounts).

of their employees (and former employee) which may be deemed improper or "coercive."[67]

In some instances, former employees have been found to have the practical ability to obtain documents in the possession of their former employer, or an entity over which they used to exercise some degree of control, even though the former employer/entity was not a party to the case. For example, a defendant/former senior executive was ordered to produce documents in the possession of his former employer, even though the employee handbook stated that such documents were the employer's property and employees could not take documents home unless necessary for work.[68] The court found that employees were permitted to utilize documents, thus, the defendant, as a senior officer, had the practical ability to obtain them. Yet, even where courts have applied the Practical Ability Standard in this context, they have reached inconsistent results.[69] In contrast, some courts applying the Legal Right Standard have found that

[67] *See, e.g.*, Debbie Kaminer, *Can Employers Ask Applicants for Social Media Login Information,* N.Y.L.J. (July 27, 2012), http://www.newyorklawjournal.com/id=1202564023558/Can-Employers-Ask-Workers-Applicants-for-Social-Media-Login-Information?slreturn=20160428100635.

[68] *In re* Flag Telecom Holding, Ltd. Sec. Litig., 236 F.R.D. 177 (S.D.N.Y. 2006).

[69] *Cf*. Diaz v. Washington State Migrant Council, 165 Wash. App. 59, 265 P.3d 956 (2011) (reversing contempt finding and applying federal Practical Ability Test, court finds that corporate director had no duty to make personal records regarding immigration status available to the corporation he or she serves, and there had been no showing that defendant non-profit had practical ability to secure personal records belonging to its directors); Piazza's Seafood World, L.L.C. v. Odom, No. CIV.A. 07-413-BAJ-CN, 2011 WL 3664437 (M.D. La. Aug. 19, 2011) (noting Practical Ability Standard, court found that as an ex-commissioner of a state agency, the defendant no longer had custody or control of the documents in the possession of the agency).

former employees did not have Rule 34 "control" over documents in the possession of their former employer.[70]

Under the Practical Ability Standard, current employees sometimes have been found to have the practical ability to obtain documents in the possession of their employer, even where the employer is not a party to the case. For example, a defendant was ordered to produce his personnel file, which was in the possession of his current employer, and placed the burden on him to demonstrate that he had no control over the documents.[71] The court reasoned that as a high-ranking officer and director, defendant failed to present evidence that he lacked the practical ability to produce documents in his own personnel file. Likewise, a defendant corrections officer was ordered to produce prior and subsequent excessive force complaints by prison inmates against the corrections officer contained in his employer's (the N.Y. Department of Correctional and Community Services, "DCCS") files, despite the fact that the defendant's lawyer "engaged, unsuccessfully, in extensive communications with DCCS concerning Plaintiff's requests to obtain the requested documents, and DCCS is unable to accommodate Plaintiff's requests."[72] In reaching that result, the court canvassed other cases that had applied the Practical Ability Standard and noted those courts had looked at factors like:

- "a degree of close coordination";

[70] Lopez v. Chertoff, No. CV 07–1566–LEW, 2009 WL 1575214 (E.D. Cal. June 2, 2009) (under Legal Right analysis, former employee of public defender's office did not have Rule 34 control over documents in possession of her former employer); Lowe v. D.C., 250 F.R.D. 36, 38 (D.D.C. 2008) (court did not invoke either Practical Ability or Legal Right Standards but stated "[f]ormer employees of government agencies do not have 'possession, custody, or control' of documents held by their former employers").

[71] *In re* Teligent, Inc., 358 B.R. 45 (Bankr. S.D.N.Y. 2006).

[72] Gross v. Lunduski, 304 F.R.D. 136 (W.D.N.Y. 2014).

- "similar interests, missions or goals";
- "interests are sufficiently aligned and closely interrelated"; and
- a "sufficient nexus."[73]

6. The Practical Ability Standard may Compel Service Providers to Produce Information Owned by Clients and Customers even if the Service Provider has no Legal Right to Demand or Obtain such Documents and ESI

Courts have applied the Practical Ability Standard to trump the absence of a party's legal right to control documents by imposing on parties who provide services a duty to preserve and produce documents stored on their client's servers. For example, in an employment matter, plaintiffs sued their employer, Accenture, for age discrimination.[74] While employed by Accenture, plaintiffs performed Information Technology (IT) work for Accenture's client, Best Buy, and were provided bestbuy.com email accounts during the service period. Plaintiffs moved to compel discovery of emails sent by Accenture employees through Best Buy's email server with bestbuy.com email addresses. Accenture objected on the ground that the emails were stored on Best Buy's servers and were contractually owned by Best Buy—which was not a party in the case. The court found these facts irrelevant for purposes of applying the Practical Ability Test, reasoning: "[i]f an Accenture employee with a bestbuy.com email address can access information sent from or received by his or her bestbuy.com email address within his or her

[73] *Id.*

[74] Hageman v. Accenture, LLP, No. CIV. 10-1759 RHK/TNL, 2011 WL 8993423 (D. Minn. Oct. 19, 2011).

normal day-to-day work, then that information is within Accenture's control."[75]

Several other courts applying the Practical Ability Standard have found that similar obligations exist between service providers and their customers.[76] Courts have also used a "relationship" standard to determine Rule 34 "control" as between entities that conduct business with one another but otherwise have

[75] The *Hageman* court did issue one caveat, denying plaintiffs' motion with respect to information stored on Best Buy's server to the extent it was "inaccessible to Accenture employees within their normal day-to-day activity[]," explaining that:

> [t]he fact that Accenture employees used bestbuy.com email addresses does not make information that is no longer accessible [to] [*sic*] those Accenture employees within Accenture's possession, custody, and control merely because the information may be stored or archived on the bestbuy.com server. The contract between Accenture and Best Buy does not state that Accenture can freely access the bestbuy.com server or has a contractual right to obtain information on the bestbuy.com server upon request. Rule 45 is the proper vehicle for Plaintiff to obtain information from the bestbuy.com server that cannot be accessed by an Accenture employee within his or her normal day-to-day activity.

Id. at *4.

[76] *See* Chevron Corp. v. Salazar, 275 F.R.D. 437, 451 (S.D.N.Y. 2011) (lead counsel had "practical ability" to obtain and produce email from other professionally affiliated law firms and individuals in response to subpoena); Ice Corp. v. Hamilton Sundstrand Corp., 245 F.R.D. 513 (D. Kan. 2007), *objection overruled by, motion to strike denied by,* No. 05-4135-JAR, 2007 WL 3026641 (D. Kan. Oct. 12, 2007) (granting plaintiff's motion to compel where court found that based on the master service agreement between defendants and contractors, defendants had sufficient control and practical ability to obtain the documents); Chicago Ins. Co. v. Wiggins, No. 02-73801, 2005 U.S. Dist. LEXIS 27159 (E.D. Mich. Aug. 12, 2005) (plaintiff had practical ability to demand materials that third parties used to train plaintiff's employees).

no corporate or legal relationship.[77] Yet, some courts applying the Practical Ability Standard have taken a more nuanced approach—again reinforcing the inconsistent application of this standard—moving away from outright sanctioning the producing parties even where the court found the party had "control." In these cases, the courts have instead compelled the producing party to make efforts to obtain the requested documents from non-parties and to document their efforts to obtain the information with the court, or face the possibility of sanctions.[78] One court found the contractual relationship between the defendant and its subcontractor satisfied "control" under Rule 34, but ruled that the defendant could either produce any responsive documents in the subcontractor's possession or provide the requesting party with an affidavit detailing its efforts to obtain the documents.[79]

[77] *See* R.F.M.A.S., Inc., v. So, 271 F.R.D. 13, 24 (S.D.N.Y. 2010) (relationship between jewelry designer and her manufacturer sufficient to establish Rule 34 control, stating "[e]vidence in a party's 'control' has been interpreted to mean evidence that the party has the legal right, authority or practical ability to obtain by virtue of its relationship with the party in possession of the evidence").

[78] Sekisui Am. Corp. v. Hart, No. 12 CIV. 3479 SAS FM, 2013 WL 2951924 (S.D.N.Y. June 10, 2013) (despite notifying Defendants of its intent to seek damages in October 2010, Plaintiff's failure to implement litigation hold until January 2012 and failure to notify the outside vendor managing its computer operations that it needed to preserve relevant electronically stored information until nearly three months after the suit was filed was held to constitute negligent spoliation).

[79] Sedona Corp. v. Open Sols., Inc., 249 F.R.D. 19 (D. Conn. 2008). *See also* Cummings v. Moran Shipping Agencies, Inc., No. 3:09CV1393 RNC, 2012 WL 996883 (D. Conn. Mar. 23, 2012) (ordering plaintiff to make efforts to obtain the requested documents not in his possession and if unable to do so, to file an affidavit detailing his efforts); *In re* Vitamin C Antitrust Litig., No. 06-MD-1738, 05-CV-0453, 2012 U.S. Dist. LEXIS 166720 (E.D.N.Y. Nov. 19, 2012) (plaintiff failed to meet burden to demonstrate practical ability to obtain documents where defendant denied possession, custody, or control and

Service provider cases in Legal Right Standard jurisdictions result in more consistent and arguably more equitable outcomes. In one case the court denied defendant's motion to compel production of documents used by and in the possession of its independent claims adjustor.[80] The court reasoned that the appropriate vehicle to obtain these documents was via a Rule 45 subpoena.[81]

plaintiffs failed to show that, for example, defendant's independent auditing firm would turn over the documents to defendant upon defendant's request; but court directed defendant to make such a request and reminded plaintiffs that they should have sought the documents directly from the audit firm "years ago when discovery was ongoing"); Fisher v. Fisher, No. CIV. WDQ-11-1038, 2012 WL 2050785 (D. Md. June 5, 2012) (as bank account holder, defendant found to have practical ability to obtain bank records, but applying the Rule 26(b)(2)(C) proportionality test, court directed plaintiff to subpoena the financial institutions, except to the extent it would be less expensive for defendant to obtain and produce these documents).

[80] Bleecker v. Standard Fire Ins. Co., 130 F. Supp. 2d 726 (E.D.N.C. 2000).

[81] *See also,* Haskins v. First Am. Title Ins. Co., No. CIV. 10-5044 RMB/JS, 2012 WL 5183908 (D.N.J. Oct. 18, 2012) (in class action in Legal Right jurisdiction, defendant Title Insurance Company ordered to serve litigation hold notice on its third-party agents to preserve the third-party agents' closing files, where contracts between the Title Insurance Company and each of the third-party agents expressly required agent to maintain and preserve documents and make them available to defendant for inspection and copying on demand at any time; order carved out any agreements that did not contain similar language); Inline Connection Corp. v. AOL Time Warner, Inc., No. C A 02-272-MPT, 2006 WL 2864586 (D. Del. Oct. 5, 2006) (finding no legal right of defendants to obtain documents in the possession of third-party telephone companies).

7. Effect of "Control" Issues on Third-Party Discovery

The application of the Practical Ability Standard may also unduly increase the burden of parties by requiring them to obtain documents from non-parties.[82]

However, in *Lynn v. Monarch Recovery Management, Inc.*, the court recognized that even under a practical ability analysis, Rule (26)(b)(2)(C) considerations of proportionality, including burden, expense, and convenience made a Rule 45 subpoena the appropriate vehicle through which a party should seek documents from a non-party when the producing party did not have possession or custody of billing information of its telephone provider.[83]

[82] Chevron Corp. v. Salazar, 275 F.R.D. 437 (S.D.N.Y. 2011) (lead counsel waived privilege in related matter and was compelled to produce documents from co-counsel because it had the practical ability to obtain the documents); S.E.C. v. Strauss, No. 09 CIV. 4150 RMB/HBP, 2009 WL 3459204 (S.D.N.Y. Oct. 28, 2009) (discovery obligations trump "most other commitments"; practical ability means access); Bleecker v. Standard Fire Ins. Co., 130 F. Supp. 2d 726 (E.D.N.C. 2000) (court rejected application of Practical Ability Test to compel party to produce documents in possession and custody of third party and explained that "ability to obtain" test would usurp principles of Federal Rules of Civil Procedure by permitting parties to obtain documents from non-parties who were not subject to the control of any party to the litigation).

[83] Lynn v. Monarch Recovery Management, Inc., 285 F.R.D. 350, 361 (D. Md. 2012):

> Rule 34 requires a party to produce only those documents that are within the party's "possession, custody, or control." Fed. R. Civ. P. 34(a)(1). "Rule 34 'control' does not require a party to have legal ownership or actual physical possession of any [of the] documents at issue." *Goodman v. Praxair Servs., Inc.*, 632 F. Supp. 2d 494, 515 (D. Md. 2009) (citation omitted). Instead, "documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party." *Id.* (citation and internal quotation marks omitted); *Steele Software Sys., Corp. v. DataQuick Info. Sys., Inc.*, 237 F.R.D. 561, 563–65 (D. Md. 2006).

Another recent case[84] also suggests that even though a party may have the "practical ability" to obtain documents from a non-party, a Rule 45 subpoena was the appropriate discovery device for collecting the documents since they were not under the producing party's physical control.

In those cases, the court determined that proportionality of the costs and burdens associated with discovery were so great that a Rule 45 subpoena was the correct method of extracting such discovery. *Lynn* and *Fisher* thus indicate that physical control over documents should be the dispositive factor in determining the appropriate procedural discovery device.

> Because Defendant has an account with the telephone carrier, Defendant likely has "the right, authority, or practical ability" to obtain an itemized telephone bill from the carrier, and may be compelled to do so. *See Goodman*, 632 F.Supp.2d at 515. However, Fed. R. Civ. P. 26(b)(2)(C) instructs the Court to "limit the frequency or extent of discovery otherwise allowed" if, *inter alia*, "the discovery sought . . . can be obtained from some other source that is more convenient, less burdensome, or less expensive." In light of the foregoing, the parties are DIRECTED as follows: If there are any additional documents not previously produced "identifying any calls to Plaintiff or 301-620-2250" in Defendant's actual possession or custody, Defendant must produce them, subject to the parties' stipulated confidentiality order, if Defendant contends that they contain confidential information. *See* Fed. R. Civ. P. 34(a)(1). If documents responsive to this request are not in Defendant's possession or custody, but are in the physical custody of a non-party telephone carrier, Defendant will not be compelled to produce them. *See* Fed. R. Civ. P. 26(b)(2)(C)(i). Rather, Plaintiff may obtain the documents by issuing a Fed. R. Civ. P. 45 subpoena to the telephone carrier.

[84] Fisher v. Fisher, No. CIV. WDQ–11–1038, 2012 WL 2050785 (D. Md. June 5, 2012).

D. *How new Technologies may Influence the Rule 34 Possession, Custody, or Control Analysis*

New technologies and organizational initiatives can further blur the lines of who actually "controls" Documents and ESI for purposes of preservation and production. They also complicate the practical problems associated with preserving and producing Documents and ESI that a party does not directly control.[85]

1. Cloud Computing

For purposes of this Commentary, we will refer to "cloud computing" simply as the use of a remote device or network to store, manage, preserve, or backup any of a party's rightfully owned data or software.[86] In this context, there are two major

[85] The drafters of the 2015 federal rule amendments specifically took note of how new technologies were impacting litigation:

> Significant amounts of ESI will be created and stored not only by sophisticated entities with large IT departments, but also by unsophisticated persons whose lives are recorded on their phones, tablets, cars, social media pages, and tools not even presently foreseen. Most of this information will be stored somewhere on remote servers, often referred to as the "cloud," complicating the preservation task.

See Advisory Committee Report, *supra* note 5.

[86] A more technical and thorough definition of Cloud Computing has been published by the National Institute of Standards and Technology:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

issues with cloud computing: (1) the location of the data, and (2) who is managing the data (be it one's own company or a third party). The increasingly widespread use of cloud computing services to store information raises questions with respect to the ownership of the information, the right and ability to control the information, and the disposition of the information at the expiration of the cloud computing service contract. Frequently, businesses make decisions to use cloud computing resources on the basis of business judgments, in order to fulfill business needs, improve efficiencies, and reduce costs. However, when a contract is made with cloud providers, there is often little or no ability to effectively negotiate terms with the cloud provider because the provider only accepts standardized agreements.

Multi-tenancy issues: Cloud computing environments may use operating system tools to host the business applications and data of more than one client in the same physical or logical computing environment, which is referred to as "Multi-tenancy" or "Split-tenancy." Further, multi-tenant computing environments may also store together ("commingle") the data of multiple clients in the same logical area of computer memory or on the same physical storage device.

Since this data is commingled, it is more difficult to show which data is owned by whom. Unlike a simple index used to track boxes stored in a warehouse, multi-tenancy computing environments may require an understanding of how a computing environment uses metadata to track, manage, and maintain logical distinctions among commingled data to comply with legal obligations to access, preserve, collect, and understand commingled data.

Peter Mell and Tim Grance, *The NIST Definition of Cloud Computing (Draft)* (Jan. 2011), http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf.

Location/Jurisdiction issues: Data stored "in the cloud" may also reside in more than one physical location which raises issues about the body of law applicable to such data, thereby posing additional preservation and collection challenges, especially since data sets may either be split into multiple locations or redundant storage locations.

Importantly, the third-party vendor's data retention policies and data preservation protocols may differ from or conflict with those of the data owner. Third-party vendors may also be subject to different statutory obligations on the basis of the jurisdiction in which they operate. To the extent such inconsistencies arise, data owners may face additional compliance issues and litigation risk and expense when extracting data. They also may find that they have conflict of law issues when attempting to recover their own data.

Privacy and security issues: Data stored in the cloud may be accessible by a greater number of people, including the cloud vendor's employees. Moreover, when data is held by a cloud provider, there is a risk that it can be sought directly from the cloud provider—in some instances without notice to the customer.[87]

The issues of who has possession, custody, or control in this age of electronic information is complicated by cost, burden, access, privacy, and contractual issues that simply did not exist in

[87] *See* Catherine Dunn, *Microsoft Reveals Law Enforcement Requests for Customer Data,* LAW TECHNOLOGY NEWS (March 26, 2013), http://www.corpcounsel.com/id=1202593423164/Microsoft-Reveals-LawEnforcement-Requests-for-Customer-Data ("In general, we believe that law enforcement requests for information from an enterprise customer are best directed to that customer rather than a tech company that happens to host that customer's data," [Microsoft General Counsel Brad] Smith said. "That way, the customer's legal department can engage directly with law enforcement personnel to address the issue.").

a world populated only by hardcopy documents. In short, unique issues of location, access, and multi-tenancy make cloud computing quite different than boxes of paper files stored in a depository.

2. Social Media

Social Media sites have complex possession, custody, and control issues because there is often a commingling of interests and sources as it pertains to speech and data communicated and collected on these sites. This information is generally in the custody of the third-party company which hosts the social media platform. But courts commonly require production of social media data and information from both individual[88] and corporate sources. There is no question that individuals and corporations have control over the data which is created on these social media sites; however, they do not host this data and do not have physical possession of this data.

[88] *See, e.g.*, Quagliarello v. Dewees, No. CIV.A. 09-4870, 2011 WL 3438090 (E.D. Pa. Aug. 4, 2011) (plaintiff's social media relevant to rebut emotional distress claims); E.E.O.C. v. Simply Storage Mgmt, LLC, 270 F.R.D. 430, 436 (S.D. Ind. 2010) (rejecting EEOC's claim that producing social networking content would infringe on claimants' privacy because merely locking a profile from public access does not prevent discovery and ordering EEOC to produce "any profiles, postings, or messages (including status updates, wall comments, causes joined, groups joined, activity stream, blog entries)," third-party communications, photographs, and videos for the claimants that "reveal, refer, or relate to any emotion, feeling, or mental state, as well as communications that reveal, refer, or relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state"; and instructing that in accordance with the liberal discovery standard of Rule 26, in carrying out the court's order "the EEOC should err in favor of production"); Ledbetter v. Wal-Mart Stores, Inc., No. 06-CV-01958-WYDMJW, 2009 WL 1067018 (D. Colo. Apr. 21, 2009) (court ordered plaintiffs to produce email and other communications from Facebook, MySpace, and Meetup.com).

When information regarding a social media account is requested by a party in litigation or an investigation, it is the duty of the custodian to produce a valid copy of the data available. There are tools that can assist in the download of this data, but in many cases a complete set of data can only be recovered with the consent or cooperation of the "owner" of the data.

Corporations do not own or control their employees' personal social media accounts. There have been instances where employees' personal accounts contained information or speech relevant or desired as evidence by a corporation. While some have attempted to argue that under the Practical Ability Standard, corporations may have the "practical ability" to obtain data from social media sites they do not own or control merely by asking their employees to preserve/produce it, no court has specifically held this to be true. To the contrary, as noted above, an employer's demand for this information from an employee may be viewed as improper or "coercive."[89] Likewise, many states have enacted legislation that specifically prohibit an employer from seeking such information from an employee, and an employer's attempt to solicit an employee's usernames and passwords to facilitate a social media capture may violate those states' privacy statutes.[90]

[89] *See, e.g.*, Debbie Kaminer, *Can Employers Ask Applicants for Social Media Login Information,* N.Y.L.J. (July 27, 2012), http://www.newyorklawjournal.com/id=1202564023558/Can-Employers-Ask-Workers-Applicants-for-Social-Media-Login-Information?slreturn=20160428100635.

[90] See, e.g.:

- Philip L. Gordon & Joon Hwang, *Making Sense of the Complex Patchwork Created by Nearly One Dozen New Social Media Password Protection Laws*, LITTLER (July 2, 2013), http://www.littler.com/making-sense-complex-patchwork-created-nearly-one-dozen-new-social-media-password-protection-laws ("In a single season, spring 2013, seven states enacted social media password protection legislation, bringing the total number of states to 11 since Maryland enacted

Employers also need to be aware of restrictions on policies they issue concerning employees' use of social media, as they may conflict with federal or state regulations.[91]

3. The "Bring your Own Device to Work" Movement[92]

"BYOD," or Bring Your Own Device is an increasingly popular corporate practice where employees purchase and own the physical hardware device (i.e., a smartphone or tablet) that then

the first such law in May 2012. Bills are pending in more than 20 other states. The current roster of states, dominated by the Rocky Mountain Region and the Far West, is as follows: Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Mexico, Oregon, Utah and Washington. New Jersey appears poised to join this group as the state's legislature amends a bill conditionally vetoed by Governor Christie in May."); *and*

- Philip Gordon & Joon Hwang, *New Jersey Becomes the Twelfth State to Enact Social Media Password Protection Legislation*, LITTLER (Sept. 1, 2012), http://www.littler.com/new-jersey-becomes-twelfth-state-enact-social-media-password-protection-legislation-recent-amendment ("On August 29, 2013, New Jersey became the twelfth state to enact social media password protection legislation, continuing the nationwide trend towards imposing some form of restriction on employer access to the restricted, personal social media content of applicants and employees. The new law becomes effective on December 1, 2013.").

[91] *See, e.g.*, *NLRB's Acting General Counsel Issues Third Guidance Document on Social Media and Approves One Policy*, LITTLER (June 5, 2012), http://www.littler.com/publication-press/publication/nlrbs-acting-general-counsel-issues-third-guidance-document-social-0 (noting that policy provisions that, among other things, required employees to protect confidentiality, prohibited inappropriate postings, encouraged employees to be respectful, fair, and courteous, and addressed the friending of co-workers, could potentially violate the National Labor Relations Act).

[92] The Sedona Conference is preparing a more detailed commentary on BYOD issues that will be available on its website once it is released for public comment.

is connected to a corporate network system or otherwise used to conduct the company's business. There are a myriad of issues that are created via BYOD initiatives.[93] As a general matter, an employer does not have "control" over or the right to access personal information and data stored on home or personal computers, personal email accounts, personal PDAs, etc., of its employees. Thus, if an adversary demands such information in discovery, an employer can legitimately object. Yet, if an employer has a BYOD program, and has the ability to access employees' personal devices for work data, the lines concerning personal data and responsibility become blurred.

Likewise, the reality is that an employee may constructively and realistically have both custody and control over a BYOD device. Although the device may hold enterprise "owned" information, the employee both owns and accesses the data. Without the employee's consent,[94] an employer is not likely to have the legal right to both secure control and custody of the device, much less preserve information on the same device.[95]

[93] For a thorough discussion of BYOD issues, *see The "Bring Your Own Device" to Work Movement: Engineering Practical Employment and Labor Law Compliance Solutions*, THE LITTLER REPORT (May 2012), http://www.littler.com/files/press/pdf/TheLittlerReport-TheBringYourOwnDeviceToWorkMovement.pdf.

[94] At least one court has held that an employer's ability to secure consent from its employees can only go so far. *See* Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 325, 990 A.2d 650, 665 (2010) (rejecting employer's claim to access employee's attorney-client communications "[b]ecause of the important public policy concerns underlying the attorney-client privilege").

[95] *See, e.g.*, Matthew Enterprise, Inc. v. Chrysler Grp. LLC, No. 13-cv-04236-BLF, 2015 WL 8482256 (N.D. Cal. Dec. 10, 2015) (employee's phone was not in Rule 34 possession, custody, or control of employer).

4. Changing Locations/Jurisdictions

In the hard copy age, attorneys and clients could definitively determine the location of documents. In contrast, electronic documents may be physically stored in one jurisdiction, accessed and used for business purposes in a different (or multiple) jurisdiction(s), and stored for backup purposes in yet another jurisdiction. Electronic documents and data may also be stored on a variety of devices, including servers, hard drives, external media, handheld devices, backup tapes, portable hard drives, data archives, or employees' dual-use/BYOD personal devices.

As a result, lawyers and courts may struggle to determine the location of electronic documents as well as to identify the entity and/or individual properly charged with legal possession, custody, or control of electronic documents. Choice of law disputes may also arise over the body of law applicable to determine the privacy considerations that govern the preservation, access, collection, and production of electronic documents.

IV. THE SEDONA CONFERENCE PRINCIPLES ON POSSESSION, CUSTODY, OR CONTROL—WITH COMMENTARY

***Principle 1**: A responding party will be deemed to be in Rule 34 or Rule 45 "possession, custody, or control" of Documents and ESI when that party has actual possession or the legal right to obtain and produce the Documents and ESI on demand.*

Comments:

A. Interpretation of Possession, Custody, or Control for Purposes of Rules 34 and 45 Should be Consistent across Federal Circuits

As noted above, the various federal circuits have defined Rule 34 or Rule 45 "possession, custody, or control" differently and inconsistently, leading to a lack of clarity for lawyers and organizations that must deal with information in multiple jurisdictions. The varying standards and often inconsistent application of the standards themselves have left parties without definitive guidance and a clear road map when attempting to make legal and defensible discovery decisions, and the courts without clear standards for adjudicating discovery issues. Further, the imprecision of the Practical Ability Test has resulted in inconsistent and, at times, inequitable results in many contexts.[96] The

[96] For the most part, when addressing Documents held by third/non-parties the safe harbor contained in Rule 37(e) will not apply because a party will not have "control" over a non-party's "electronic information systems" to determine their operations (routine, good faith, or otherwise). This further underscores the problems with the current framework, whereby on the one hand a party may have Rule 34 "possession, custody, or control" over third-party data, but on the other hand, the Safe Harbor in the current rules does not apply because the party does not "control" the data. For example, in *GenOn Mid-Atl v. Stone & Webster*, 282 F.R.D. 346, 354 (S.D.N.Y. 2012), the plaintiff was found to have control over documents in the possession of a third-party litigation consultant that was expected to provide expert testimony at trial. The court held that "common sense" suggested that the plaintiff could have obtained the documents from the consultant merely by asking

problems with practical ability, and support for abandoning that standard are explored in more detail in Section III, *supra*.

B. A Framework for a More Objective Definition of "Control"

A more reliable, objective approach to fulfilling a party's Rule 34 and Rule 45 obligations would be to base the interpretation of the language "possession, custody, or control" on the definition of "control" as the legal right to obtain and ability to produce Documents and ESI on demand. Courts in the Third, Fifth, Sixth, Seventh, Eighth, Ninth, Tenth, and Eleventh Circuits apply the Legal Right Standard set forth in Principle 1. That standard establishes that a party is deemed to have possession, custody, or control only if that party has: (1) actual possession of Documents and ESI; or (2) the legal right to obtain Documents and ESI. It is upon this well-established legal footing that this Commentary advocates that Rule 34 or Rule 45 "control" should be defined as the legal right to obtain Documents and ESI and ability to produce them on demand. This would also avoid the potentially unfair results from the application of the Practical Ability Standard, as detailed in Section III, *supra*.

1. Application of "Control" Under Relevant Legal Right Case Law

Illustrative of the definition of "control" in Principle 1 are recent cases decided by the Ninth Circuit where a contractual basis was lacking, such that "control" was found not to exist:

for them, and that the consultant would have honored a request by the plaintiff that the documents be preserved. The plaintiff failed to direct the consultant to preserve the documents, and they apparently were destroyed by the consultant in its normal course of business. Although the court found that the plaintiff had functional control over the documents, it declined to issue sanctions because the plaintiff sufficiently demonstrated that the defendant was not prejudiced.

- *Ubiquti Networks, Inc. v. Kozumi USA Corp.*[97] In *Ubiquti*, the court denied a motion to compel defendants to obtain and produce documents from a consultant, a resident of Taiwan. Although the consultant had provided web design services to the defendant company, had an email account on the company's system (which had not been preserved), and was the brother of an individual defendant, the court found no evidence of a contract or any other legal basis upon which the defendants could legally compel the consultant to produce documents. In denying the motion to compel, the court reasoned: "'[a] party responding to a Rule 34 production request . . . is under an affirmative duty to seek that information reasonably available to [it] from [its] employees, agents, or others subject to [its] control.'"[98]
- *In re NCAA Student-Athlete Name & Likeness Litigation.*[99] In *In re NCAA,* the court held that "[n]either the NCAA Constitution nor the Bylaws grants the NCAA the right to take possession of its members' Documents and ESI," therefore, the NCAA had insufficient control over the documents to retrieve them from its member schools and produce them to the plaintiffs.[100]

The Ninth Circuit has also held that a "relationship" between entities is insufficient to impose Rule 34 "control" over

[97] No. 12-cv-2582 CW JSC, 2013 WL 1767960 (N.D. Cal. Apr. 15, 2013).

[98] *Cf.* Hageman v. Accenture, LLP, No. CIV. 10-1759 RHK/TNL, 2011 WL 8993423 (D. Minn. Oct. 19, 2011) (*supra* note 7 and accompanying text).

[99] No. 09-CV-01967 CW NC, 2012 WL 161240, at *3 (N.D. Cal. Jan. 17, 2012) (citing *In re* Citric Acid Litig., 191 F.3d 1090, 1107 (9th Cir. 1999)).

[100] *Id.* at *5.

Documents and ESI held by a third party without telltale hallmarks of control founded in a legal right to obtain the Documents and ESI from the third party. The plaintiff in *In re Citric Acid Litigation* had subpoenaed Coopers & Lybrand in the U.S. to produce documents from both the U.S. firm as well as a Coopers firm located in Switzerland. The court held that the U.S. firm did not have control over the Swiss firm, because:

> [a]lthough members use the 'Coopers & Lybrand' name, each firm is autonomous. Firms do not share profits or losses, nor do they have any management, authority, or control over other member firms. In addition, C&L-International does not exercise management, authority, or control over member firms. Of particular relevance to the case at hand, C&L-US does not have any economic or legal interest in C&L-Switzerland, and C&L-Switzerland has no such interest in C&L-US.[101]

Indeed, in holding that production would not be compelled pursuant to Rule 34, the court pointed out the impracticability of the Practical Ability Test:

> Ordering a party to produce documents that it does not have the legal right to obtain will oftentimes be futile, precisely because the party has no certain way of getting those documents. . . . There is no mechanism for C&L-US to compel C&L-Switzerland to produce those documents, and it is not clear how [plaintiff] Varni wants C&L-US to go about getting the ECAMA documents, since C&L-Switzerland could legally—and without breaching any contract—continue to refuse to turn

[101] *In re* Citric Acid Litig., 191 F.3d at 1106.

> over such documents. Because C&L-US does not have legal control over C&L-Switzerland's documents, Varni could not compel C&L-US to produce those documents.[102]

Another application of the Legal Right Standard can be seen in the context of the obligation to preserve websites referenced by hyperlinks within a document. Under the Legal Right Standard, there is no such duty to preserve hyperlinks. As the websites referenced by those links are maintained by generally unrelated third parties, the producing party has no legal right to obtain the content of those sites.[103]

2. Application of "Control" Under Restatement Law

The definition of Rule 34 "control" proposed in this Commentary is also supported by other well-established legal authorities that specifically define control consistent with the Legal Right Standard, including the Restatements. To be clear, by describing these various tort-based principles below, it is not this Commentary's intention to impose a tort-based test for Rule

[102] *Id.* at 1108.

[103] *See, e.g.*, Phillips v. Netblue, Inc., No. C-05-4401 SC, 2007 WL 174459, at *2–3 (N.D. Cal. Jan. 22, 2007) (content of reference website links not considered to be within a party's possession, custody, or control); Ferron v. Echostar Satellite, Inc., 658 F. Supp. 2d 859, 864 (S.D. Ohio 2009) *aff'd*, 410 F. App'x 903 (6th Cir. 2010) (plaintiff failed to establish how defendant's failure to maintain website links constituted "bad faith" under the court's inherent sanction power); Philbrick v. eNom, Inc., 593 F. Supp. 2d 352, 372 n.23 (D.N.H. 2009) (court would not sanction defendant for failure to preserve website links where there was no evidence that defendant ever had such information, and plaintiff had also failed to preserve them). *But cf.* United States v. Cyberheat, Inc., No. CV-05-457-TUCDCB, 2007 WL 686678, at *8–9 (D. Ariz. Mar. 2, 2007) (FTC able to obtain images in emails from Hotmail email "trap accounts" where Microsoft maintained web link information within emails and could capture the corresponding web page).

34 possession, custody, or control. Rather, the reference is meant to be merely instructive.

a. Agency

The Restatement (Third) of Agency examines the issue of control from many perspectives as it pertains to the relationship of agency. In particular, § 1.01 cmt. f is instructive as it explains the concept of interim control:

> (1). Principal's power and right of interim control—in general. An essential element of agency is the principal's right to control the agent's actions. Control is a concept that embraces a wide spectrum of meanings, but within any relationship of agency the principal initially states what the agent shall and shall not do, in specific or general terms. Additionally, a principal has the right to give interim instructions or directions to the agent once their relationship is established.[104]

This concept of control presupposes that a principal has the legal right to be able to demand actions from its agent, thereby controlling what the agent shall and shall not do. This is consistent with the Rule 34 Legal Right Standard, and the Rule 34 standard this Commentary is advocating.

b. Torts

The Restatement (Third) of Torts on Physical & Emotional Harm, § 56, provides that retained control for purposes of direct liability for negligence of an independent contractor can be

[104] Restatement (Third) of Agency § 1.01 cmt. f (2006).

established by a contractual right of control or by the hirer's actual exercise of control.[105]

Additionally, several other sections of the Restatement (Second) of Torts address the concept of "control." For example, control-based liability regimes founded in tort doctrine assign liability where:

- parents fail to control their children to prevent intentional harm to others;[106]
- actors fail to control third parties to prevent intentional harm where there is an ability to control third parties and the actor knows or should know of the need to control a third party;[107] and
- a lessor of land retains control of a portion with a dangerous condition the lessor could have discovered and prevented harm.[108]

In contrast, when a party cedes control to another, the Restatement recognizes a halt to liability for the party who has relinquished control.[109] Similarly, § 414 assigns liability to an actor for the torts of her independent contractor where the actor "retains the control of any part of the work."[110]

All of these concepts from the Restatement are consistent with the Rule 34 Legal Right Standard, and the Rule 34 standard this Commentary is advocating.

[105] *See* Restatement (Third) of Torts § 56 (2012).

[106] Restatement (Second) of Torts § 316 (1979).

[107] Restatement (Second) of Torts § 318 (1979).

[108] Restatement (Second) of Torts § 360 (1979).

[109] Restatement (Second) of Torts § 372 (1979).

[110] Restatement (Second) of Torts § 414 (1970).

c. Judgments

The Restatements (Second) of Judgments also addresses the concept of "control."[111] Under principles of the law of judgments, a non-party to an action who controls or substantially participates in the control of the presentation on behalf of a party is bound by the determination of the issues decided.[112]

This too is consistent with the Rule 34 Legal Right Standard, and the Rule 34 standard this Commentary is advocating.

3. Examples of "Control" in the Agency Context

Under principles of agency law, a master's control over her agent is the lynchpin of liability. Under § 219, a master will be liable for her servant's torts when the servant's conduct violated a non-delegable duty.[113]

Cases in the master-servant context are therefore instructive. For example, in *Schmidt v. Burlington Northern and Santa Fe Railway Co.*[114] the court analyzed control on the basis of an employer's right to control its employee's conduct "on the job." The court reasoned:

> [f]or Schmidt to succeed under the sub-servant theory, he must show BNSF controlled or had the right to control his physical conduct on the job. It is not enough for him to merely show WFE was the railroad's agent, or that he was acting to fulfill the railroad's obligations; BNSF's generalized oversight of Schmidt, without physical control or

[111] Restatement (Second) of Judgments §§ 37 and 39 (1982).

[112] Restatement (Second) of Judgments § 39 (1982).

[113] Restatement (Second) of Agency § 219 (1958).

[114] 605 F.3d 686 (9th Cir. 2010).

> the right to exercise physical control of his daily work is insufficient.[115]

Likewise, under the doctrine of respondeat superior, a principal is vicariously liable for his agent's negligent acts done in the scope of the agent's employment so long as the principal controls the means and method by which the agent performs his work.[116] In the case of Rule 34 and Rule 45, it is equally well-reasoned to say that actual control over Documents and ESI is the lynchpin to any duty or obligation. Indeed, some courts have already looked to agency concepts when applying Rule 34.[117]

C. *The Legal Right Standard is a Better Test*

[115] *See also* Pinero v. Jackson Hewett Services, Inc., 638 F. Supp. 2d 632, 640 (E.D. La. 2009) (principal liable for actions of agent when the relationship of the parties includes the principal's right to control physical details of the actor as to the manner of his performance which is characteristic of the relation of master and servant); Ramos v. Berkeley Cty., No. CIV. A. 2:11-3379-SB, 2012 WL 5292895 (D.S.C. Oct. 25, 2012) (granting defendant's motion for judgment on pleadings, dismissing claims because defendant employer was state entity and subject to control of county authorities).

[116] *See* Ramsey v. Gamber, 469 F. App'x 737 (11th Cir. 2012) (citing Martin v. Goodies Distribution, 695 So.2d 1175, 1177 (Ala.1997)); Ware v. Timmons, 954 So.2d 545, 549–50 (Ala. 2006). *See also* Universal Am–Can, Ltd. v. W.C.A.B. (Minteer), 563 Pa. 480, 490, 762 A.2d 328, 333 (2000) ("[C]ontrol over the work to be completed and the manner in which it is to be performed are the primary factors in determining [Rule 34 control] status."); Meyer v. Holley, 537 U.S. 280, 291, 123 S. Ct. 824, 154 L. Ed. 2d 753 (2003) (finding that courts have not imposed liability for failure to supervise in and of itself).

[117] *See, e.g.*, JPMorgan Chase Bank, N.A. v. KB Home, No. 2:08-CV-1711-PMP-RJJ, 2010 WL 1994787 (D. Nev. May 18, 2010) (granting motion to compel because agency relationship was sufficient to find control for purposes of Rule 34); *cf.* Insignia Sys. v. Edelstein, No. 09-4619, 2009 U.S. Dist. LEXIS 98399 (D.N.J. Oct. 20, 2009) (denying motion to compel local counsel to produce documents in possession and custody of lead counsel because no agency relationship existed among counsel).

During the public comment period, the following comments were received:

- A comment was received from several judges that reside in a Circuit that applies the Practical Ability Standard indicating they do not agree with the Commentary's "adoption of the 'legal right standard' to the exclusion of the 'practical ability' standard," because:
    - "omitting the 'practical ability' test could lead to gamesmanship";[118]
    - the problem of document requests issued to a U.S. company in federal litigation to obtain information from a foreign affiliate, possibly in violation of foreign blocking statutes or data privacy laws, "is one of cross-border discovery generally, not of possession, custody or control in particular"; and
    - "[w]hile it may be useful to have a uniform standard in all federal circuits . . . this may be another area where lawyers are concerned about judicial discretion."[119]

[118] The following example was given in the Comment:

> A party may regularly obtain needed information from an affiliate, but when sued state that it has no legal right to obtain information. Or worse, that same defendant may obtain the "good" documents or ESI from its affiliate, while declining to obtain the bad, claiming it has no legal right to compel production.

[119] According to the Comment:

> While there may be outlier judges, or some reported cases that were wrongly decided, that is no reason to advocate

- A comment was received from an industry group that strongly supported the Commentary and in particular, Principle 1, for several reasons, including:
    - it would establish a common, national standard which is "an important discovery reform";
    - courts that apply "the nebulous 'practical ability standard' engage in a highly subjective inquiry that downplays the importance of having any control over—or any legal right—to the information at issue," resulting in a "checkerboard of widely divergent standards";[120]
    - the Practical Ability Standard leads to a "case-by-case" determination of matters vs. the Legal Right Standard which is "fairer and more predictable";
    - the practical ability framework encourages discovery of information over which no party to the action has "possession, custody

abandonment of the practical ability test and the judicial discretion accompanying it.

[120] The following example was noted:

Compare In re Vivendi Univ., S.A., Sec. Litig., No. 02 CIV. 5571 RJH HBP, 2009 WL 8588405, at *3 (S.D.N.Y. July 10, 2009) ("[I]nterlocking officers or directors, without a showing of actual control, does not establish the practical ability of the parent to obtain the documents of the subsidiary."), *with SRAM, LLC v. Hayes Bicycle Grp., Inc.*, No. 12 C 3629, 2013 WL 6490252, at *4 (N.D. Ill. Dec. 10, 2013) (finding "control" where "SRAM has provided undisputed evidence that the two companies share officers and directors and having interrelated corporate structures").

or control" and Rule 45 is already in place for precisely this type of scenario;

- there is "an inherent unfairness in applying a court-ordered compulsion to require X to obtain documents from Y when X can apply no legal compulsion to force Y to turn over the documents," and "parties should not be encouraged by courts to apply pressure without legal justification—simply by virtue of having, for example, the upper hand in a business relationship." Moreover, "a requirement that one entity 'voluntarily' disclose information to another, without the protection of a court order but under threat of sanctions imposed upon the requesting party, runs directly against both the legal trend of increased protection of individuals' information and the reality that more and more information about everyone is available somewhere, if only the right party is asked to produce it";[121] and

[121] Examples noted in the comment included:

> [A]n employer's request to an employee to turn over highly personal information to which the employer is not entitled, no matter how the request is phrased, would run a significant risk of being deemed "coercive."
>
> [O]ne company's request for information from an affiliate, in the absence of a legal right to obtain the information, puts unfair pressure on both the party asking for documents and the party which has to respond. The party making the request cannot "back up" its request with any legal authority, despite the fact that it might itself face sanctions if the other party says "no." And the recipient of the request is forced to weigh the legal and non-legal risks of non-production against the potential risks of disclosing information—likely including financial

  - the approach suggested in the Commentary contains a mechanism to "weed out attempts to structure document maintenance to avoid discovery obligations."[122]

Taking all of those comments into consideration, Sedona believes the Legal Right Standard espoused in the Commentary is a better standard. The Practical Ability Standard:

- is inherently vague—it does not give parties notice of what factors will impact a court's decision making;
- is unevenly applied, thus it leads (as noted in the industry group's submission and throughout the Commentary)—and has the potential to lead—to disparate results;

> and personal information in nearly any case, and sometimes also including health-related, educational, or other information subject to special protection—without even the "legal compulsion" which can sometimes justify such disclosure.
>
> To the extent cross-border production is required, the potential application of non-U.S. law heightens the risk. But even within the U.S., a requirement that one entity "voluntarily" disclose information to another, without the protection of a court order but under threat of sanctions imposed upon the requesting party, runs directly against both the legal trend of increased protection of individuals' information and the reality that more and more information about everyone is available somewhere, if only the right party is asked to produce it.

[122] According to the Comment:

> Under the suggested approach, if a party demonstrates that it does not possess and is without the legal right to obtain requested information, the requesting party can challenge the claim if the relevant facts . . . suggest that a party's lack of control is not merely the by-product of its business decisions but rather an attempt to avoid having control over documents it would prefer not to produce.

- produces results that can vary case-by-case and judge-by-judge, leading to what can be perceived as random results, or at least the potential for different results before different judges and/or where a case lands;
- in the cross-border context, can be used to override foreign data protection laws that may legally restrict the ability to produce data outside of the country in which it resides;[123]
- in the parent/subsidiary/affiliate context, does not appropriately consider corporate formalities that apply to legally distinct entities;

[123] Risk in this already uncertain area has escalated greatly since the Edward Snowden revelations concerning U.S. national security measures threw into question existing cross-border data transfer mechanisms, culminating in the EU/U.S. Safe Harbor agreement being struck down in October 2015 (*see* Schrems v. Data Protection Commissioner, Court of Justice of the European Union, Press Release No 117/15, The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid, 6 October 2015, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf (with link to underlying decision)) and sparking growing enforcement activity from European data protection authorities including in France and Germany. *See, e.g.*, David Meyer, *Here Comes the Post-Safe Harbor EU Privacy Crackdown*, FORTUNE (Feb. 25, 2016), http://fortune.com/2016/02/25/safe-harbor-crackdown/.

Moreover, the stakes are set to rise further as data protection law reforms in Europe exponentially increase fines for violations. When finalized, it is anticipated that fines under the General Data Protection Regulation (GDPR) may be up to 4% of a company's total world annual gross revenue. *See* Committee on Civil Liberties, Justice and Home Affairs, Press Release, Data protection package: Parliament and Council now close to a deal, 15 December 2015, http://www.europarl.europa.eu/news/en/news-room/20151215IPR07597/Data-protection-package-Parliament-and-Council-now-close-to-a-deal.

Nor is this issue limited to Europe as countries around the globe develop tougher data protection regimens with higher fines.

- can create the appearance of unfairness—because it is unbounded by any clear (or "nebulous" as characterized by the Comment from the industry group) factors,[124] there is a potential for cases to be decided differently based purely on "discretion" of different judges;[125] and
- could lead to "futile" and unfair results.[126]

This is not a sound basis for making legal decisions.

In contrast, the Legal Right Standard:

- is grounded in clear, well-established factors (as well as other well-established legal authorities that define control consistent with the Legal

[124] Those may include amorphous concepts like the following over which there are no legal norms:

- "a degree of close coordination";
- "similar interests, missions or goals";
- "interests are sufficiently aligned and closely interrelated"; and
- a "sufficient nexus."

See, e.g., Gross v. Lunduski, 304 F.R.D. 136 (W.D.N.Y. 2014).

[125] That is not to say there is not a fundamental and important need for judicial discretion in the U.S. Judicial system. As an example, the analytical framework of the modified business judgment rule discussed in Principle 3 is an area where individual judges should apply their discretion to those factors based upon the specific factual circumstances of cases.

[126] *Accord* Matthew Enter., Inc. v. Chrysler Grp. LLC, No. 13-cv-04236-BLF, 2015 WL 8482256 (N.D. Cal. Dec. 10, 2015) ("Even if the court were to order that Stevens Creek [car dealership] collect emails from its employees' personal accounts, Chrysler has not identified any authority under which Stevens Creek could force employees to turn them over. The Ninth Circuit has recognized that '[o]rdering a party to produce documents that it does not have the legal right to obtain will oftentimes be futile, precisely because the party has no certain way of getting those documents.'").

Right Standard, as detailed in this Commentary[127]);

- provides notice to the parties of those standards;
- offers consistency in how it should be applied; thus, the result should not depend on where a case lands;
- appropriately considers competing legal interests that can impact "control," including foreign data protection laws and corporate formalities that apply to legally distinct entities; and
- overall leads to fairer results (including with respect to the futility of complying with court orders).

As the new December 1, 2015 Amendments to the Rules of Civil Procedure expressly recognized, consistency across circuits through uniform, national standards is a laudable goal.[128] Parties' legal obligations should not depend on where a case is filed. The approach espoused in this Commentary achieves this important objective. Helping resolve the disparity among Circuits to bring a uniform, national standard to this important area of the law is also consistent with Sedona's mission of moving the law forward in a just and reasoned way.

Just as important, the Legal Right Standard provides clear guidance resulting in its consistent application, which also

[127] There are no such parallels for the Practical Ability Standard.

[128] One of the primary drivers of the 2015 amendments to Rule 37(e) was to "provide a uniform standard in federal courts." *See* FED. R. CIV. P. 37(e)(2), Committee Note (Dec. 15, 2015). *See also*, Advisory Committee Report, *supra* note 5, at B-14, B-17 ("Resolving the circuit split with a more uniform approach . . . has been recognized by the Committee as a worthwhile goal. . . . [The] primary purpose of [amended Rule 37(e)] is to eliminate the circuit split on [a key aspect of the rules].").

furthers Fed. R. Civ. P. 1's goal of "just, speedy and inexpensive determination of every action and proceeding."

Moreover, if a requesting party truly needs information that a responding party can demonstrate it does not have the legal right to obtain, the requesting party is not left without recourse—it can subpoena the Documents and ESI from the non-party that legally controls them via Rule 45, which squarely addresses the discovery of such non-party information. Stated another way, the approach espoused by this Commentary as a whole (including incorporation of the "Legal Right Plus Notification Standard" in Principle 5) fairly puts the onus on the party that claims it needs the information (via its request in the first instance) to obtain it via Rule 45.

A final note: one court has already favorably cited the public comment version of this Commentary before this final version was released, for the proposition that the majority of circuits already follow the Legal Right Standard:

> What does it mean for a party to have control over data like the data disputed here? "Control is defined as the legal right to obtain documents upon demand." Like the majority of circuits, the Ninth Circuit has explicitly rejected an invitation "to define 'control' in a manner that focuses on the party's practical ability to obtain the requested documents."[129]

D. *Illustrations of what Should and Should Not Constitute Rule 34 "Control" Under a Consistent Standard*

The following is a non-exclusive list of illustrative examples where "control" for purposes of disputes under Rules 34 and 45

[129] Matthew Enterprise, Inc. v. Chrysler Grp. LLC, No. 13-cv-04236-BLF, 2015 WL 8482256, at *3 n.37 (N.D. Cal. Dec. 10, 2015).

will or will not exist under the proposed, uniform standard espoused by Principle 1 and this Commentary.

- Illustrative situations/examples where Rule 34 "control" exists:
    - actual possession of data
    - clear contractual right to access or obtain the data
    - deliberate decision to outsource critical business data
    - deliberate decision to move data to foreign jurisdiction for litigation advantage
    - individual obtaining information from their own ISP account (email, Facebook, etc.)
    - separate sister/parent-subsidiary corporation has a legal right to obtain Documents and ESI from its sister corporation
- Illustrative situations/examples where Rule 34 "control" does not exist:
    - customer relationships where there is no legal right to demand data from a customer
    - informal business relationships, i.e., the ability to "ask" for Documents or ESI
    - employer/employee relationships, e.g., employer does not have the legal right to obtain personal Documents and ESI from a director, officer, or employee's personal cell phone, personal email account, or personal social networking sites; employee does not have the legal right to demand or remove data from his/her employer

- former directors, officers, and employee relationships where no legal right to demand data exists
- separate sister/parent-subsidiary corporation does not have a legal right to obtain Documents and ESI from its sister corporation
- partial ownership, minority control situations where no legal right to demand data exists
- international affiliate subject to data privacy or blocking statutes (e.g., company compelled to collect and produce Documents and ESI or data from a country where doing so would be impermissible and perhaps a crime)

Principle 2: *The party opposing the preservation or production of specifically requested Documents and ESI claimed to be outside its control, generally bears the burden of proving that it does not have actual possession or the legal right to obtain the requested Documents and ESI.*

Comment:

Whether "Control" Exists must be Answered, in the First Instance, by the Responding Party

Principle 2 is born out of the wellspring of common sense, but grounded in well-established principles of jurisprudence pursuant to the Federal Rules of Civil Procedure. For example, it is a logical presumption that the responding party would have access to the facts necessary to determine control, e.g., to cite one of the examples listed in the comments to Principle 1, *supra* Section IV(D), whether a contractual relationship exists between a consultant and the organization such that access to the data exists.[130]

More particularly, the justification for placing the burden of demonstrating lack of control can be found in a similar provision of Fed. R. Civ. P. 26(b)(2)(B) which states: "[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, *the party from whom discovery is sought must show* that the information is not reasonably accessible because of undue burden or cost." (emphasis added)

Further, under Fed. R. Civ. P. 34, the party objecting to a discovery request has the obligation to state a reason for such objection, i.e., a lack of control over Documents and ESI requested.

However, this Principle generally applies when the responding party has greater knowledge of or access to the information that bears upon the inquiry. Where the requesting party has equal or superior access to the facts about whether the responding party has actual possession or the legal right to obtain the requested Documents and ESI, the burden should be applied accordingly.[131] Likewise, Principle 2 would not preclude a

[130] *See* Ubiquti Networks, Inc v. Kozumi USA Corp, No. 12-cv-2582 CW (JSC), 2013 WL 1767960 (N.D. Cal. Apr. 15, 2013).

[131] *See, e.g.*, Enviropak Corp. v. Zenfinity Capital, LLC, No. 4:14CV00754 ERW, 2014 WL 5425541, at *7 (E.D. Mo. Oct. 22, 2014) (denying plaintiff's motion to compel production of documents after defendant properly objected to the request as seeking information equally available in public records, because defendant did not control the documents requested and they were in the public domain); Sec. & Exch. Comm'n v. Samuel H. Sloan & Co., 369 F. Supp. 994, 995 (S.D.N.Y. 1973) (denying motion for production of transcript of administrative hearing because "[i]t is well established that discovery need not be required of documents of public record which are equally accessible to all parties").

requesting party from demonstrating that the responding party indeed has control in the appropriate case.

This Principle is also not intended to imply a general duty for a responding party to identify Documents and ESI that might be relevant in a case that are not within a party's "possession, custody, or control." Instead, it only applies to Documents and ESI that are "specifically requested," in accordance with the general mandates of Rule 34.[132] Stated another way, this Principle does not apply unless and until the requesting party has met its burden to be as specific as possible when requesting

[132] *See, e.g.*, FED. R. CIV. P. 34(b)(1)(A) ("Contents of the Request. The request must describe with *reasonable particularity* each item or category of items to be inspected.") (emphasis added); Mancia v. Mayflower Textile Servs. Co., 253 F.R.D. 354, 357–58 (D. Md. 2008):

> [Rule 26(g)] provides a *deterrent* to both *excessive discovery* and *evasion* by imposing a certification requirement that obligates each attorney to *stop and think about the legitimacy of a discovery request*. . . . [T]he rule aspires to eliminate one of the most prevalent of all discovery abuses: kneejerk discovery requests served without consideration of cost or burden to the responding party. Despite the requirements of the rule, however, the reality appears to be that with respect to certain discovery, principally interrogatories and document production requests, lawyers customarily serve requests that are far broader, more redundant and burdensome than necessary to obtain sufficient facts to enable them to resolve the case through motion, settlement or trial.

(emphasis in original); Frey v. Gainey Transp. Servs., No. CIVA 1:05CV1493 JOF, 2006 WL 2443787, at *9 (N.D. Ga. Aug. 22, 2006) (Courts frown on overly broad preservation/"spoliation" letters/demands that "lend itself to an effort on any plaintiff's part to sandbag a defendant in the event that any of those materials were not preserved."). *Accord* FED. R. CIV. P. 34(b) Committee Note (Dec. 15, 2015) (Although objections to Rule 34 requests must be stated with specificity under the amended Rule, "[a]n objection may state that a request is overbroad.").

information in discovery or making pre-litigation preservation demands.

During the public comment period, a very short comment was received stating that in the commenter's view, Principle 2 "shifts the burden of proof improperly." While we agree this Principle shifts the burden of proof to the responding party,[133] we believe this is a fair compromise and the correct result for several reasons:

- First, the burden is not a high one. If a party does not have actual possession or custody of Documents and ESI that are "specifically requested" under a proper Rule 34 request,[134] or the legal right to obtain such Documents and/or Data, a simple representation (via a meet-and-confer letter, declaration, discovery response, or deposition testimony) so stating this meets the burden. The burden would then switch to the requesting party to demonstrate that the

[133] *See, e.g.*, Matthew Enterprise, Inc. v. Chrysler Grp. LLC, No. 13-cv-04236, 2015 WL 8482256 (N.D. Cal. Dec. 10, 2015) ("The party seeking production of the documents . . . bears the burden of proving that the opposing party has such control."); Alexander Interactive, Inc. v. Adorama, Inc., No. 12 CIV. 6608 PKC JCF, 2014 WL 61472, at *3 (S.D.N.Y. Jan. 6, 2014) ("Where control is contested, the party seeking production of documents bears the burden of establishing the opposing party's control over those documents."); St. Jude Med. S.C., Inc. v. Jassen-Counotte, 104 F. Supp. 3d 1150, 1159 (D. Ore. 2015) ("The burden is on the party seeking the production of documents to prove that the opposing or subpoenaed party has the requisite control."). *Accord In re* Porsche Cars N. Am., Inc., No. 2:11-MD-2233, 2012 WL 4361430, at *4 (S.D. Ohio Sept. 25, 2012) ("Speculation that one company has legal control over the documents of another company simply because they are related corporate entities is insufficient to establish control and compel discovery.").

[134] *See* FED. R. CIV . P. 34 (b)(1)(A) ("Contents of the Request. The request must describe with reasonable particularity each item or category of items to be inspected.").

responding party indeed has the legal right to obtain the specific Documents and ESI they want, if they believe that is the case.

- As noted above, the burden of proof is intended to be fluid; if the requesting party has equal or superior access to information about the responding party's legal right to obtain the requested Documents and ESI, then the burden should shift to the requesting party. In short, the parties and the court have a collective responsibility to address these issues, which follows how responsibilities are allocated when addressing similar proof issues under the Federal Rules.[135]
- Finally, Sedona wants to ultimately have a balanced approach to these issues and believes this is a fair trade-off for achieving a national standard. While responding parties will no longer be unfairly burdened with having to preserve, search, review, and produce Documents and ESI they have no legal right to obtain, there is a now a small burden placed on them to demonstrate they do not have the legal right to do so

[135] *See, e.g.*, FED. R. CIV. P. 26(b), Committee Note (Dec. 15, 2015) (emphasis added):

> Restoring the proportionality calculation to Rule 26(b)(1) does not change the existing responsibilities of the court and the parties to consider proportionality, and the change does not place on the party seeking discovery the burden of addressing all proportionality considerations.
>
> Nor is the change intended to permit the opposing party to refuse discovery simply by making a boilerplate objection that it is not proportional. *The parties and the court have a collective responsibility to consider the proportionality of all discovery and consider it in resolving discovery disputes.*

> when faced with a specifically tailored request for such Documents and ESI.

Principle 3(a): *When a challenge is raised about whether a responding party has Rule 34 or Rule 45 "possession, custody, or control" over Documents and ESI, the Court should apply modified "business judgment rule" factors that, if met, would allow certain, rebuttable presumptions in favor of the responding party.*

Principle 3(b): *In order to overcome the presumptions of the modified business judgment rule, the requesting party bears the burden to show that the responding party's decisions concerning the location, format, media, hosting, and access to Documents and ESI lacked a good faith basis and were not reasonably related to the responding party's legitimate business interests.*

Comments:

A. Rule 34 Application of the Business Judgment Rule

> The business judgment rule is an acknowledgment of the managerial prerogatives of [ ] directors [of a corporation] under [a state statute]. It is a presumption that in making a business decision the directors of a corporation acted on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company. Absent an abuse of discretion, that judgment will be respected by the courts. The burden is on the party challenging the decision to establish facts rebutting the presumption.[136]

[136] Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984), *overruled on other grounds by* Brehm v. Eisner, 746 A.2d 244 (Del. 2000) (internal citations omitted).

As applied in the context of possession, custody, or control of Documents and ESI, the business judgment rule would acknowledge the managerial prerogatives of an enterprise in managing its Documents and ESI if it acts on an informed basis, in good faith, and in the honest belief that the action taken was in the best interests of the organization. Once this showing is made, absent demonstrable proof that decisions concerning the management of Documents and ESI lacked a good faith business basis, those decisions will be respected by the courts.[137] The burden is on the party challenging the decision to establish facts rebutting the presumption.[138] Cases that apply the business judgment rule identify foundational principles that courts may apply, in a slightly modified manner, to adjudicate disputes

[137] In the context of motion practice concerning electronic discovery disputes, pre-litigation decisions by an organization concerning the treatment of Documents and ESI may be documented and supported by sworn affidavits of fact submitted by an affiant who is competent and authorized to make such affidavits.

[138] The business judgment rule arises and is typically applied in the context of corporate transactions. This Commentary seeks to translate the deference that courts grant to a corporate board's business decisions into deference that courts should grant to an entity's pre-litigation decisions concerning IT systems and information management in the context of electronic discovery. The authors note that in contrast to board decisions concerning corporate transactions, lower-level personnel within an organization typically make pre-litigation IT and information management decisions. For this reason, this Commentary does not advocate a literal application of each aspect of the business judgment rule to an entity's or organization's pre-litigation decisions.

For a thorough discussion of information management in the context of eDiscovery, *see* The Sedona Conference, *Commentary on Information Governance*, 15 SEDONA CONF. J. 125 (2014), *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20Commentary%20on%20Information%20Governance.

concerning Rule 34 possession, custody, or control of Documents and ESI, including:

- a rebuttable presumption that good faith decisions concerning the management of Documents and ESI are not subject to discovery;[139]
- absent a colorable rebuttal of the presumption, courts will not substitute their judgment for that of the responding party if the decision can be attributed to a rational business purpose;[140]
- the presumption shields good faith business decisions that are reasonably prudent and believed to be in the entity's best interest at the time they are made;[141]
- courts will not overturn decisions concerning the management of Documents and ESI unless the decisions lack any rational business purpose;[142] and

[139] *See, e.g.*, Seidman v. Clifton Sav. Bank, S.L.A., 205 N.J. 150, 166, 14 A.3d 36, 45 (2011):

> Under the business judgment rule, there is a rebuttable presumption that good faith decisions based on reasonable business knowledge by a board of directors are not actionable by those who have an interest in the business entity. The rule protects a board of directors from being questioned or second-guessed on conduct of corporate affairs, except in instances of fraud, self-dealing, or unconscionable conduct; it exists to promote and protect the full and free exercise of the power of management given to the directors. Stated differently, bad judgment, without bad faith, does not ordinarily make officers individually liable.

[140] Omnicare, Inc. v. NCS Healthcare, Inc., 818 A.2d 914, 928 (Del. 2003).

[141] Oberbillig v. W. Grand Towers Condo. Ass'n, 807 N.W.2d 143, 154 (Iowa 2011).

[142] Laborers' Local v. Intersil, 868 F. Supp. 2d 838, 846 (N.D. Cal. 2012).

- the rebuttable presumption shields entities from allegations of spoliation arising from good faith business decisions made in an informed and deliberate manner. However, entities may be susceptible to a spoliation finding where their decisions demonstrate bad faith.[143]

The type of deference afforded by a modified business judgment rule analysis is already enshrined in electronic discovery case law.[144] In the eDiscovery context, courts have already recognized the type of presumptions that are allowed by the business judgment rule, by similarly deferring to an entity's data management decisions.[145] This type of deference to good faith business decisions also acknowledges that the management of ESI, including in the context of preservation and spoliation, "cannot be analyzed in the same way as similar claims involving

[143] TSG Water Res., Inc. v. D'Alba & Donovan Certified Pub. Accountants, P.C., 260 F. App'x 191, 197 (11th Cir. 2007).

[144] "[Because] there are many ways to manage electronic data, litigants are free to choose how this task [preservation] is accomplished" and responding parties are "best situated" to evaluate the detailed procedures, methodologies, and technologies "appropriate for preserving and producing their own electronic data and documents." The Sedona Conference, *Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible*, 10 SEDONA CONF. J. 281, 284 (2008) (citing Zubulake v. UBS Warburg LLC ("Zubulake IV"), 220 F.R.D. 212, 218 (S.D.N.Y. 2003) and Principle 6 of The Sedona Conference, *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, THE SEDONA CONFERENCE (2nd ed. 2007), *available at* https://thesedonaconference.org/publication/The%20Sedona%20Principles).

[145] *See* E.I. du Pont de Nemours and Co. v. Kolon Indus., Inc., No. 3:09CV58, 2011 WL 1597528 (E.D. Va. Apr. 27, 2011) (deferring to producing party's decision after the onset of litigation to shorten retention period of email in view of evidence that party's preservation process was reasonable and undertaken in good faith).

static information."[146] Rule 37(e) further buttresses the exercise of deference because it shields entities from spoliation liability when the routine, good faith operation of electronic information systems causes the loss of information after the onset of a duty to preserve.

Further, the Federal Rules' meet and confer obligations, particularly with respect to scope of discovery, issues about disclosure of Documents and ESI, protective orders, and motions to compel[147] should obviate the need for formal discovery into pre-litigation business decisions about the management of Documents and ESI for purposes of applying the presumptions of the business judgment rule. In situations where the modified business judgment presumptions are being invoked, those rules should encourage parties to informally exchange general information about the circumstances under which the pre-litigation decision(s) concerning management of the Documents and ESI at issue were made. *However, it is important to note that those considerations only apply if a responding party is relying upon the modified business judgment rule presumptions.* Stated another way, this Principle is not intended to create a general right to inquire about or conduct discovery into pre-litigation business decisions about a party's management of Documents and ESI; it is only if the modified business judgment rule is being asserted that such disclosures may be required to capitalize on the presumptions. Likewise, litigants and the courts can use Rule 26(b)(2)(C)(iii) as a proxy for one of the main tenets of the

[146] The Sedona Conference, *Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible*, *supra* note 144, at 285 (quoting Lee H. Rosenthal, A Few Thoughts on Electronic Discovery After December 1, 2006, 116 YALE L. J. POCKET PART 167 (2006), http://yalelawjournal.org/forum/an-overview-of-the-e-discovery-rules-amendments).

[147] *See* FED. R. CIV. P. 26(c) and (f) and FED. R. CIV. P. 37(d)(1)(B).

business judgment rule, namely the application of a rebuttable presumption that good faith decisions concerning the management of Documents and ESI are not subject to discovery.[148]

To summarize, the presumption that an entity made good faith pre-litigation business decisions concerning the management of its Documents and ESI shall apply when: (1) after asserting an intention to rely upon the modified business

[148] The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 11 SEDONA CONF. J. 289, 294 (2010), *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Proportionality. *See also* Wood v. Capital One Servs., LLC, No. 09-CV-1445 NPM/DEP, 2011 WL 2154279, at *5, 7 (N.D.N.Y. Apr. 15, 2011) (noting that "the scope of discovery is defined in the first instance by relevance to the claims and defenses in a case" and, applying proportionality principles, denying plaintiff's motion to compel production of emails and other ESI where "the relevance of the specific discovery sought is marginal, and the information sought is not likely to play an important role in resolving the material issues in the case"); Tamburo v. Dworkin, No. 04 C 3317, 2010 WL 4867346, at *3 (N.D. Ill. Nov. 17, 2010) (ordering a phased discovery schedule "to ensure that discovery is proportional to the specific circumstances of this case, and to secure the just, speedy, and inexpensive determination of this action"); E.I. du Pont de Nemours and Co. v. Kolon Industries, Inc., No. 3:09CV58, 2011 WL 1597528, at *10 (E.D. Va. Apr. 27, 2011) (citing *Victor Stanley*'s, *infra* following case citation, discussion of proportionate preservation conduct and denying motion for spoliation sanctions where responding party took reasonable measures to preserve information and could not have reasonably known that certain custodians' emails would be relevant to the other side's defenses); Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 522–23 (D. Md. 2010):

> [W]hether preservation or discovery conduct is acceptable in a case depends on what is reasonable, and that in turn depends on whether what was done—or not done—was proportional to that case and consistent with clearly established applicable standards. . . . [A]ssessment of reasonableness and proportionality should be at the forefront of all inquiries into whether a party has fulfilled its duty to preserve relevant evidence.

(internal citation and quotation omitted).

judgment rule presumption, the entity meets its obligation to make good faith Rule 26 disclosures concerning pre-litigation decisions that were made about Documents and ESI and (2) absent indicia of bad faith. Once that showing is made, if the requesting party wants to challenge the presumption, it bears the burden to demonstrate that the producing party's pre-litigation decisions about Documents and ESI were made in bad faith, i.e., the entity did not act on an informed basis, or in good faith, and in the honest belief that the action taken was in the best interests of the organization, by adducing actual evidence (not mere speculation)[149] in support of such a claim in accordance with the mandates of Rules 26(g) and 11.[150] Facts supporting an

[149] *See, e.g.*, *In re* Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (vacating order allowing discovery of certain databases where there was no factual finding of "some non-compliance with discovery rules by Ford"); Scotts Co., LLC v. Liberty Mut. Ins. Co., No. CIV. A. 2:06-CV-899, 2007 WL 1723509 (S.D. Ohio June 12, 2007) (mere suspicion that defendant was withholding ESI is an insufficient basis to permit discovery on discovery, including forensic searches of defendant's computer systems, network servers, and databases); Hubbard v. Potter, 247 F.R.D. 27 (D.D.C. 2008) (rejecting a request for additional discovery because speculation that other electronic documents existed does not overcome a Rule 26(g) certification); Beverly Hills Unified Sch. Dist. v. Fed. Transit Admin., No. CV 12-9861-GW SSX, 2013 WL 6154168 (C.D. Cal. Nov. 7, 2013) (belief that destroyed emails would demonstrate failure to comply with federal law too speculative to justify additional discovery); Rusk v. New York State Thruway Auth., No. 10-CV-0544A SR, 2011 WL 6936344, at *2 (W.D.N.Y. Dec. 29, 2011) (denying plaintiff's motion to compel as "[p]laintiff's speculation that additional e-mails exist is insufficient to overcome counsel's declaration that a search for responsive documents has been conducted and that responsive documents have been disclosed").

[150] The Advisory Committee's Notes to Rule 26(g) explain that the rule "parallels the amendments to Rule 11" and "requires that the attorney make a reasonable inquiry into the factual basis of his response, request, or objection." FED. R. CIV. P. 26(g) Advisory Committee Notes (1983). Further, "[t]he duty to make a 'reasonable inquiry' is satisfied if the investigation undertaken by the attorney and the conclusions drawn therefrom are reasonable

"improper purpose" attack against the presumption could include business decisions that render the information more difficult or expensive to access for litigation without offering a corresponding business advantage, or downgrading the "usability" of electronic information without a corresponding business reason for doing so.

B. Appropriate Modifications of the Business Judgment Rule for Rule 34 and Rule 45 Analysis of Possession, Custody, or Control

To be fairly applied in the Rule 34 and Rule 45 "possession, custody, or control" context, some adjustments need to be made to the traditional business judgment rule factors. These include the following:

- First, the business judgment rule's traditional "abuse of discretion" standard should be eliminated in this context, in favor of the "control" paradigm advanced earlier in this Commentary.[151]
- Second, the traditional form of the business judgment rule requires courts to honor the organization's directors' business judgment absent an abuse of their discretion. In the context

under the circumstances. It is an objective standard similar to the one imposed by Rule 11." *Id*.

[151] Further, when a court attempts to adjudicate motive, it is difficult to apply the business judgment rule's "abuse of discretion" test because it distracts from the analysis of the entity's underlying good or bad faith. Under a modified business judgment rule adapted to provide an analytical framework to adjudicate disputes concerning the possession, custody, or control of Documents and ESI, the entity and its personnel would enjoy a presumption that business decisions taken within the scope of their duties were made in the good faith and honest belief that the action taken was in the best interests of the company. Determination of the entity's intent (i.e., their "good faith" or not) take a back seat to determining whether the entity made a legitimate business decision, regardless of intent.

of Rule 34 possession, custody, or control, however, IT executives and other personnel with decision-making authority are not directly analogous to members of boards of directors, who are company executives of the highest level. In contrast, personnel charged with decision making regarding the management of electronic information typically occupy a lower rung in corporate managerial hierarchies.

- Third, the traditional factors that courts have examined to determine whether a company properly exercised its business judgment[152] should be adjusted as follows for the Rule 34 context:

TRADITIONAL BUSINESS JUDGMENT RULE	**RULE 34 POSSESSION, CUSTODY, OR CONTROL BUSINESS JUDGMENT RULE**
Pre-decision conduct	Same
The decision-making method	Same
The decision-makers themselves	Same
Formality of the decision	Business basis of the decision
Impact of the decision on the directors, the company, and the shareholders	Impact of the decision on the possession, custody, or control of Documents and ESI

In particular, set forth below is a table that in the left column recites ***non-exclusive***[153] factors cited by courts applying the

[152] *See, e.g.*, *In re* Abbott Laboratories Derivative Shareholders Litig., 325 F.3d 795, 806 (7th Cir. 2003); Ocilla Indus., Inc. v. Katz, 677 F. Supp. 1291, 1298 (E.D.N.Y. 1987); Herald Co. v. Seawell, 472 F.2d 1081, 1101 (10th Cir. 1972); *In re* Gulf Fleet Holdings, Inc., 491 B.R. 747, 770 (Bankr. W.D. La. 2013); *In re* PSE & G S'holder Litig., 173 N.J. 258, 296, 801 A.2d 295, 319 (2002).

[153] The table is not intended to serve as an exhaustive, exclusive, or mandatory 'checklist' of requirements or analytical factors.

business judgment rule to adjudicate business disputes,[154] and in the right column contains suggestions for how the business judgment rule factors should be applied in the Rule 34 context.

TRADITIONAL BUSINESS JUDGMENT RULE FACTOR	**RULE 34 POSSESSION, CUSTODY, OR CONTROL BUSINESS JUDGMENT RULE FACTOR**
Whether the decision was made with requisite care and diligence	Adopt as is
Whether the decision was an exercise in arbitrariness, favoritism, discrimination, or malice	Adopt as is
Whether the decision was made after reasonable inquiry	Adopt as is
Whether the decision was made after reasonable investigation and in a cool, dispassionate, and thorough fashion	Adopt as is

[154] *See* Baldwin v. Bader, 585 F.3d 18, 22 (1st Cir. 2009); Cia Naviera Financiera Aries, S.A. v. 50 Sutton Place South Owners, Inc., 510 F. App'x 60, 63 (2d Cir. 2013); Halebian v. Berv, 644 F.3d 122, 131 (2d Cir. 2011); *In re* Lemington Home for Aged, 659 F.3d 282, 292 (3d Cir. 2011), *as amended* (Oct. 20, 2011), *subsequent mandamus proceeding sub nom. In re* Baldwin, 700 F.3d 122 (3d Cir. 2012); Dellastatious v. Williams, 242 F.3d 191, 194 (4th Cir. 2001); Bolton v. Tesoro Petroleum Corp., 871 F.2d 1266, 1274 (5th Cir. 1989); Priddy v. Edelman, 883 F.2d 438, 443 (6th Cir. 1989); *In re* Abbott Laboratories Derivative Shareholders Litig., 325 F.3d 795, 807 (7th Cir. 2003); Potter v. Hughes, 546 F.3d 1051, 1059 (9th Cir. 2008); Hoye v. Meek, 795 F.2d 893, 896 (10th Cir. 1986); TSG Water Resources, Inc. v. D'Alba & Donovan Certified Public Accountants, P.C., 260 F. App'x 191, 198 (11th Cir. 2007); Pirelli Armstrong Tire Corp. v. Retiree Med. Benefits Trust, 534 F.3d 779, 791 (D.C. Cir. 2008).

TRADITIONAL BUSINESS JUDGMENT RULE FACTOR	**RULE 34 POSSESSION, CUSTODY, OR CONTROL BUSINESS JUDGMENT RULE FACTOR**
Whether the methods and procedures followed in gathering and analyzing information prior to making a decision were restricted in scope, shallow in execution, a mere pretext, half-hearted, or a sham	Adopt as is
Whether the decision was made independently	Adopt as is
Whether the decision-maker was assisted by counsel or other "reputable outside advisors"	Whether the decision-maker was assisted by "reputable advisors"[155]
Whether the decision was made in reliance on advice of experienced and knowledgeable counsel	Whether the decision was made in reliance on advice of experienced and knowledgeable personnel[156]
Whether the decision was delegated to a person who was not properly supervised	Adopt as is
Whether the decision-makers complied with any applicable legal duties	Adopt as is
Whether the decision was documented	Adopt as is
The speed with which the decision was made	Adopt as is
Whether the decision was the result of collusion between a director and an outsider	Whether the decision was demonstrably the result of an improper attempt to render information less useable or accessible to achieve tactical advantage in litigation

[155] Reputable advisors include internal or outside advisors.

[156] Experienced and knowledgeable personnel include internal or outside resources.

TRADITIONAL BUSINESS JUDGMENT RULE FACTOR	RULE 34 POSSESSION, CUSTODY, OR CONTROL BUSINESS JUDGMENT RULE FACTOR
Whether the decision was made with a "we don't care about the risks" attitude	Adopt as is
Whether the decision promoted directors' personal interests	Not applicable
Whether benefits accruing to the directors from the decision were made available to other shareholders on equal terms	Not applicable
Whether the decision was fair	Not applicable

Importantly, it is recognized that the business judgment rule was created to protect members of the Boards of Directors, not rank-and-file executives, managers, or other decision-makers. Courts should translate the rule to fit the circumstances of electronic discovery when applying it to pre-litigation decisions made by an entity's personnel below the board of director level concerning the management of electronic information. When a corporate document/data storage or retention decision is made by a person whose legal duties arise from the employment relationship instead of membership on the board, examination of the decision should legitimately include inquiry into why the decision-maker was authorized to make the decision. The question of "why" reflects directly on the issue of whether the company acted "in good faith."

Finally, like other areas of electronic discovery, the business judgment rule provides courts with an analytical framework to conduct case and fact specific inquiries[157] to resolve parties' Rule 34 and Rule 45 disputes over possession, custody, or control.[158]

C. *The (Re)Emergence of Information Governance*

During the past several years, there has been a renewed recognition that one of the most effective ways to streamline eDiscovery in litigation, including the associated costs, is to better organize massive volumes of data in the first instance, or

[157] Determining when the duty to preserve is triggered is always a fact-specific analysis that depends on the unique circumstances of each case. *See generally* Rimkus Consulting Grp., Inc. v. Cammarata, 688 F. Supp. 2d 598, 613 (S.D. Tex. 2010) (The "analysis [of when the duty to preserve arises] depends heavily on the facts and circumstances of each case and cannot be reduced to a generalized checklist of what is acceptable or unacceptable.") (citing Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 464–65 (S.D.N.Y. 2010), *abrogated by* Chin v. Port Auth. of New York & New Jersey, 685 F.3d 135 (2d Cir. 2012)); Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 522 (D. Md. 2010) ("[T]he duty to preserve evidence should not be analyzed in absolute terms; it requires nuance, because the duty 'cannot be defined with precision.'") (internal quotation omitted); Cache La Poudre Feeds, LLC v. Land O' Lakes, Inc., 244 F.R.D. 614, 621 (D. Colo. 2007) (When deciding when the duty to preserve evidence arises, "[u]ltimately, the court's decision must be guided by the facts of each case."). *Cf. also* The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265, 268 (2010), *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Legal%20Holds ("The basic principle that an organization has a duty to preserve relevant information in anticipation of litigation is easy to articulate. However, the precise application of that duty can be elusive.").

[158] This is an area where individual judges can apply their discretion in applying the business judgment factors.

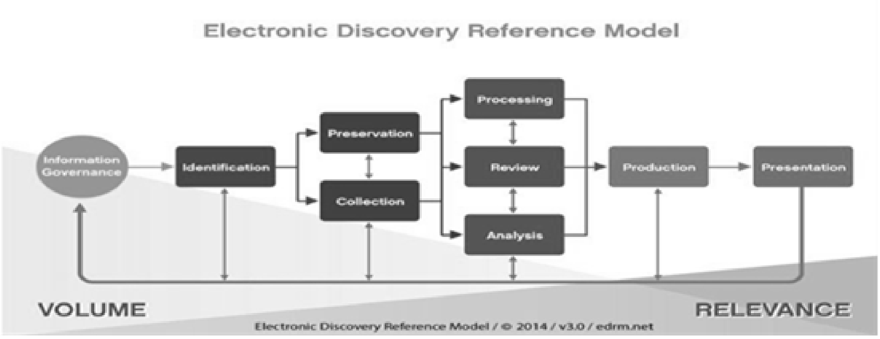
what is sometimes referred to as a focus on the left-hand side of the EDRM (Electronic Discovery Reference Model).[159]

The Sedona Conference has specifically published a Commentary on those issues.[160] The *Commentary on Information Governance* notes that the benefits of establishing an information governance program include: "enhanced compliance with legal obligations for records retention, privacy and data security, and e-discovery, as information policies and processes are rationalized, integrated, and aligned in accord with the organization's information governance strategy."[161]

Applying the modified business judgment factors in the context of Rule 34 and 45 possession, custody, or control decisions will further the goal of encouraging the expansion of information governance programs to help reduce eDiscovery costs in litigation, which is again consistent with the mandates of Fed. R. Civ. P. 1.

Principle 4: *Rule 34 and Rule 45 notions of "possession, custody, or control" should never be construed to override conflicting*

[159]



[160] *See* The Sedona Conference, *Commentary on Information Governance*, 15 SEDONA CONF. J. 125, 134 (2014), *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20Commentary%20on%20Information%20Governance.

[161] *Id*. at 134.

state or federal privacy or other statutory obligations, including foreign data protection laws.

Comments:

The mere fact that a party may be deemed to have possession, custody, or control over certain Documents or ESI is not necessarily dispositive of whether the Documents and ESI ultimately can or should be produced. State and federal statutory limitations, privacy laws, or international laws may preclude or limit disclosure of the kind of Documents or ESI sought. Thus, the possession, custody, or control analysis should also factor in federal and state statutory non-disclosure obligations, along with foreign data protection laws, to ensure that discovery obligations are not inconsistent and do not force non-compliance. This is particularly true when the scope of discovery implicates disclosure of information involving consumers' rights and privacy considerations.

A. Examples of Overriding Statutory Restrictions

For example, the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), precludes financial institutions from "disclos[ing] to a nonaffiliated third party any nonpublic personal information, unless such financial institutions provide or have provided to the consumer a notice that complies with section 6803 of this title."[162] The statute by its terms supersedes "any [s]tate statute, regulation, order, or interpretation" to the extent that they are inconsistent with state law.[163] A number of courts have interpreted this language to hold that GLBA preempts any inconsistent or contrary state law, rule, ordinance, or court order.[164] Additionally, at least one court

[162] 15 U.S.C.A. § 6802(a) (1999).

[163] 15 U.S.C.A. § 6807(a) (1999).

[164] *See* Bowler v. Hawke, 320 F.3d 59 (1st Cir. 2003) (GLBA preempts state statutes regulating insurance); Cline v. Hawke, 51 F. App'x 392 (4th Cir. 2002)

has extended GLBA non-disclosure requirements to third parties with whom the financial institution does business.[165]

Similarly, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the release of individually identifiable "protected health information" by health care providers to litigants and may be in conflict with discovery obligations.[166] Among other things, HIPAA precludes health care providers from responding to "a subpoena, discovery request, or other lawful process that is not accompanied by an order of court or administrative tribunal" unless the health care provider "receives satisfactory assurance . . . from the party seeking the information" of "reasonable efforts" to (i) provide appropriate notice to the affected patient or (ii) secure a qualified protective order.[167] However, HIPAA by its terms establishes a floor, not a ceiling, thus more restrictive state statutes (meaning those under which the patient is afforded greater protection from disclosure) are not preempted.[168]

Other federal statutes such as the Genetic Information Nondiscrimination Act of 2008 (GINA),[169] Computer Fraud & Abuse

(GLBA preempted certain West Virginia insurance regulations); Gen. Motors Corp. v. Kilgore, 853 So. 2d 171 (Ala. 2002) (GLBA preempts Alabama law permitting discovery of certain information).

[165] Union Planters Bank v. Gavel, No. CIV. A. 02-1224, 2002 WL 975675 (E.D. La. May 9, 2002), *vacated on other grounds,* 369 F.3d 457 (5th Cir. 2004) (holding that GLBA precludes a third party from complying with a subpoena absent consent of the defendant's customers where the third party's business was financial in nature).

[166] 45 C.F.R. § 164.512(e) (2016).

[167] *Id.*

[168] 45 C.F.R. § 160.203 (2016).

[169] Pub. L. No. 110–233, 122 Stat. 881 (May 21, 2008).

Act (CFAA),[170] and Stored Communications Act (SCA),[171] and their state equivalents, likewise impose strict limitations on disclosure of data and further limit the manner in which such data may be obtained, which may be in conflict with discovery obligations. For example, under Fed. R. Civ. P. 34, a court may find that an employer has sufficient control over corporate data on dual-use devices (devices used by an employee for both business and personal purposes, also known as "bring your own device" (BYOD)) and is obligated to preserve and produce such relevant information. However, under some circumstances, employers may risk liability for reviewing certain information stored on an employee's dual-use device regardless of the employer's policy or of the employee's purported "consent," leaving employers in an unwinnable discovery catch-22.[172]

Likewise, employers who access information stored on a dual-use device, even with the employee's authorization, could still be exposed to liability for statutory breaches under certain circumstances due to the nature of the data stored on the device, for example, if the employer accessed information protected by GINA or the American's With Disabilities Act (ADA).[173] In addition, many states have enacted some type of social media password protection laws, which prohibit employers from requiring employees to disclose user names and passwords for

[170] 18 U.S.C. § 1030.

[171] 18 U.S.C. §§ 2701–2712.

[172] *See, e.g.*, Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2008); computer trespass laws that have been enacted by all 50 states; Pure Boot Camp, Inc. v. Warrier Fitness Boot Camp, LLC, 587 F. Supp. 2d 548 (S.D.N.Y. 2008); Pietrylo v. Hillstone Restaurant Grp., No. CIV.06-5754(FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009).

[173] 42 U.S.C. § 12112 *et seq*. (1995).

personal social networking accounts like Facebook, Twitter, and LinkedIn.[174]

Thus, while a responding party may have control over certain Documents or ESI based on the manner and location in which they are stored, production of such information in the course of litigation must be reconciled with overarching privacy considerations by which a responding party is statutorily bound. Accordingly, courts evaluating whether a responding party has possession, custody, or control should give deference to state and federal statutes limiting or precluding disclosure, and litigants should not be punished in discovery disputes for complying with such laws.

B. International Law must also be Considered

[174] *See* Philip L. Gordon & Joon Hwang, *Making Sense of the Complex Patchwork of State Social Media Password Protection Laws Creates Challenges for Employers*, LITTLER (May 13, 2013), http://www.littler.com/making-sense-complex-patchwork-created-nearly-one-dozen-new-social-media-password-protection-laws ("In a single season, spring 2013, seven states enacted social media password protection legislation, bringing the total number of states to 11 since Maryland enacted the first such law in May 2012. Bills are pending in more than 20 other states. The current roster of states, dominated by the Rocky Mountain Region and the Far West, is as follows: Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Mexico, Oregon, Utah and Washington. New Jersey appears poised to join this group as the state's legislature amends a bill conditionally vetoed by Governor Christie in May."); Brent Johnson, *Christie signs bill banning N.J. companies from forcing workers to hand over social media passwords*, THE STAR LEDGER (August 29, 2013), http://www.nj.com/politics/index.ssf/2013/08/christie_signs_bill_banning_nj_companies_from_forcing_workers_to_hand_over_social_media_passwords.html ("Gov. Christie signed a bill today that will ban New Jersey companies from forcing workers to hand over user names or passwords to their social media accounts. Under [the legislation], companies will be fined $1,000 if they request or demand access to workers' or potential employees' accounts on websites like Facebook, Twitter, LinkedIn and Pinterest.").

The same analysis is necessary when parties seek foreign data that may be subject to data privacy and blocking statutes that operate to legally preclude discovery and/or movement of private data across the border into the United States.[175] At least 58 countries have been identified as having some form of autonomous data protection laws.[176] The consequences for violating international laws can be severe.[177] Moreover, a party may believe it owns ESI under United States law, but in fact may not own it under the laws of various foreign jurisdictions. As such, where international law is implicated, the question is not limited to whether a party simply has custody, but also whether the party actually has ownership over the Documents and ESI sought.[178] As a result, the relatively broad discovery permitted by United States federal courts is in direct conflict with international restrictions on data movement.[179]

[175] See 45 C.F.R. § 164.512(e); The Sedona Conference, Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery, supra note 48; see also Moze Cowper and Amor Esteban, E-Discovery, Privacy, and the Transfer of Data Across Borders: Proposed Solutions for Cutting the Gordian Knot, 10 SEDONA CONF. J. 263 (2009).

[176] *See* The Sedona Conference, *International Overview of Discovery, Data Privacy & Disclosure Requirements*, THE SEDONA CONFERENCE (Sept. 2009), https://thesedonaconference.org/publication/International%20Overview%20of%20Discovery%20Data%20Privacy%20and%20Disclosure%20Requirements.

[177] See The Sedona Conference, Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery, supra note 48.

[178] *See Data Protection Laws of the World Handbook* (Cameron Craig, Paul McCormack, Jim Halpert, Kate Lucente, and Arthur Cheuk of DLA Piper, eds., 2012), http://www.edrm.net/resources/data-privacy-protection/data-protection-laws.

[179] *Id.* at 23–26.

Indeed, foreign data laws such as the European Union's (EU) Data Protection Directive, directly conflict with ESI disclosure obligations that are otherwise required pursuant to the Fed. R. Civ. P.[180] Under some circumstances, the failure to adhere to foreign data laws could lead to criminal prosecution. For example, a violation of the German Federal Data Protection Act (BDSG), drafted to comply with the EU's Data Protection directive, makes disclosure of information protected by the German BDSG a criminal offense carrying substantial fines and/or jail terms.[181]

As discussed above, a responding party can find itself in a Catch-22 where it must collect and produce Documents and ESI pursuant to United States law but doing so would be impermissible and perhaps a crime in foreign jurisdictions. For this reason, courts evaluating possession, custody, and control in cases involving cross-border corporate families or in which Documents and ESI are otherwise protected by international laws should defer to international data privacy and blocking statutes by which a litigant may also be bound.

Principle 5: *If a party responding to a specifically tailored request for Documents or ESI (either prior to or during litigation), does not have actual possession or the legal right to obtain the Documents or ESI that are specifically requested by their adversary because they are in the "possession, custody, or control" of a third party, it should, in a reasonably timely manner, so notify the requesting party to enable the requesting party to obtain the*

[180] *See* Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC); http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[181] *See, e.g.*, *In re* Vitamins Antitrust Litig., No. 99-197TFH, 2001 WL 1049433 (D.D.C. June 20, 2001).

Documents or ESI from the third party. If the responding party so notifies the requesting party, absent extraordinary circumstances, the responding party should not be sanctioned or otherwise held liable for the third party's failure to preserve the Documents or ESI.

Comment:

As discussed throughout this Commentary, there are various situations in which a responding party does not own or "control" the Documents or ESI that have been requested, and instead is claiming that such Documents and ESI are in the hands of a third party.

For example, an employer may become aware that a custodian used a dual-use/BYOD personal device, personal webmail, or a personal social media account to communicate about the facts underlying the lawsuit and those sources may contain relevant information. The employer, however, does not have Rule 34 "control" as espoused by this Commentary. In accordance with the Legal Right Plus Notification Standard, a responding party claiming it does not own or "control" relevant Documents and ESI is required to timely notify the requesting party,[182] which allows the requesting party the opportunity to obtain those Documents and ESI from the third party.

From a practical standpoint, this approach enables the requesting party, who has the greatest need and incentive to preserve the information, to learn about the existence of the data at around the same time as the responding party, and to have the same ability as the responding party to take steps to attempt to preserve or obtain access to the Documents or ESI from third parties through subpoenas or other mechanisms. If a responding party complies with its notice obligations, it should not be

[182] Charter Oak Fire Insurance Co. v. Marlow Liquors, 908 F. Supp. 2d 673, 679 (D. Md. 2012) (citing Silvestri v. Gen. Motors Corp., 271 F.3d 583, 591 (4th Cir. 2001)).

sanctioned if third parties do not cooperate with preservation or production efforts.

The concept of this Principle applies to pre-litigation demands for preservation as well, thus the language "either prior to or during litigation."

Moreover, similar to the discussion in the comment to Principle 2, this Principle is also not intended to imply a general duty for a responding party to identify Documents and ESI that might be relevant in a case that are not within a party's possession, custody, or control. Instead, it only applies to Documents and ESI that are "specifically requested," in accordance with the general mandates of Rule 34.[183] Stated another way, this Principle does not apply unless and until the requesting party has met its burden to be as specific as possible when requesting information in discovery or making pre-litigation preservation demands.

[183] *See supra* note 133.

TAR 1 Reference Model: An Established Framework Unifying Traditional and GenAI Approaches to Technology-Assisted Review

Tara Emory, Jeremy Pickens, and Wilzette Louis[1]

Table of Contents

A. Introduction 110

B. TAR and GenAI 112

C. TAR 1 Reference Model 117

D. Workflows for Discriminative TAR 1 and GenAI TAR 1, Compared 119

E. Considerations for GenAI versus Discriminative Algorithms in TAR 1 129

F. Hybrid Workflows: Mixing Algorithms 134

G. Conclusion 136

[1] At Redgrave Data, Tara Emory is Senior Vice President of Legal AI Strategy and General Counsel; Jeremy Pickens is Head of Applied Science; and Wilzette Louis is Director of Client Solutions. Thanks to our colleagues Dave Lewis, Mike Kearney, France Jaffe, and Rees Crosby, and to Nick Snavely of Redgrave LLP, for their contributions to this article.

A. INTRODUCTION

In eDiscovery, Generative Artificial Intelligence (GenAI) in the form of Large Language Models (LLMs) may offer more efficient approaches for many tasks, including document review. GenAI algorithms can be used similarly to traditional machine-learning algorithms for this purpose, through a process involving iterative training, sampling, and statistics.

In large matters, different aspects of document review are often divided into different workflows and teams. These workflows often begin with a "first-pass review" in which documents are tagged so they can be easily managed into other workflows (e.g., production or substantive review). Many workflow options exist in which human review teams handle the tagging of documents. When that human effort is alternatively replaced with machine tagging, it is accomplished through a form of Technology-Assisted Review (TAR) known as TAR 1, a workflow that involves tagging documents through the use of predictive algorithms. TAR 1 is applicable to GenAI review when it is used for first-pass review.

GenAI is promising as a new solution and will be a useful approach if it proves to be at least as effective as the options of human review or traditional TAR 1, and comparable in time and costs required. In addition, GenAI's potential to also perform other tasks that are traditionally done after first-level review, such as privilege review or summarization, may further save on costs and time.

The steps of TAR 1 (referred to interchangeably as both a process and a workflow) involve building a predictive model and then demonstrating its effectiveness. These steps ensure that the practitioners who use it are successful in their goals and confident in the outcome. GenAI can be used for first-level review in place of the discriminative machine-learning algorithms that have traditionally been used in TAR 1. Therefore, other than substituting a new algorithm, the conceptual steps of a TAR 1 process are essentially identical, regardless of which type of predictive algorithm is used. In order to facilitate successful outcomes, GenAI as a predictive algorithm needs to be wrapped in a process known to be familiar, reasonable, effective, and defensible by practitioners doing machine tagging for first-pass review: TAR 1.

We provide a reference model to serve as a foundation for first-pass workflows that use artificial intelligence/machine learning to integrate them into the established process of TAR 1. We also provide diagrams of the tasks within the steps of the reference model for discriminative TAR 1 (TAR 1 using discriminative algorithms) and GenAI TAR 1 (TAR 1 using generative AI algorithms) to demonstrate their similarities and differences. One can view predictive algorithms as engines, while the TAR 1 process is a vehicle. The engines may vary, but the steering, seating, wheels, and other key features of the vehicle are unchanged. To understand what engine to use for different goals, empirical studies are needed on comparative benefits in terms of time, cost, effectiveness, consistency, and other metrics of interest. The TAR 1 reference model may guide those studies, and help practitioners understand the similarities and differences between TAR 1 workflows using traditional discriminative algorithms and those using GenAI.

B. TAR AND GENAI

1. TAR

Coined by Maura Grossman and Gordon Cormack, TAR was defined in the Grossman-Cormack Glossary of Technology-Assisted Review:[2]

> **Technology-Assisted Review (TAR)**: A process for Prioritizing or Coding a Collection of Documents using a computerized system that harnesses human judgments of one or more Subject Matter Expert(s) on a smaller set of Documents and then extrapolates those judgments to the remaining Document Collection. Some TAR methods use Machine Learning Algorithms to distinguish Relevant from Non-Relevant Documents, based on Training Examples Coded as Relevant or Non-Relevant by the Subject Matter Experts(s), while other TAR methods derive systematic Rules that emulate the expert(s)' decision-making process. TAR processes generally incorporate Statistical Models and/or Sampling techniques to guide the process and to measure overall system effectiveness.

As made clear in this definition, TAR is a process that (a) uses subject-matter experts to (b) train a computerized system (algorithm) to make predictions and (c) guides both the training and the results of that process via sampling and various kinds of statistics.[3]

[2] Maura R. Grossman and Gordon V. Cormack, *The Grossman-Cormack Glossary of Technology-Assisted Review*, 2013 FED. CTS. L. REV. 7 (January 2013).

[3] Note also that not all prediction engines are discriminative supervised machine learning, or even supervised machine learning, as articulated in the TAR definition. For example, expert systems are not supervised machine

Most currently available TAR implementations utilize supervised machine learning, more specifically discriminative supervised machine learning, as the prediction engine. A supervised machine-learning algorithm takes human-labeled data (e.g., documents that the human has coded responsive or not responsive[4]) as input, and the machine learns a function that makes predictions on untagged documents. The term "discriminative" refers to a specific kind of predictive algorithm that separates, or discriminates, between positive and negative labels. Common examples of discriminative algorithms used in TAR include support vector machine classifiers and logistic regression classifiers. A myriad of TAR workflows exist, and parties may use different ones to meet different goals. While variations and hybrid approaches exist, TAR 1[5] and TAR 2[6] often describe the most common general approaches.

learning in that they do not learn a predictive function from data. Rather, humans derive If-Then rules for the machine to follow, with rules mimicking the types of decisions that an expert would make. A typical eDiscovery workflow involves humans examining documents from a project to learn about their contents, then writing and refining rules, and then testing and measuring the rules' performance. Once a set of rules is fixed, the machine then applies the rules to extrapolate predictions onto untagged documents. This expert systems workflow bears much similarity to the way GenAI is used in TAR, particularly with how the efforts of the human and the machine are divided.

[4] While responsiveness (to document requests in discovery) and relevance (to a matter or topic) differ in meaning, they are often used interchangeably in eDiscovery discussions, and our use of one or the other is not intended to be significant in this article.

[5] TAR 1 is also known as SAL (Simple Active Learning) and SPL (Simple Passive Learning), and as "two-stage TAR," wherein training and review are two separate activities. Humans iteratively train a model for a finite number of steps, and then the model labels the remainder of the documents.

[6] TAR 2 is also known as CAL (Continuous Active Learning™), as well as "one-stage TAR," wherein training and review are the same activity. In

2. GenAI

GenAI, in the form of Large Language Models, is based on deep learning models that have been trained on enormous amounts of text from which they have learned how to predict the next words in a given sequence based on a "prompt." They do not discriminate between classes; rather, they sequentially generate words probabilistically. By itself, an LLM is not a supervised machine learning model; it only does next-word prediction. Suppose, however, that the LLM is fed with the following word sequence:

> I am looking for information about cows. Here is the text of a document: "The farmer went to his barn to put out square bales for the bovines." Is this text relevant to my information need? Please answer yes or no.

The combination of the prompt with the LLM in essence becomes a (generative) supervised machine learning classifier.[7] The instructions to the LLM about the nature of information being sought (cows), combined with the document for which a prediction is desired, plus instructions about the text to generate, form the supervision. The LLM generates text that serves as a prediction. The length of the generated text may be short, but the LLM is nonetheless generative rather than discriminative. While it should most of the time respond with "yes" or "no" as instructed, it selects its response from limitless options, so there

TAR 2, humans tag the documents, and the model is updated continuously to include the new examples they have tagged.

[7] Specifically, this kind of supervised machine learning is known as "zero shot learning," because the LLM can make predictions about a class of interest (responsive or not responsive to an issue) from a straightforward natural language description of that issue, rather than from labeled training documents.

is also some probability of generating other responses, e.g., "giraffe." All instances of "yes" can be considered responsive and "no" can be considered not responsive. All instances of anything else can either be considered either not responsive or a non-answer (failure to predict) that indicates a need for further review.[8] In this manner, the LLM becomes capable of extrapolating onto untagged documents based on a human-written description of relevant information.

In eDiscovery, GenAI may additionally be used in many other ways, including but not limited to summarizing documents, answering questions, giving explanations, extracting key information, identifying personal information, identifying and reviewing foreign language documents, and privilege logging. This article discusses using GenAI for document review in eDiscovery, specifically, its capability to assist in first-pass review by tagging documents based on its predictions.

3. TAR 1

This article analyzes the TAR 1 workflow to provide a unified lens through which to understand its application regarding different kinds of predictive engines. TAR 1 is a form of TAR in which the machine predictively tags the documents in the project population in two sequential stages: build the model, then classify the population. Its most frequent application is facilitating the selection of documents that are most likely responsive for compliance with production requirements. It generally aims for efficiency by reducing the amount of effort needed to build the predictive model while maximizing the effectiveness (precision and recall) of the predictions. It involves building a model

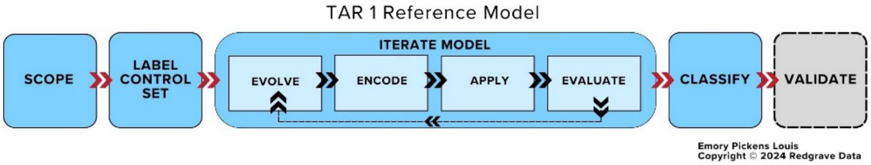
[8] The LLM can be asked to generate rankable categories as well, such as "super tippy top relevant," "highly relevant," "relevant," "not so relevant," and "not even close," with cutoffs drawn at different points. There are many possibilities, but the principle remains the same.

to classify the project document population, and then tagging that population (e.g., responsive or not responsive). The project document population, with predicted tags applied, can then be filtered for other tasks, such as selecting documents predicted responsive for production. Therefore, TAR 1 is usually cost-effective and quick compared to workflow options that require human review to tag documents.

While largely bypassing human first-pass review with TAR 1 can greatly save on costs and time, at least for its most common purpose of production compliance, it also introduces certain risks. It will inevitably predictively tag as responsive documents that are not, potentially risking unnecessarily revealing some confidential or sensitive information in productions, and even may risk possible challenges by other parties for overproduction. While complementary workflows are carried out to search for, review, and withhold or redact certain documents (e.g., privileged or personal information), some documents containing such information may be missed if they do not contain the criteria used to create those workflows, like keywords. Therefore, TAR 1-based productions can also risk the inclusion of such information. Furthermore, whereas first-pass human reviewers can tag documents and often identify and communicate insights about the documents for the case team, TAR 1 only tags documents.

C. TAR 1 REFERENCE MODEL

The TAR 1 Reference Model depicts the established, defensible TAR 1 process, in which the effectiveness of the result is measured through sampling and statistics. These five steps of 1) **Scope**, 2) **Label Control Set**, 3) **Iterate Model**, 4) **Classify**, and 5) **Validate** apply regardless of the algorithm used to predict a responsiveness tag, whether that is the traditionally used discriminative algorithms, GenAI, expert systems, or any number of other predictive techniques.



Reprinted with permission from Redgrave Data. Click on graphic for expanded view.

The steps of TAR 1 are:

1. **Scope:** Assemble the project document population and establish the definition of responsiveness
2. **Label Control Set:** Tag a random document sample to estimate the effectiveness of model predictions
3. **Iterate Model:** Create and improve a model to predict responsiveness
   a. **Evolve** the selection of information that will be used to improve prediction
   b. **Encode** the improved information into the model
   c. **Apply** the model to the control set
   d. **Evaluate** the model's performance on the control set to determine whether to continue or exit the model iteration loop
4. **Classify:** Apply the completed model to the untagged project document population to classify each document as responsive or not responsive

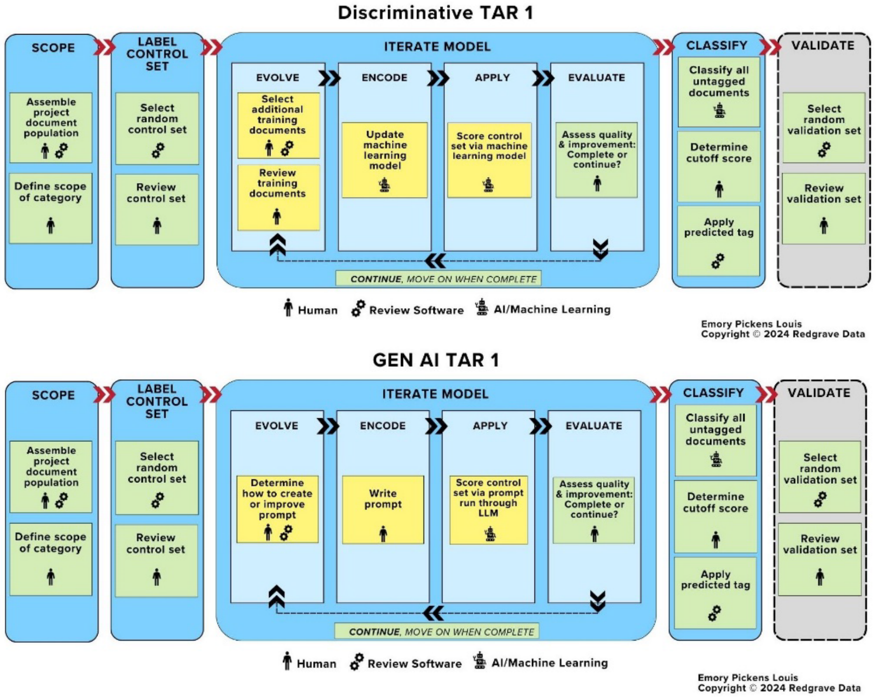
5. **Validate (optional):** Additional testing of the classified documents further evaluates the result

These steps reflect the TAR 1 process standard in eDiscovery. Its structure has enabled practitioners to efficiently and successfully use machine learning, expert systems, and now GenAI, to tag documents in a first-pass review, with metrics capable of demonstrating that the results meet requirements of reasonableness and proportionality. The conceptual steps of this TAR 1 reference model are not literal descriptions of every possible variation, and practitioners occasionally introduce slight modifications, without departing from core concepts.[9] At its essence, the steps of the TAR 1 Reference Model determine whether iterations are productive and improve the model, and whether the model's predictions are reasonably effective.

[9] For example, one practice is to move the **Label Control Set** step into the **Iterate Model** step. In this minor variation, after each **Iterate Model** round, a new set of control documents are selected and reviewed, while the prior round's documents are used in the **Evolve** and **Encode** steps. For traditional discriminative TAR 1, this approach was initially used in some workflows. However, random samples (large enough to create sufficient certainty of model improvement) could be more efficiently taken and reused as controls sets, while active learning rather than random sampling during Model Iteration became preferred as a more efficient training approach.

D. WORKFLOWS FOR DISCRIMINATIVE TAR 1 AND GENAI TAR 1, COMPARED

The TAR 1 Reference Model illustrates a general TAR 1 workflow, which can involve different underlying algorithms. From this general model we can derive specific workflow diagrams for the tasks entailed when using traditional discriminative prediction engines versus when using GenAI.


Discriminative TAR 1
SCOPE
Assemble project document population
Define scope of category
LABEL CONTROL SET
Select random control set
Review control set
ITERATE MODEL
EVOLVE
Select additional training documents
Review training documents
ENCODE
Update machine learning model
APPLY
Score control set via machine learning model
EVALUATE
Assess quality & improvement: Complete or continue?
CONTINUE, MOVE ON WHEN COMPLETE
CLASSIFY
Classify all untagged documents
Determine cutoff score
Apply predicted tag
VALIDATE
Select random validation set
Review validation set
Human
Review Software
AI/Machine Learning
Emory Pickens Louis
Copyright © 2024 Redgrave Data
GEN AI TAR 1
SCOPE
Assemble project document population
Define scope of category
LABEL CONTROL SET
Select random control set
Review control set
ITERATE MODEL
EVOLVE
Determine how to create or improve prompt
ENCODE
Write prompt
APPLY
Score control set via prompt run through LLM
EVALUATE
Assess quality & improvement: Complete or continue?
CONTINUE, MOVE ON WHEN COMPLETE
CLASSIFY
Classify all untagged documents
Determine cutoff score
Apply predicted tag
VALIDATE
Select random validation set
Review validation set
Human
Review Software
AI/Machine Learning
Emory Pickens Louis
Copyright © 2024 Redgrave Data

Images reprinted with permission from Redgrave Data. Click on graphics for expanded view.

Through the reference model, the above workflow diagrams compare and contrast the tasks for workflows using traditional discriminative algorithms in discriminative TAR 1, and GenAI in GenAI TAR 1. The workflows are nearly identical; matching task boxes in the diagram are green to demonstrate consistency. They differ only in the **Iterate Model** steps of **Evolve**, **Encode**, and **Apply**, which we show with yellow task boxes, though the different approaches still accomplish the same five steps of the Reference Model. For convenience, we discuss these steps below in context of a responsiveness review, although TAR 1 can be used for other purposes.

Same

Step 1: Scope:

The project document set is assembled, and the scope of responsiveness is established. This step ensures that any subsequent human tagging or work done on the control set or the predictive model reflects substantive and statistical requirements to guide model iteration and prediction quality. If the responsiveness scope or project population changes after the project has begun, both the predictions and measurements may become incorrect and misleading.

Assemble project document population: The document set for the TAR review project should be selected.

Define scope of category: Attorneys determine the scope of responsiveness, defining each relevant issue or topic to be incorporated as responsive. The scope may be shaped by procedural requirements, facts known about the case, and requests for production. It is different from the document review protocol, which is based on the defined scope of responsiveness. While document review protocols may be adjusted for clarity and effectiveness, the scope of responsiveness should remain the same throughout a TAR project.

Same

Step 2: Label Control Set:

The control set in a TAR 1 review functions as a test to estimate the predictive model's performance.[10]

<u>Select random control set</u>: A random population sample is selected from the TAR project population as a control set and remains independent from the training process. This sample provides an unbiased estimate of model effectiveness during the **Iterate Model** step. The larger the sample, the higher the confidence will be that the model's result for the control set is similar to its result on the entire review population. To ensure a model will be built that produces effective predictions on the general review population, the documents in that control set and any information directly gleaned (either by machine or by human) from those documents must not influence the Evolve step during **Iterate Model**.

<u>Review control set</u>: The control set undergoes human review. The tags of responsive or not responsive applied by the human reviewer will be compared to the model's predictions.

[10] Control sets are a tool for the reviewing party to determine when proportionality considerations can limit their need to continue iterating the model to achieve better results. Control sets may not always be necessary, if a final validation demonstrates that the model was so effective as to leave little room for improvement through further iteration and make such efforts disproportional to potential benefits. Nevertheless, the purpose of the control set is to dramatically increase the probability that the final validation will be a success, so there is a chicken-egg consideration at play.

≠ Different

Step 3: Iterate Model:

A process loop is used to build a model that will predict the responsiveness of untagged documents. The **Iterate Model** step involves four sub-steps: a) **Evolve**, b) **Encode**, c) **Apply**, and d) **Evaluate**.

Other than excluding control set documents from the **Evolve** step, the TAR 1 training process is unrestricted on how and why documents and other information are selected, though practitioners should be mindful that some techniques will be more effective than others. Once the actual model building takes place, the model is then tested by applying it to the control set documents to estimate precision and recall of the results, and improvement (or lack thereof) compared to prior iterations. Then, a decision can be made about whether to continue iterating.

≠ **a.** **Evolve:** This step involves improving the selection of information used to update a model's predictions.

Discriminative TAR 1

GenAI TAR 1

Select additional training documents: Training documents are added as examples. Modern approaches to discriminative TAR 1 usually focus on selecting documents that will increase diversity (representativeness) of the examples or decrease uncertainty in areas where the model is most unsure. Examples can be selected in other ways, such as through random sampling or by human determination.

Review training documents: The new training documents are then reviewed and tagged by humans. This process may require a decent volume of training document review.

Determine how to create or improve prompt: A natural language prompt must be developed for the LLM. For an initial prompt, the prompt writer will need to consider the scope of responsiveness and information known about the document population to design the writing of an effective prompt. The writer needs to plan on how to instruct the system to analyze documents and determine responsiveness. The review software will typically specify the format for the LLM outputs (and automatically include those as part of the instructions to the LLM in the Apply step). For subsequent iterations, sources of information for potential improvements must be considered.[11] This

[11] The work division between an LLM and humans in GenAI TAR 1 closely tracks that for expert systems, in which humans write "If-Then" rules for the machine. In place of If-Then rules, however, humans write natural-language, instructional prompts for the LLM. Both involve training the human, so the human can learn to write rules or a prompt to improve the model. For GenAI TAR 1 (and what we might call Expert Systems TAR 1), this occurs in the **Evolve** step. In contrast, discriminative TAR 1 trains the machine rather than the human, in the **Encode** step.

selection process is performed by a human, optionally assisted by machine-learning and information-retrieval algorithms. Example sources for prompt development can include custodial interviews and review of project documents (except those in the control set). The prompt writer should not be the same person who reviewed control documents or be exposed to information from the control set's contents, to avoid contaminating the objectivity and correctness of the control set.

b. **Encode:** The evolved information is incorporated into the model.

Update machine learning model: Using all training documents reviewed, the machine-learning algorithm updates the model, i.e. the machine learns.

Write prompt: Using the new information about how to improve a prompt that the human has now learned, the human rewrites the prompt.

c. **Apply:** The updated model makes predictions on the control set.

Score control set via machine learning model: A machine-learning algorithm uses the updated model to score the control set documents.

Score control set via prompt run through LLM: An LLM uses the prompt to generate a response for each control set document. The LLM's generative responses are then converted to scores or classifications.[12]

2. **Evaluate**: The model's performance is evaluated and a determination is made to complete or continue the Iterate Model loop.

Assess quality and improvement, and complete or continue: The control set scores are used to measure the quality of the model's predictions, typically with metrics of recall and precision.[13]

[12] While not reflected in the diagram, review software will generally also submit its own instructions to the LLM to accompany the human's prompt, directing the LLM to provide responses in a format that the software can then map to classify each document. This will also be the case when the prompt is submitted in the **Classify** step.

[13] Within a TAR workflow, recall is the percentage of all responsive documents found, out of all responsive documents in the project population. Precision in this context is the percentage of documents classified as responsive by the process that are actually responsive. *See The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition*, 21 SEDONA CONF. J. 263, 360–61 (2020) (citing The Sedona Conference, *Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, 15 SEDONA CONF. J. 217 (2014) ("When describing search results, recall is the number of documents retrieved from a search divided by all of the responsive documents in a collection. For example, in a search for documents relevant to a document request, it is the percentage of documents returned compared against all documents that should have been returned and exist in the data set"); *Id*. at 354, ("When describing search results, precision is the number of true positives retrieved from a search divided by the total number of results returned. For example, in a search for documents

That quality is also compared to prior iterations to measure the extent of the model's improvement. Humans decide whether to continue the model iteration loop or complete it, based on whether the results are satisfactory, and the burden of additional model iteration loops is likely to outweigh benefits of continuing this process.

Step 4: Classify:

Same

The built model is applied to the "real world" of the general project document population to predict responsiveness.

🤖 Classify all untagged documents: The completed model is run on all untagged documents to predict responsiveness. While this step is the same for both algorithms, the execution will be a little different. Discriminative TAR 1 algorithms' model will calculate a score (probability of responsiveness) for each document, while GenAI TAR 1 involves receiving a generated string of text from the prompt-fed LLM, which is then mapped to classification or to gradated scores. In traditional TAR 1 workflows using discriminative models, this step is commonly, but not necessarily, done at the same time as **Apply** in **Iterate Model.**

🧍 Determine cutoff score: For systems that predict with a score, whether discriminatively or

relevant to a document request, it is the percentage of documents returned that are actually relevant to the request").

generatively, a human determines the cutoff point. Based on the metrics of recall and precision from the control set, certain scores or predicted categories of documents can reasonably and defensibly be tagged responsive, and others not responsive. The higher the recall of the selected cutoff point, the more documents will be included, and the lower precision will be. When TAR 1 is used for production purposes, the cutoff point may be determined based on a legal requirement to meet a certain recall level (such as through a stipulated TAR protocol) or proportionality considerations of the value and burden of using different cutoff points.

⚙ <u>Apply predicted label to documents</u>: Based on the determined cutoff or predicted classification, the TAR software labels documents as responsive or not responsive.

Step 5: Validate (optional):

Same

Additional sampling tests, through precision and recall, whether the model's extrapolation to the project population is as effective as was expected based on the control set. It validates the result rather than the model, which can eliminate subtle biases that may be introduced by repeated control set evaluation. However, this has historically not been standard practice in eDiscovery.

⚙ <u>Select random validation set</u>: A random population sample is selected from the document set that was classified by the model.

🧍 <u>Review validation set</u>: The validation set undergoes human review. The tags of responsive or not responsive applied by the human reviewer are compared to the tags applied by the model to assess the results of the TAR 1 process.

E. CONSIDERATIONS FOR GENAI VERSUS DISCRIMINATIVE ALGORITHMS IN TAR 1

GenAI TAR 1 introduces promising advantages that could make it an important tool for eDiscovery practitioners. Studies are needed in several areas to assist practitioners in evaluating whether and when to select GenAI TAR 1, discriminative TAR 1, other workflows, or even hybrid approaches that blend GenAI TAR 1 with other workflow options. This field is still in the early stages of evaluation. Initial studies have tested the effectiveness of GenAI predictions for document tagging in various ways, including against humans, against discriminative algorithms, and against other LLMs.[14] There are not yet studies comparing fully iterated TAR 1 workflows using GenAI versus using discriminative algorithms, though they will surely come in time. Specific issues for study, and that practitioners should consider to decide what will best serve their needs, should include 1) precision and recall, 2) risk of sensitive information

[14] *See* ROSHANAK OMRANI, ET AL., BEYOND THE BAR: GENERATIVE AI AS A TRANSFORMATIVE COMPONENT IN LEGAL DOCUMENT REVIEW, Relativity and Redgrave Data (Feb. 2024) (comparing to manual review); Colleen M. Kenney, Matt S. Jackson & Robert D. Keeling, *Replacing Attorney Review? Sidley's Experimental Assessment of GPT-4's Performance in Document Review*, THE AMERICAN LAWYER, https://www.law.com/americanlawyer/2023/12/13/replacing-attorney-review-sidleys-experimental-assessment-of-gpt-4s-performance-in-document-review/?slreturn=20240204151012 (Dec. 13, 2023) (comparing to manual review); SUMIT PAI, ET AL., EXPLORATION OF OPEN LARGE LANGUAGE MODELS FOR EDISCOVERY, Proceedings of the Natural Legal Language Processing Workshop (Dec. 2023) (comparing different LLMs), *available at* https://aclanthology.org/2023.nllp-1.17.pdf; JASON R. BARON, NATHANIEL W. ROLLINGS & DOUGLAS W. OARD, USING CHATGPT FOR THE FOIA EXEMPTION 5 DELIBERATIVE PROCESS PRIVILEGE, Proceedings of the Third International Workshop on Artificial Intelligence and Intelligent Assistance for Legal Professionals in the Digital Workplace (June 2023) (comparing discriminative and LLM performance for FOIA deliberative process privilege analysis), *available at* https://ceur-ws.org/Vol-3423/paper4.pdf.

disclosure, 3) knowledge gain and accomplishment of related tasks, 4) total project cost, 5) total project time, 6) ease of use, and 7) whether different algorithms may best serve different needs.

1. **Recall and precision:** Precision concerns may be somewhat alleviated if either GenAI TAR 1 or discriminative TAR 1 is found to be more precise than the other at similar defensible recall levels.[15] Use of TAR 1 has been limited in part because when human review is skipped and documents that are predicted responsive are then produced, significant numbers of not-responsive documents are often included. This limitation may resolve if GenAI can reduce that risk by achieving higher precision (fewer nonresponsive documents in the production set) at the same or higher recall rates (finding as many or more responsive documents) compared to discriminative TAR 1.[16] On the other hand, unlike discriminative TAR 1, GenAI TAR 1 may only classify at a few gradations of responsiveness, which may require selection of cutoff points with lower-than-desired responsiveness in some cases.[17]

[15] To the extent even higher recall may be achieved with GenAI with high precision, burdens of producing at higher recall levels may be reduced and create a win-win in which producing parties may face less risk while producing even more responsive documents to receiving parties, as compared to current industry practices.

[16] Metrics are essential to determining effectiveness of any process, including GenAI. Although some practitioners may be more accepting of GenAI TAR 1 than discriminative TAR 1 because GenAI can "explain" its decisions, those decisions are also predictive text and do not inherently give credibility to its classification predictions.

[17] Discriminative algorithms produce real-valued scores that allow very fine gradations that often can near-uniquely rank all documents in the project population, from those predicted most to least responsive. This facilitates

2. **Sensitive information:** Another hesitation for traditional TAR 1 workflows has been the risk of sensitive information disclosure, such as privileged or personal information, when it is used to produce documents without human review. While this risk is mostly managed with additional workflows, such as keyword screens for privileged information with human review, it is always possible that important information was missed. But, in addition to predicting documents as responsive or not during a TAR 1 workflow, GenAI may simultaneously also be able to identify confidential and sensitive information, saving costs and time, if it can do so with similar effectiveness as traditional approaches.
3. **Knowledge gain and multitasking:** Because TAR 1 applies tags without human review, it is known to do little for case teams in terms of gaining knowledge and insights about the documents from first-pass reviewers. As discussed, this limitation of TAR 1 may be lessened or overcome, because GenAI can also create summaries and identify key points in documents as it also predicts responsiveness, which may then be useful for case teams. It may be able to simultaneously accomplish other tasks

a practitioner's selection of a cutoff score based on many options with different recall and precision scores (e.g., produce at 75% responsiveness with 55% precision, at 80% responsiveness with 45% precision, or many other options in between). In contrast, if GenAI TAR 1 only classifies documents into a few gradations of responsiveness (e.g., binary as responsive or not, or on a small scale), practitioners may have to choose between a cutoff point with very high recall and low precision, or low recall and higher precision, with no choices in between. For example, given a result with few gradations, assume two result points, with one of 50% recall and 90% precision, and the next possible cutoff point option with 98% recall at 25% precision (which may contain the vast majority of the review population). With no options in between, one may be faced with only two unhelpful choices.

discriminative TAR 1 does not, further saving time and costs over those workflows, such as identifying privileged material and personal information, identifying and reviewing foreign language documents, and privilege logging. It remains to be seen whether such additional uses of GenAI in conjunction with predictive uses can be deployed in ways that make it more useful and cost effective than human first-pass review.

4. **<u>Costs</u>:** Total costs of GenAI TAR 1, including direct costs of the tool as well as attorney (prompt iteration) and litigation support costs, need to be evaluated against other options. Currently, compared to discriminative algorithm use, each document reviewed by GenAI will be at a considerably higher cost. In many cases, discriminative TAR models can be iterated and applied without limit and without incurring additional costs. In contrast, GenAI is more expensive, and may involve additional costs for every prompt sent and answered in the steps of **Iterate Model** and **Classify**, at least one for every document in the project population. However, GenAI TAR 1 also has the potential to save on costs from attorneys and support staff. Discriminative TAR 1 generally requires training with several thousand documents that are often, though not necessarily, reviewed by subject-matter expert (high-cost) reviewers. This effort should be compared to the cost of any document review and other efforts that will be required for effective prompt writing and iteration in GenAI TAR 1 .

5. **<u>Time</u>:** The total speed of project completion should be considered, including both human and machine time. Workflows must fit circumstances of case needs and deadlines, so timing matters. Currently, machine time for GenAI TAR 1 is slower than discriminative TAR. However, this will likely improve and may also be offset if the

prompt development process is faster than reviewing training documents for discriminative TAR training, as discussed above. Though again, some review of documents will likely be required during GenAI TAR 1 prompt iteration as well.

6. **Ease of use:** GenAI TAR 1 may be preferred by practitioners if it is easier and more practical to use. To begin with, the process of writing a query may feel more approachable, and not require much instruction to try, as opposed to most discriminative TAR systems. In addition, attorneys generally do not relish reviewing thousands of documents to train discriminative TAR 1, and GenAI may save them this task if prompt writing and development is easier. On the other hand, reviewing documents is not a challenging task, and the comparative ease of successful prompt writing and iteration is still unknown.[18] Some may be dissuaded from GenAI TAR 1 adoption if it presents less certainty of success, costs, and time; this may also be affected by the skill of the prompt writer. In addition, GenAI TAR 1 requires the prompt writer to be a different person than the control set reviewer, and shielded from exposure to the control set, which may limit its practicality for some case teams.
7. **Other considerations:** Practitioners should keep in mind that even studies on the above issues do not guarantee their own project will always have similar results. It may be that different circumstances affect outcomes, such as type of matter, document volumes, nature of responsiveness and issues, case team composition, and other factors.

[18] In some circumstances, it may be easier to recognize whether a document is responsive than it is to describe all aspects of responsiveness.

F. HYBRID WORKFLOWS: MIXING ALGORITHMS

GenAI may be integrated with other eDiscovery tools to yield even more possibilities for TAR 1 and other workflow improvements. Hybrid approaches are already common in eDiscovery workflows generally, with mixtures of machine learning, search terms, conceptual search, and structured (metadata) analytics. The most effective use of GenAI, including but not limited to its application in GenAI TAR 1, may involve integration with other approaches.

In fact, GenAI as used for query responses is already a hybrid of processes, as it often leverages a type of combination workflow known as RAG (Retrieval Augmented Generation). This approach involves a (nongenerative) conceptual search of the query against the document set to find the most closely related documents. Those documents are then fed to the LLM along with the query as a prompt, and the LLM then produces a response based on those documents.

The process of GenAI TAR 1 may similarly benefit from other traditional systems. The process of evolving a prompt may be enhanced by discriminative algorithms, as well as diversity algorithms, which may identify documents that will be most helpful for the prompt writer by expanding their knowledge of "unknown unknowns" in the project population. Additionally, where GenAI TAR 1 predictions may designate large volumes of documents as responsive but only provide limited gradations of responsiveness, traditional discriminative algorithms based on a modicum of training may fill in the gaps by providing within-gradation secondary scores.

Conversely, GenAI used more broadly may be able to generate content useful to assist TAR 1 training for both discriminative and GenAI TAR 1. For example, it could generate search queries to retrieve potentially useful training documents, create synthetic training documents, or tag documents to train a discriminative algorithm. When using GenAI TAR 1, it can help prompt writers evolve their prompts by asking questions to identify and clarify unintended ambiguities in the defined scope of responsiveness.

With GenAI as another tool in the belt of eDiscovery practitioners, new and creative applications will continue to appear. However, novelty must be accompanied by evaluation if it is to become innovation; just because something can be done does not mean it will produce a better outcome than a related, known-effective approach, no matter how plausible the novel idea seems.

G. CONCLUSION

As illustrated in the TAR 1 Reference Model, established and defensible processes for predictively tagging documents through a TAR 1 process follow steps of: 1) **Scope**, 2) **Label Control Set**, 3) **Iterate Model**, 4) **Classify**, and 5) (optionally) **Validate**. While GenAI, in the form of LLMs, offers new possibilities for improving the efficiency and effectiveness of first-pass document review, its use still follows the established steps of TAR 1. This process, which involves sampling and statistics, will help promote successful outcomes on first-pass review projects for practitioners using GenAI — as it has helped those same practitioners when using discriminative approaches.

Especially as GenAI capabilities increase and costs and time it requires go down, GenAI has potential to become a preferred approach to TAR 1, as discussed above. Future studies may demonstrate that GenAI can be a more effective choice. To improve TAR 1 workflows, and relative to discriminative models and not just to linear review, GenAI will need to achieve improved recall and precision, effectively and efficiently incorporate other tasks that go beyond first-pass review, be cost effective and sufficiently fast, and be practical for case teams to use. In addition, the potential to mix GenAI with other algorithms into hybrid approaches may further increase its value in improving first-pass review.

Guided by the structured approach of the TAR 1 Reference Model, practitioners have much to consider in selecting approaches, given the well-known benefits and risks of discriminative TAR 1, the untested but potential capabilities of GenAI TAR 1, and the option to mix algorithms. Approaches to document review may change significantly in some ways with the incorporation of GenAI, but they will also be fundamentally unchanged in others.

THE UBIQUITOUS ROLE OF THE SPECIFIC "INTENT TO DEPRIVE" REQUIREMENT OF AMENDED RULE 37(e)(2)(B)

"The Sedona Conference . . . accurately captures the critical concept." [1]

Thomas Y. Allman[2]

INTRODUCTION

On December 1, 2015, a completely revised Federal Rule of Civil Procedure 37(e) came into effect to provide a single, uniform standard for determining when measures would be available for the irrevocable loss of electronically stored information ("ESI") "that should have been preserved in the anticipation or conduct of litigation." Subdivision (e)(2) of the Amended Rule makes severe measures such as adverse inferences—or curative measures that are tantamount to a sanction—available only when a party has acted with "specific intent" to deprive another party of the use of ESI in the litigation. According to the advisory committee's note, Rule 37(e) "forecloses reliance on

[1] Letter from Bradford A. Berenson, Vice President and Sr. Counsel, Response to the Federal Rules Advisory Committee by the General Electric Company to the Request to Bench, Bar and Public for Comments on Proposed Rules (Aug. 2013), at 11, *available at* https://downloads.regulations.gov/USC-RULES-CV-2013-0002-0599/attachment_1.pdf.

[2] Copyright 2024 Thomas Allman. Tom is Chair Emeritus of Sedona Conference Working Group 1 (WG1) and a former General Counsel. He was a member of the E-Discovery Panel at the 2010 Duke Litigation Conference that advocated development of Amended Rule 37(e). *See, e.g.*, Thomas Y. Allman, *Preservation Rulemaking After the 2010 Litigation Conference*, 11 SEDONA CONF. J. 217, 223 (2010) (concerns about pre-rulemaking authority are "overblown"). The then-current version of Rule 37(e) dealt only with sanctions imposed under the Federal Rules.

inherent authority or state law" to determine when the listed measures should be used.[3]

The "intent to deprive" standard was recommended by the Steering Committee of the Sedona Conference Working Group One ("WG1")[4] during the public comment period as a substitute for the proposed requirement that a party's actions were "willful *or* in bad faith."[5] Sedona proposed a required showing of "specific intent" to deprive another party of relevant material evidence "prior to the imposition of sanctions and/or any curative measure that would be tantamount to a sanction."[6] The Discovery Subcommittee endorsed that approach after the final public hearing in Dallas, Texas.[7] It captures the critical understanding that allowing adverse inferences based on ordinary negligence "was a minority viewpoint that the advisory

[3] Prelitigation variations in the federal approach were "largely the product" of common law regulation via inherent power. A. Benjamin Spencer, *The Preservation Obligation: Regulating and Sanctioning Pre-Litigation Spoliation in Federal Courts*, 79 FORDHAM L. REV. 2005, n.6 (2011) (the time is "ripe" for a uniform federal approach).

[4] Response by The Sedona Conference Working Group 1 Steering Committee to Request to Bench, Bar and Public for Comments on Proposed Rules (Aug. 2013), at 13 (Nov. 26, 2013), *available at* https://downloads.regulations.gov/USC-RULES-CV-2013-0002-0346/attachment_1.pdf [hereinafter Sedona Comment].

[5] It permitted an adverse-inference jury instruction "only" if the party's actions "caused substantial prejudice in the litigation and were willful or in bad faith." Preliminary Proposal, Rule 37(e)(1)(B)(1), Agenda Book, Advisory Committee on Civil Rules (April 10-11, 2014) at 393, *available at* https://www.uscourts.gov/sites/default/files/fr_import/CV2014-04.pdf [hereinafter Agenda Book].

[6] Sedona Comment, *supra* note 4, at 13.

[7] Discovery Subcommittee Meeting Notes, Dallas (Feb. 8, 2014) (discussing Sedona approach that focused on "a specific intent to deprive an opposing party of evidence"), Agenda Book, *supra* note 5, at 405.

committee and the Supreme Court explicitly rejected."[8] The Rules Committee subsequently conceded that the initial proposal was "not the best we can do."[9]

This essay acknowledges and celebrates the ubiquitous nature of the "specific intent" requirement, whether the finding is made by the court or the jury. While most courts decide disputes about intent for themselves, some turn to the jury as "a mechanism for resolving the intent to deprive issue" or as a curative measure under Subdivision (e)(1).[10] While there is a "proper" evidentiary aspect to lost information that does not require such a finding, such a finding is required when there is a plausible risk of overreaction to negligent conduct to ensure that the core policy of the Amended Rule is maintained. It is not beyond the ability of a reasonable jury to fairly process the evidence under those circumstances.

INTENT TO DEPRIVE

Spoliation of evidence involves the intentional, reckless, or negligent destruction, alteration, or failure to preserve evidence that is relevant to ongoing or anticipated litigation. Courts have long admitted evidence tending to show that a party destroyed evidence relevant to the dispute being litigated, permitting an inference (the "spoliation inference") that the destroyed evidence would have been unfavorable to the position of the

[8] Steven Baicker-McKee, *Mountain or Molehill?*, 55 DUQ. L. REV. 307, 323 n.72 (2017).

[9] Minutes, Civil Rules Advisory Committee (April 10-11, 2014) at 18, *available at* https://www.uscourts.gov/sites/default/files/fr_import/CV04-2014-min.pdf.

[10] Doe v. Willis and Swift Trans., Case No. 8:21-cv-1576-VMC-CPT. 2023 WL 2918507, at *15 (M.D. Fla. Apr. 12, 2023).

offending party.[11] If the loss does not result from a "specific motive or intention" to keep information from another party, the "backbone" of the evidentiary logic supporting adverse inferences is lacking.[12] It permits courts and juries to acknowledge "new evidence created by the act of suppression itself," which serves as a "form of compensation in place of what the suppressed evidence would have shown."[13] It can fill in the gaps in proof on the merits.

Because of the Amended Rule, a court or jury may presume that missing ESI was "unfavorable" only if a party acted with an intent to deprive another party of the information's use in the litigation. The crucial element is not whether ESI was intentionally destroyed, but "rather the reason for the destruction."[14] The Rule rejects cases such as *Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99 (2nd Cir. 2002), that authorizes sanctions based on a finding of "negligence or gross negligence."[15] A showing of either "will not do the trick."[16] By clarifying that

[11] Schmid v. Milwaukee Electric Tool, 13 F.3d 76, 78 (3rd Cir. 1994); *see also* Kenneth J. Withers, *Risk Aversion, Risk Management, and the "Overpreservation" Problem in Electronic Discovery*, 64 S.C. L. REV. 537, 547 (2013) (noting role of King's Bench decision in Armory v. Delamirie, (1722) 93 Eng. Rep 664 (K.B.); 1 Strange 506).

[12] The "necessary showing of belief" in a weak case is lacking. John MacArthur Maguire & Robert C. Vincent, *Admissions Implied from Spoliation or Related Conduct*, 45 YALE L. J. 226, 235 (1935).

[13] Dale A. Nance, *Missing Evidence*, 13 CARDOZO L. REV. 831, 876 (1991).

[14] Hunting Energy Servs. v. Kavadas, Case No. 3:15-CV-228 JD, 2018 WL 4539818, at *11 (N.D. Ind. Sept. 20, 2018) (citing Bracey v. Grondin, 712 F.3d 1012, 1019 (7th Cir. 2013).

[15] Committee Note. The First, Second, Sixth, Ninth, and in at least one circumstance, the D.C. circuits had all concluded that negligence could be sufficient. Gregory P. Joseph, *Rule 37(e): The New Law of Electronic Spoliation,* 99 JUDICATURE No. 3, at 1.

[16] Applebaum v. Target Corp., 831 F.3d 740, 745 (6th Cir. 2016).

unintentional destruction of relevant ESI is not sufficient, the Amended Rule is "now aligned" with the Sedona Principles.[17] Courts that permitted adverse inferences for losses under those circumstances now routinely decline to impose such sanctions.[18]

The "intent to deprive" standard is "akin to" requiring a showing of bad faith but is defined "even more precisely."[19] The requirement is satisfied if "the evidence shows, or it is reasonable to infer, that a party purposely destroyed evidence to avoid its litigation obligations."[20] Courts often must rely on circumstantial evidence. The timing of the destruction, the method of deletion, the reason some evidence was preserved, and the existence of institutional policies on preservation can be relevant.[21] A lack of credible explanation for the conduct can be powerful circumstantial evidence that the party acted "with an intent to deprive."[22] In *Skanska USA Civil Southeast v. Bagelheads, Inc.*, for example, there was "no cogent explanation, apart from bad faith" for the "systemic failure to make *any* effort to preserve cell

[17] Thomas Y. Allman, *The Sedona Principles (Third edition): Continuity, Innovation, and Course Corrections*, 51 AKRON L. REV. 889, 913–14 & nn.171 &180 (2017). Principle 14 provides that a breach of duty to preserve ESI may be addressed by "remedial measures, sanctions or both," but sanctions are available only if a party acted with intent to deprive. *Id*. at 918.

[18] John J. Jablonski, *Not-So-New E-Discovery Amendments Are Making A Lasting Impression*, LEGAL BACKGROUNDER, Vol. 35, No. 10 (Apr. 24, 2020).

[19] Advisory Committee on Civil Rules Report to the Standing Committee (May 2, 2014) at 42, *available at* https://www.uscourts.gov/sites/default/files/fr_import/ST2014-05.pdf.

[20] Facebook, Inc. v. OnlineNIC Inc., Case No. 19-CV-07071-SI (SVK), 2022 WL 2289067, at *6 (N.D. Cal. Mar 28, 2022).

[21] Laub v. Horbaczewski, Case No. CV 17-6210-JAK (KS), 2020 WL 9066078 (C.D. Cal. July 22, 2020).

[22] Ala. Aircraft Indus, Inc. v. Boeing Co., 319 F.R.D. 730, 746 (N.D. Ala. 2017) ("blatantly, irresponsible behavior").

phone data" until at least seven months after a litigation hold was in place (emphasis in original). [23]

The intent of corporate parties is determined by a nuanced version of respondeat superior.[24] In *Decker v. Target*, the court concluded that Target had acted with intent to deprive because it had failed to properly instruct the employees who did not retain the missing ESI.[25] In *Moody v. CSX Transportation,* it was the "stunningly derelict" failure of various employees that justified the conclusion that the failure to preserve critical ESI involved an intent to deprive.[26] In *Government Employees Health Association v. Actelion Pharmaceuticals*, however, there was no intent to deprive because it was "just as likely" that the approval of the deletion at issue was the result of "inattention."[27]

MEASURES AVAILABLE[28]

There is a wide spectrum of "measures" available when the predicate requirements of the Amended Rule are met. The ESI must have been irrevocably lost because the party failed to take reasonable steps to preserve ESI that "should have been preserved." A predicate showing of prejudice is also required

[23] 75 F.4th 1290, 1302 (11th Cir. 2023) (affirming bench trial ruling).

[24] Charles Yablon, *Byte Marks: Making Sense of new F.R.C.P. 37(e),* 69 FLA. L. REV. 571, 585, 587 (2017).

[25] Case No. 1:16-cv-00171-JNP-BCW, 2018 WL 4921534, at *4 (D. Utah Oct. 10, 2018) ("Target is the party that destroyed the records").

[26] 271 F. Supp. 3d 410, 425–26, 431–32 (W.D.N.Y. 2017).

[27] 343 F.R.D. 474, 484–85 (D. Md. 2023) (noting that the evidence did not demonstrate by "clear and convincing evidence or even a preponderance of the evidence" that the actions were done with intent to deprive).

[28] The Rules Committee deliberately used the term "measures" to emphasize that spoliation involves a continuum of responses that are not adequately differentiated by labels.

because Rule 37(e) applies only if relevant evidence has been lost.[29] This makes sense for a number of reasons, not the least of which is the lack of prejudice in the loss of irrelevant ESI.[30] To qualify for the very specific and severe measures under Subdivision (e)(2), however, the movant must "additionally show that" the party "acted with an intent to deprive."[31]

SUBDIVISION (e)(2)

When a party has lost ESI while acting with an intent to deprive, Subdivision (e)(2) authorizes severe measures such as permissive or mandatory adverse inference jury instructions as well as dismissals or defaults. A typical permissive jury instruction permits the jury, upon a factual finding by the court of spoliation, to presume that the missing ESI was unfavorable to one party and/or favorable to the other. As the Chair of the Discovery Subcommittee explained, the task involved "is inference, not the rebuttable presumption of evidence law."[32]

In *GN Netcom v. Plantronics*, for example, a jury was instructed that it could "presume that the lost evidence would have been relevant and helpful to GN's case and/or would have been harmful to Plantronics's case." The court had determined that intent to deprive existed since a corporate executive had

[29] Polk v. General Motors LLC, Case No. 3:20-v-549-MMH-LLL, 2024 WL 326624 at *21 (M.D. Fla. Jan. 29, 2024) (because of the prejudice "some sanction or curative measure is warranted").

[30] Snider v. Danfoss, LLC, 15 CV 4748, 2017 WL 2973464, at *4 (N.D. Ill. July 12, 2017).

[31] Su v. U.S. Postal Serv., Case No. 3:23-cv-05007-RJB, 2024 WL 21670, at *4 (W.D. Wash. Jan. 2, 2024).

[32] Minutes, Civil Rules Advisory Committee (April 10-11, 2014) at 24, lines 983–88 988 (quoting remarks of Hon Paul Grimm, Chair of Discovery Subcommittee), *available at* https://www.uscourts.gov/sites/default/files/fr_import/CV04-2014-min.pdf.

deleted an unknown number of emails, urged others to do the same, and the company was unwilling to pay a nominal fee to an expert to fully assess the spoliation.[33] In *Kelley v. BMO Harris Bank*, the court instructed the jury that it could assume that the contents of destroyed email backup tapes would have been adverse or detrimental to BMO.[34]

However, the Committee Note acknowledges that a court may conclude that the "intent finding should be made by a jury."[35] While this includes the predicate finding necessary for dismissals or defaults,[36] the focus is on framing the appropriate instruction for a jury that will be deciding the merits at trial.[37] The Note provides that "the court's instruction should make clear that the jury may infer from the loss of the information that it was unfavorable to the party that lost it only if the jury first finds that the party acted with the intent to deprive another party of the information's use in the litigation."[38]

[33] C.A. No. 12-1318-LPS, 2017 WL 4417810, at *3 (D. Del. Oct. 5, 2017) (Final Instruction), *rev'd on other grounds*, 930 F.3d 76, 89 (3rd Cir. 2019) (excluded expert testimony "could have changed the outcome of the case").

[34] Case No. 19-cv-1756 (WMW), 2023 WL 4145827, at *1 (D. Minn. June 23, 2023) (Jury Instruction No. 9) (Doc. 349, Nov. 8, 2022).

[35] FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

[36] Some courts may choose to delay deciding on whether such measures are available until the jury decides.

[37] The Rules Committees subsequently received a related analysis of the topic that concluded that if the Rule 37 proposal were to preclude the option of submitting factual issues such as culpability to the jury in any capacity, it would "change the way some courts have handled adverse inference instructions in some cases." Memorandum, Andrea L. Kuperman, General Counsel, Rules Committees, Allocating Fact-Finding Roles for Sanctions Imposed Under Inherent Authority, May 9, 2014, at 46 (citing, inter alia, Rimkus Consulting Grp. v. Cammarata, 688 F. Supp.2d 598, 607 (S.D. Tex. 2010).

[38] The Note was updated to conform to the changes in the Amended Rule after the text was finalized.

The court in *DR Distributors v. 21 Century Smoking* explained that relying on the jury is appropriate if there is enough admissible evidence for a reasonable person to conclude that the defendants "intended to destroy this ESI" as well as to find that they did not.[39] Any spoliation-related evidence easily "clears the baseline relevance hurdle to admissibility of Federal Rules of Evidence 401 and 402."[40] The trial judge plays a "limited, screening role."[41] In *Modern Remodeling v. Tripod Holdings*, for example, the court admitted evidence of resetting a laptop and planned to instruct the jury that it could determine if it was done to deprive the other party of the evidence and determine the impact it might have had on the merits of the claims or defenses.[42] The movant must first persuade the jury, however, that the party acted with the intent to deprive the opposing party of the ESI's use in the litigation.[43]

In *Alabama Aircraft Industries v. Boeing*, the Eleventh Circuit agreed that permitting the jury to infer the lost information was unfavorable if it found Boeing deleted it with intent to deprive "correctly stated the law" and did not mislead the jury. It was instructed that it was "for you to decide what force and effect to give it in light of all the evidence in this case," because it was "the judge of the facts as to . . . what happened to these

[39] 513 F. Supp. 3d 839, 981 (N.D. Ill. Jan. 1, 2021).

[40] The Sedona Conference, *Commentary on ESI Evidence and Admissibility, Second Edition*, 22 SEDONA CONF. J. 83, 176 & n.213 (2021).

[41] Joseph, *supra* note 15, at 40.

[42] Civil Action No. CCB-19-1397, 2021 WL 3852323, at *15 (D. Md. Aug. 27, 2021). The jury returned a substantial verdict in favor of the movant after a three-week trial, and the district judge found no basis for a new trial under Rule 59. 2022 WL 21782160 (D. Md. June 10, 2022)

[43] EEOC v. GMRI, Inc., Case No. 15-20561-CIV-LENARD/GOODMAN, 2017 WL 5068372, at *3 (S.D. Fla. Nov. 1, 2017) ("if the jury were to agree" it may infer from the loss of ESI that it was unfavorable).

electronic documents, and why it happened." [44] Panels in the Fourth[45] Fifth,[46] Eighth[47] and Eleventh Circuits[48] have acknowledged appropriate use of this option as have numerous district courts, as is reflected in the decisions collected in Appendix A.

Regardless of whether the court or the jury makes the intent finding, the jury receiving a permissive form of jury instruction is permitted to determine what the absent evidence would show.[49] This involves an exercise of the jury's *discretion* to draw inferences as warranted by the evidence.[50] In *Infogroup v. DatabaseUSA*, the Eighth Circuit agreed that the combination of a permissive inference "with the other evidence" was sufficient for the jury to find the movant had proven the claims at issue.[51] In *In re Google Play Store Antitrust Litigation,*[52] the court opted to give a permissive adverse inference jury instruction rather than impose a case-termination measure because "this antitrust case

[44] Case No. 20-11141, 2022 WL 433457, at *16 n.19 (11th Cir. 2022) (per curiam).

[45] Lee v. Belvac Prod. Mach., Inc., Case No. 20-1805, 2022 WL 4996507, at *3-4 (4th Cir. Oct. 4, 2022) (per curiam).

[46] Van Winkle v. Rogers, 82 F.4th 370 (5th Cir. 2023) (involving loss of tangible evidence).

[47] Infogroup Inc. v. DatabaseLLC, 956 F.3d 1063, 1067 (8th Cir. 2020).

[48] *Alabama Aircraft*, 2022 WL 433457, at *6 & *16 n.19 (11th Cir. Feb. 14, 2022) (per curiam).

[49] Deerpoint Grp., Inc. v. Agrigenix, LLC, Case No. 1:18-cv-00536-AWI-BAM, 2022 WL 16551632, at *22-24 (E.D. Cal. Oct. 31, 2022) (the "precise" wording will be determined by the trial judge).

[50] Arch Ins. Co. v. Broan-NuTone, LLC, 509 F. App'x 453, 459 (6th Cir. 2012) (while the jury has such discretion without it, a permissive jury instruction comes "dressed in the authority of the court, giving it more weight than if merely argued by counsel alone").

[51] 963 F.3d 1063, 1067 (8th Cir. 2020).

[52] 664 F. Supp. 3d 981 (N.D. Cal. 2023).

will not be decided on the basis of lost Chat Communications."[53] Courts are reluctant to shortcut the ability to present the merits of a case unless the pretrial conduct has "clearly and irremediably precluded a fair trial."[54]

SUBDIVISION (e)(1)

Subdivision (e)(1) permits a court, upon finding prejudice to another party from the loss of information, "to order measures no greater than necessary to cure the prejudice" involved. This includes "informing the jury" of the circumstances of the loss, which has become particularly attractive.[55] In *Storey v. Effingham County*, involving carelessness in the handling surveillance videos, the court planned to allow the party to present evidence and argument regarding the failure to preserve and instructed the jury to consider this "along with all the other evidence in the case in making its decision."[56] In *Franklin v. Howard Brown Health Center*, the District Judge planned to allow the parties to present evidence and argument to the jury regarding the failure to preserve evidence and then to consider "appropriate jury instructions" at trial.[57]

[53] Instruction No. 13, Permissive Inference, Case 3:20-cv-05671-JD, Coc. 592, Filed Dec. 6, 2023, at 17.

[54] Saul v. Tivoli Sys., 97 Civ. 2386 (DC)(MHD), 2001 U.S. Dist. LEXIS 9873, at *54-55 (S.D.N.Y. July 17, 2001) (noting the "accepted judicial policy" favoring resolution of cases on their merits and the Seventh Amendment right to a jury trial).

[55] Thomas Y. Allman, *Dealing with Prejudice: How Amended Rule 37(e) Has Refocused ESI Spoliation Measures*, 26 RICH. J.L. & TECH 1, *78, Appendix (2020) (collecting cases).

[56] CV-415-149, 2017 WL 2623775, at *5 (S.D. Ga. June 16, 2017).

[57] Case No. 1:17 C 8376, 2018 WL 5831995, at *1 (Nov. 7, 2018).

Parties typically are permitted to "argue for whatever inference they hope the jury will draw."[58] This includes arguments that the missing ESI "contains information unfavorable" to the party that lost it.[59] The Committee Note also permits the court to instruct the jury that it may consider the evidence of the circumstances of the loss, along with all the other evidence in the case, in making its decisions.[60] In *EPAC Technologies v. Harper-Collins Christian Publishing,* for example, the jury was informed that a party had negligently failed to preserve data that "may have shown" certain information relevant to the merits and that it could "give this whatever weight you deem appropriate as you consider all the evidence presented at trial." The Sixth Circuit approved the instruction because it was no greater than necessary to cure the prejudice. [61]

However, a Court may *not* instruct the jury that it may presume from the loss alone that the missing evidence was unfavorable to the party that lost it.[62] (emphasis added). The jury

[58] Best Value Auto Parts Distribs., Inc. v. Quality Collision Parts, Inc., No. 19-12291, 2021 WL 2201170 at *4 (E.D. Mich. May 31, 2021) ("Let the jury decide"). The court observed that the non-moving party could "argue that the jurors should not draw any inference from his conduct."

[59] Atta v. Cisco Sys., Inc., Civil Action File No. 1:18-cv-1558-CC-JKL, 2020 WL 7384689, at *9 (N.D. Ga. Aug. 3, 2020).

[60] FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

[61] 810 F. App'x 389, 403 (6th Cir. 2020)

[62] FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment (jury instructions are appropriate "to assist [the jury] in its evaluation" other than instructions to which subdivision (e)(2) applies"). *But see* HiQ Labs, Inc. v LinkedIn Corp., 639 F. Supp. 3d 944, 979–80 (N.D. Cal. 2022) and Phoenix Process Equip. Co. v. Capital Equip. & Trading Corp., Civil Action No. 3:16-CV-024-CHB, 2022 WL 3094320, at *18 (W.D. Ky. July 18, 2022), *aff'd* 2022 WL 3088102, at *2 (W.D. Ky. Aug.3, 2022).

may not "attach independent significance" to the lost ESI[63] by authorizing remedies that are *de facto* Rule 37(e)(2) measures.[64] Without a predicate "intent to deprive" finding, the "jury might make an adverse inference on its own from negligent conduct based on the arguments and evidence presented."[65] The Discovery Subcommittee had concluded that "we want to bar a presumption from the loss of information alone, but also to allow inferences from all the evidence, including the failure to preserve."[66]

The Sedona Conference urged that the Amended Rule should require a finding of "specific intent to deprive" *both* when a "sanction" was to be imposed *and/or* if a curative measure was "tantamount" to a sanction.[67] The Discovery Subcommittee agreed[68] and the Committee Note was revised to state:

> "Care must be taken, however, to ensure that curative measures under subdivision (e)(1) do not have the *effect* of measures that are permitted under subdivision (e)(2) only on a finding of intent

[63] Whitesell Corp. v. Electrolux Home Prods., Inc., CV 103-050, 2022WL 3372761, at *5 (S.D. Ga. Aug. 16, 2022) (excluding an argument that was "akin to an adverse inference instruction").

[64] Gov't Emps. Health Ass'n v. Actelion Pharms. Ltd., 343 F.R.D. 474, 487 (D. Md. 2023).

[65] Ariana J. Tadler and Henry J. Kelston, *What You Need to know About the New Rule 37(e),* 52-JAN-TRIAL 20, 24 n.15 (Jan. 2016) (such a result could "undermine" the heightened level of culpability required for adverse inferences).

[66] Discovery Subcommittee Call Notes (Mar. 12, 2014) at 3, Agenda Book, *supra* note 5, 444–45.

[67] Sedona Comment, *supra* note 4, at 13.

[68] Discovery Subcommittee Call Notes (Mar. 4, 2014) at 2-3, Agenda Book, *supra* note 5, 438 (the Note should "make it clear" measures requiring intent to deprive could not be employed as "curative" measure").

> to deprive another party of the lost information's use in the litigation." [69] (emphasis added)

As a result, some courts admonish the jury that it should not "speculate" as to what the ESI might have included or "which party (if any) it might have supported."[70] However, a better approach is to accept the possibility that the jury may choose to draw inferences but make it clear that the jury may infer from the loss of information that it was unfavorable "only if the jury first finds that the party acted" with intent to deprive, as suggested by the Committee Note.[71] That was the path chosen by Judge Johnston in *Hollis v. CEVA Logistics U.S.*, for example, where the jury was instructed:

> "If you decide that CEVA intentionally failed to preserve the video recording of November 28, 2018, to prevent Hollis from using the video recording in this case, you may—but are not required to—presume that the video recording was unfavorable to CEVA. You may then consider your decision regarding the video recording, along with all the other evidence, to decide whether CEVA terminated Hollis because of his race." [72]

"Because of the difficulty to establish intent," the court decided to leave "that determination to the jury" and to instruct the jury that it could consider the circumstances surrounding

[69] FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

[70] Gov't Emps. Health Ass'n v. Actelion Pharms. Ltd., 343 F.R.D. 474, 487 (D. Md. 2023).

[71] FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

[72] 603 F. Supp. 3d 611, 625–26 n.1 (N.D. Ill. 2022) ("The instruction is patterned after the suggested language in the Advisory Committee Notes").

the loss as a curative measure under Subdivision (e)(1).[73] Providing an additional admonition that it could presume the video was unfavorable only if it also found intent to deprive is especially useful when there is a plausible likelihood that the jury may overreact to negligent conduct by drawing adverse inferences. If it concludes that the party acted with intent to deprive after an admonition, however, subdivision (e)(2) is satisfied.[74] A jury should not be "left to roam at large with only its untutored instincts to guide it."[75]

INTENT FACT-FINDING

Rule 37(e)(2) places the responsibility on the *court* to decide if a party has acted with a specific "intent to deprive." The finding "may be made by the court when ruling on a pretrial motion, when presiding at a bench trial, or when deciding whether to give an adverse inference instruction at trial."[76] Some argue that by virtue of "experience and training," courts have superior expertise relative to resolving questions "about the plausibility of excuses" for the failure to produce evidence.[77] Most courts probably agree with the district judge in *Mannion v. Ameri-Can Freight Systems* that "when a party seeks sanctions" under Rule

[73] *Id.* 624 (citing Allman, *supra* note 55, at 64–66). The case was settled after the jury was instructed but before it commenced its deliberations.

[74] MGA Ent., Inc., v. Harris, Case No. 2:20-cv-11548-JVS-AGR, 2023 WL 2628225, at *8 (C.D. Cal. Jan. 5, 2023).

[75] Carter v. Kentucky, 450 U.S. 288, 301, 303 (1981) ("while no judge can prevent jurors from speculating" about a party's motivation, a judge can "use the unique power of the jury instruction to reduce that speculation to a minimum").

[76] FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

[77] Nance, *supra* note 13, at 879.

37(e), the judge "acts as the factfinder concerning any underlying factual disputes."[78]

The Committee Note acknowledges, however, that courts may decide to permit the jury to assess intent and suggests an appropriate form of instruction which is "distinguishable from the typical adverse inference instruction under Rule 37(e)(2)."[79] There was ample precedent for that practice prior to amending the Rule, as noted in Appendix B. A properly instructed jury is just as capable as a judge in setting aside personal preferences when fully informed about the governing legal principles.[80]

The issue is not whether there is a constitutional right to a trial by jury on the predicate findings—there is none[81]—but whether the court considers it appropriate to rely on the jury under the specific circumstances involved.[82] After all, intent is a "prototypical function" of a jury when there is "evidence from which the jury could make such a finding."[83] Juries are as competent as courts to assess the motivation involved in the failure to take reasonable steps to preserve ESI. As noted in *Modern*

[78] CV-17-03262-PHX-DWL, 2020 WL 417492, at *4 (D. Ariz. Jan. 27, 2020) ("judges, not juries" should be the ones deciding whether to impose spoliation sanctions).

[79] Poindexter v. W. Reg. Jail, Civil Action No. 3:18-1511, 2021 WL 1169383, at *4 (S.D.W. Va. Mar. 26, 2021) (the jury may be the "proper factfinder for a spoliation issue in some instances").

[80] Alexandra C. Lahav, *The Jury and Participatory Democracy*, 55 WM. & MARY L. REV. 1029, 1056 (2014).

[81] Rossbach v. Montefiore Med. Ctr., 81 F.4th 124, 138 n.8 (2nd Cir. 2023) ("a motion for sanctions" under Rule 37 does not "implicate the Seventh Amendment's jury trial guarantee.") (collecting cases).

[82] Baicker-McKee, *supra* note 8, at 320 ("while the vast majority" of judges decide the issue, the Seventh Amendment is an "important consideration in deciding whether to involved the jury").

[83] Hunting Energy Servs. v. Kavadas, Case No. 3:15-CV-228 JD, 2018 WL 4539818, at *10-11 (N.D. Ind. Sept. 20, 2018).

Remodeling v. Tripod Holdings, a jury is "perfectly capable of comprehending" for example, what is involved in a laptop reset to factory settings and a cloud-based storage system without the need for expert testimony.[84]

In *Ayers v. Heritage-Chrystal Clean*, the court explained that it did not "believe the fact-finding role on this [intent] issue should be completely taken from the jury."[85] In *Woods v. Scissons,* the court decided it would be best to "allow the determination of intent to be made on a more fully developed evidentiary record" in harmony with the "Advisory Committee Note."[86] In *Amann v. Office of the Utah Attorney General*, the issue of intent "turned on questions of the parties' motives" and witness credibility that could not be separated from the merits.[87] In *Manning v. Safelite Fulfillment*,[88] a district judge relied on the jury because it was "an available option suggested by the Advisory Committee notes to Rule 37(e) and used by other courts where intent to deprive presents a close question."[89]

However, the availability of the option "does not indicate that district courts should freely give [the intent] issue to the

[84] Civil Action No. CCB-19-1397, 2021 WL 5234698, at *4 (D. Md. Nov. 9, 2021)

[85] Case No. 1:20-cv-5076, 2022 WL 2355909, at *5 & n.2 (N.D. Ill. June 1, 2022) (the Court "believes that Ayers intentionally deleted the ESI but does not believe it was done with the intention of depriving [the other party] of the ESI (*i.e.*, it was not done in bad faith")).

[86] No. CV-17-08038-PCT-GMS, 2019 WL 3816727, at *6-7 (D. Ariz. Aug. 14, 2019). *Id.*

[87] Case No. 2:18-cv-00341-JNP-DAO, 2023 WL 7218696, at *8 & n.5 (D. Utah Nov. 2, 2023) (noting "the wisdom" of the jury trial).

[88] 17-2824 (RMB/MJS), 2021 WL 3542808, at *4 (D.N.J. Aug. 11, 2021) (reserving judgment as to sanctions(s) pending the jury's intent finding, quoting process outlined in the Committee Notes).

[89] Mark S. Sidoti and Kevin H. Gilmore, *The Resurgence of Electronic Evidence Spoliation Sanctions*, 333 N.J. LAWYER 28, 33 (Dec. 2021).

jury."[90] It may be unnecessary and counterproductive. Admitting evidence of spoliation in the middle of the trial can be disruptive and confusing, and the court is required to prevent misleading of the jury or permitting undue prejudice.[91] As famously explained in *Waymo v. Uber Technologies*, spoliation testimony should not be allowed "to consume the trial to the point that it becomes a distraction from the merits."[92] There was no reason to involve the jury in *Microvention v. Balt USA* where the party had an "abundant opportunity to present evidence on the issue of intent in the context of a pretrial motion."[93]

CONCLUSION

In keeping with traditional principles, the determination of an appropriate measure for spoliation, if any, is confined to the sound discretion of the trial judge and is assessed on a case-by-case basis. The Advisory Rules Committee was surely correct in adopting The Sedona Conference recommendation that a party must have acted with "specific intent" to deprive before imposing sanctions or permitting use of curative measures "that would be tantamount to a sanction."

[90] Van Winkle v. Rogers, 82 F.4th 370, 379 (carefully stressing that the "need to do so in this case stemmed" from the specific circumstantial evidence regarding the timing of the loss and the inability to explain the reasons for the conduct leading to failure to preserve the highly relevant evidence).

[91] *In re* Delta/Airtran Baggage Fee Antitrust Litig., Civil Action 1:09-md-2089-TCB, 2015 WL 4635729, at *14 (N.D. Ga. Aug. 3, 2015) (excluding evidence of alleged spoliation at trial "under Rule 403 of the Federal Rules of Evidence").

[92] Case No. C 17-00939 WHA, 2018 WL 646701, at *18 (N.D. Cal. Jan. 20, 2018) ("Omnibus Order").

[93] Case No. 8:20-cv-02400-JLS-KES, 2023 WL 7634109, at *1 (C.D. Cal. Nov. 13, 2023).

APPENDIX A

The following decisions involve consideration of the use of conditional forms of adverse inference jury instruction based on or inspired by the "intent to deprive" requirement of Amended Federal Rule of Civil Procedure 37(e) and the 2015 advisory committee's note.

Malibu Media, LLC v. Harrison, Cause No. 1:12-cv-1117-WTL-MJD, 2015 WL 3545250, at *6 (S.D. Ind. June 8, 2015) (citing Seventh Circuit Federal Civil Jury Instruction No. 1.20 Spoliation/Destruction of Evidence).

Epicor Software Corp. v. Alternative Tech. Sols., Inc., Case No.: SACV 13-00448-CJC (JCGx), 2015 WL 12734011, at *2 (C.D. Cal. Dec. 17, 2015).

Evans v. Quintiles Transnational Corp., Civil Action No.:4:13-cv-00987-RBH, 2015 WL 9455580, at *5, *10 (D.S.C. Dec. 23, 2015).

Cahill v. Dart, No. 13-cv-361, 2016 WL 7034139, at *4 (N.D. Ill. Dec. 2, 2016).

Gambrell v. Wilkinson CGR Cahaba Lakes, LLC, No. 2:13-cv-02146-HGD, 2017 WL 1196862, at *6 (N.D. Ala. Mar. 31, 2017).

EEOC v. GMRI, Inc., Case No. 15-20561-CIV-Lenard/Goodman, 2017 WL 5068372, at *31 (S.D. Fla. Nov. 1, 2017).

Spencer v. Lunada Bay Boys, Case No. CV-16-02129-SJO (RAOx), 2017 WL 10518023, at *12 (C.D. Cal. Dec. 13, 2017), *recomm. adopted*, 2018 WL 839862, at *1 (C.D. Cal. Feb. 12, 2018).

Gibson v. Mgmt. & Training Corp., C.A. No. 3:16-CV-624-DPJ-FKB, 2018 WL 736265, at *7 (S.D. Miss. Feb. 6, 2018).

BankDirect Capital Fin., LLC v. Capital Premium Fin., Inc., No. 15 C 10340, 2018 WL 1616725, at *12 (N.D. Ill. April 4, 2018).

Hunting Energy Servs., Inc. v. Kavadas, Case No. 3:15-CV-228 JD, 2018 WL 4539818, at *10–11 (N.D. Ind. Sept. 20, 2018).

Lexpath Techs. Holdings, Inc. v. Welch, 744 F. App'x 74, at n.2 (3rd Cir. July 30, 2018) (alluding to "proper division of fact-finding labor").

Franklin v. Howard Brown Health Ctr., No. 17 C 8376, 2018 WL 4784668, at *7 (N.D. Ill. Oct. 4, 2018), *report and recomm. adopted*, 2018 WL 2018 WL 5831995, at *1 (N.D. Ill. Nov. 7, 2018).

Infogroup, Inc. v. DatabaseUSA.com LLC, No. 18:14-cv-49, 2018 WL 6624217 (D. Neb. Dec 18, 2018), *aff'd* 956 F.3d 1063, 1067 (8th Cir. April 27, 2020).

Sosa v. Carnival Corp., 18-20957-CIV ALTONAGA/CGOODMAN, 2018 WL 6335178 (S.D. Fla. Dec. 4, 2018), *decision confirmed*, 2019 WL 330865, *3, *7 (S.D. Fla. Jan. 25, 2019).

Woulard v. Greenwood Motor Lines, Inc., Civil No. 1:17cv231-HSO-JCG, 2019 WL 3318467, at *5 (S.D. Miss. Feb. 4, 2019).

NuVasive, Inc. v. Kormanis, Case No. 1:18CV282, 2019 WL 1171486, at *13–14 (M.D.N.C. Mar. 13, 2019).

Coan v. Dunne, 602 B.R. 429, 442 (D. Conn. April 16, 2019).

Woods v. Scissons, No. CV-08038-PCT-GMS, 2019 WL 3816727 (D. Ariz. Aug. 14, 2019).

University Accounting Serv., LLC v. Schulton, Case No. 3:18-cv-1486-SI, 2020 WL 2393856, at *22 (D. Ore. May 11, 2020) ("Final Jury Instruction 12B").

Phan v. Costco Wholesale Corp., Case No. 19-cv-05713-YGR, 2020 WL 5074349 (N.D. Cal. Aug. 24, 2020) (utilizing CACI 204).

Aramark Mgmt., LLC v. Borquist, Case No. 8:18-cv-01888-JLS-KESx, 2021 WL 863746 (C.D. Cal. Mar. 8, 2021).

Poindexter v. Western Reg'l Jail, C.A. No. 3:18-1511, 2021 WL 1169383, at *4 (S.D.W. Va. Mar. 26, 2021) (refusing request but acknowledging *Vodesek v. Bayliner*), *vacated in part*, 2021 WL 1169383 (4th Cir. Mar. 26, 2021) (per curiam).

Kadribasic v. Wal-Mart, Inc., Civil Action No. 1:19-cv-03498-SDG, 2021 WL 1207468, at *5 (N.D. Ga. Mar. 30, 2021) (refusing recommendation of magistrate judge that jury decide intent).

Root v. Montana Dep't of Corrections, CV 19-164-BLG-SPW-TJC, 2021 WL 1597922, at *4 (D. Mont. April 23, 2021) (ignoring request).

Van Dam v. Town of Guernsey, Case No. 20-CV-60-SWS, 2021 WL 2942769 at *4 (D. Wyo. June 4, 2021).

Manning v. Safelite Fulfillment, Inc., Case No. 17-2824 (RMB/MJS), 2021 WL 3542808, at *4, n.8 (D.N.J. Aug. 11, 2021).

Modern Remodeling, Inc. v. Tripod Holdings, LLC, Civil Action No. CCB-19-1397, 2021 WL 3852323, at *13-14 (D. Md. Aug. 27, 2021).

Cornejo v. EMJB, Inc., SA-19-CV-01265-ESC, 2021 WL 4526703, at *5 (W.D. Tex. Oct. 4, 2021) (relying on prior 5th Circuit decisions without mention of Rule 37(e).

Mkrtchyan v. Sacramento Cty., No. 2:17-cv-2366 TLN KJN, 2021 WL 5284322, at *10 (E.D. Cal. Nov. 12, 2021).

Alabama Aircraft Indus. v. Boeing, No. 20-11141, 2022 WL 433457, at *6, *16 & n.19 (11th Cir. Feb. 14, 2022) (per curiam).

Stevens v. Brigham Young Univ.-Idaho, Case No. 4:16-cv-00530-BLW, 588 F. Supp. 3d 1117, at *15 (D. Idaho 2022).

Plymale v. Cheddars Casual Café Inc., Case No.: 7:20-CV-102 (WLS), 2022 WL 988313, at *7 (M.D. Ga. March 31, 2022).

Estate of Cindy Lou Hill, No. 2:20-cv-00410-MKD, 2022 WL 1464830, at *17 (E.D. Wash. May 9, 2022).

Hollis v. CEVA Logistics U.S., Inc., 603 F. Supp. 3d 611, 625–26 (N.D. Ill. May 19, 2022) ("Factual Findings and Jury Instruction").

Ayers v. Heritage-Crystal Clean, LLC, Case No. 1:20-cv-5076, 2022 WL 2355909, at *4 (N.D. Ill. June 1, 2022).

Meta Platforms, Inc. v. BrandTotal Ltd., 605 F. Supp. 3d 1218, 2022 WL 1990225, at *8 (N.D. Cal. June 6, 2022).

Drips Holdings, LLC v. Teledrip, LLC, Case No. 5:19-cv-2789, 2022 WL 4545233, at *3 (N.D. Ohio Sept. 29, 2022) (refusing request).

Dish Network LLC. v. Jadoo TV, Inc., Case No. 20-cv-01891-CRB (LB), 2022 WL 11270394, at *4 (N.D. Cal. Oct. 19, 2022)

LKQ Corp. v. Gen. Motors Co., No 20 CO 02753, 2022 WL 14634800, at *7, *9 (N.D. Ill. Oct 25, 2022).

Tyson v. Dep't of Energy & Envtl. Prot., No. 3:21-cv-736 (JAM), 2022 WL 16949396, at *4–5 (D. Conn. Nov. 15, 2022).

Tripp v. Walmart, Inc., Case No. 8:21-cv-510-WFJ-SPF, 2023 WL 399764 (M.D. Fla. Jan. 25, 2023).

Pable v. Chicago Transit Auth., No. 19 CV 7868, 2023 WL 2333414, at *31 & n. 17 (N.D. Ill. Mar. 2, 2023) (refusing request).

Doe v. Willis, Case No: 8:21-cv-1576-VMC-CPT, 2023 WL 2918507, at *15 (M.D. Fla. April 12, 2023).

SRS Acquiom Inc. v PNC Fin. Servs. Grp., Inc., Civil Action No. 19-cv-02005-DDD-SKC, 2023 WL 6461234 (D. Colo. Sept. 8, 2023).

Van Winkle v. Rogers, 82 F.4th 370, 379 (5th Cir. Sept. 15, 2023) (analogous result involving tangible evidence).

Microvention, Inc. v. Balt USA, LLC, Case No. 8:20-cv-02400-JLS-KES, 2023 WL 7476521, at *3 (C.D. Cal. Oct. 5, 2023).

Amann v. Office of the Utah Attorney Gen., Case No. 2:18-cv-00341-JNP-DAO, 2023 WL 7218696, at *8 & n.5 (D. Utah Nov. 2, 2023).

Shiflett v. City of San Leandro, Case No. 21-cv-07802-LB, 2024 WL 536302, at *5, *7 (N.D. Cal. Feb. 10, 2024).

APPENDIX B

The following are pre-rule decisions permitting—but in one case openly questioning[94]—jury predicate findings as a condition of exercising authority to draw adverse inferences. Some "missing evidence" instructions—not listed here—permit a jury to draw adverse inferences upon findings of predicate conditions other than culpability. The Amended Rule "does not limit" the discretion of courts to give such a "traditional" missing evidence instruction that does not require a finding of culpability.[95] The Second Circuit approved such an instruction in *Zimmerman v. Associates First Capital Corp.*,[96] which was relied upon in *Zubulake v. UBS Warburg.*[97]

Wong v. Swier, 267 F.2d 749, 761 (9th Cir.1959) (an inference is proper only "if the jury [has] first found" the party tampered with the evidence).

Glover v. BIC Corp., 6 F.3d 1318, 1330, 1332 (9th Cir. 1993) (remanding for clarification of culpability standard).

Vodusek v. Bayliner Marine Corp., 71 F.3d 148, 155 (4th Cir. 1995) ("if you find" the predicate condition "you are permitted to . . . assume" the evidence "would have been unfavorable to the plaintiff's theory in the case").

[94] Nucor Corp. v. Bell, 251 F.R.D. 191, 203–04 (D.S.C. 2008).

[95] Rule 37(e) measures are distinct because they involve "a punitive attitude or opprobrium." Discovery Subcommittee Call Notes (Feb. 8, 2014) at 3–4, Agenda Book, *supra* note 5, 407–08. *Cf.* Mali v. Fed. Ins. Co. 720 F.3d 387, 391 (2nd Cir. 2013) (permitting jury to find a missing photograph unfavorable without a finding of culpability since not intended as a sanction).

[96] 251 F.3d 376, 383 n.6 (2nd Cir. May 31, 2001) (permitting adverse inference because the destruction was intentional).

[97] 229 F.R.D. 422, 439–40, n.120 (S.D.N.Y. 2004) ("if you find that UBS could have produced this evidence . . . you are permitted, but not required, to infer that the evidence would have been unfavorable to UBS").

Testa v. Wal-Mart Stores, Inc., 144 F.3d 173, 178 (1st Cir. 1998) (jury properly instructed it could (but need not) draw negative inference if it concluded that Wal-Mart had notice of potential lawsuit and document relevance).

Caparotta v. Entergy Corp., 168 F.3d 754, 760 (5th Cir. 1999) (Dissent).

Smith v. Borg-Warner Auto. Diversified Transmission Prods. Corp., No. IP 98-1609-C-T/G, 2000 WL 1006619, at *10 (S.D. Ind. July 19, 2000) (jury may infer information unfavorable "only if you find" it was willfully destroyed in bad faith).

Saul v. Tivoli Sys., 97 Civ. 2386 (DC)(MHD), 2001 U.S. Dist. LEXIS 9873, at *55 (S.D.N.Y. July 17, 2001) (trier of fact may infer documents were adverse if it concludes they were deliberately destroyed).

Golia v. The Leslie Fay Co., No. 01 Civ. 1111 (GEL), 2003 WL 21878788, at *11 (S.D.N.Y. Aug. 7, 2003) (the jury may "if they choose:" infer it was unfavorable and apply it determining the merits).

Crowley v. Chait, Civ. No. 85-2441 (HAA), 2004 WL 7338421, at *9 (D.N.J. Dec. 29, 2004) (jury may find infer lost documents were unfavorable if found to be relevant and could have been produced).

Duque v. Werner Enters., Inc., Civil Action No. L-05-183, 2007 WL 998156, at *6 and n.6 (S.D. Tex. March 30, 2007) (referencing 3 FED. JURY PRAC. & INSTR. § 104.27).

Nucor Corp. v. Bell, 251 F.R.D. 191, 203–04 (D.S.C. 2008) (it makes "little sense" to allow a party found to have acted intentionally to "re-argue the spoliation issue before the jury").

Rimkus Consulting Grp., Inc. v. Cammarata, 688 F. Supp. 2d 598, 620, 646, 643 & n.34 (S.D. Tex. 2010) (referencing 3 FED. JURY PRAC. AND INSTR. § 104.27).

Am. Family Mut. Ins. Co. v. Roth, No. 05 C 3839, 2009 WL 982788, at *10 (N.D. Ill. Feb. 20, 2009).

Socas v. The Northwestern Mut. Life Ins. Co., No. 07-02336-CIV, 2010 WL 3894142, at *9 (S.D. Fla. Sept. 30, 2010).

Union Pump Co. v. Centrifugal Tech. Inc., 404 F. App'x 899, 903–04) (5th Cir. Dec. 16, 2010).

Johnson v. Wells Fargo Home Mortg., 635 F.3d 401, 422 & n.2 (9th Cir. 2011)

Woodward v. Wal-Mart Stores East, No. 5:09-CV-428 (CAR), 801 F. Supp. 2d 1363, 1366 (M.D. Ga. 2011).

Hallmark Cards, Inc. v. Monitor Clipper Partners, LLC, No. 08-0840-CV-W-ODS, 2012 WL 3047164, at *6 (W.D. Mo. July 25, 2012) (referencing 3 FED. JURY PRAC. AND INSTR. § 104.27).

Hallmark Cards, Inc. v. Murley, 703 F.3d 456, 459, 460–62 (8th Cir. 2013).

Mali v. Fed. Ins. Co., 720 F.3d 387, 391 (2d Cir. 2013) (if you find the nonproduction has not been satisfactorily explained, you may infer it would have been unfavorable).

Swift Transp. Co. of Ariz. v. Angulo, 716 F.3d 1127, 1133 (8th Cir. June 17, 2013).

Quantlab Techs. Ltd. v. Godlevsky, Civil Action No. 4:09-cv-4039, 2014 WL 651944, at *25 (S.D. Tex. Feb. 19, 2014).

THE SEDONA CONFERENCE U.S. BIOMETRIC SYSTEMS PRIVACY PRIMER

A Project of the Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

Author:

The Sedona Conference

Editor-in-Chief:

Brian Ray

Contributing Editors:

Julian Ackert
Melissa Ryan Clark
Brett Doran
David Kalat
Colman D. McCarthy
Francis X. Nolan, IV
Lesley Weaver

Steering Committee Liaisons:

Starr Turner Drum
Ruth Promislow

Staff Editors:

David Lumia
Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 11. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> The Sedona Conference, *U.S. Biometric Systems Privacy Primer*, 25 SEDONA CONF. J. 163 (2024).

PREFACE

Welcome to the May 2024 final version of The Sedona Conference *U.S. Biometric Systems Privacy Primer* ("*Primer*"), a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG11 is to identify and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages.

The Sedona Conference acknowledges Editor-in-Chief Brian Ray for his leadership and commitment to the project. We thank contributing editors Julian Ackert, Melissa Clark, Brett Doran, David Kalat, Colman McCarthy, Frank Nolan, and Lesley Weaver for their efforts. We also thank Starr Drum and Ruth Promislow for their contributions as Steering Committee liaisons to the project, and we thank Mark Abramowitz for his contributions.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts of the *Primer* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 meetings where drafts of this *Primer* were the subject of the dialogue. The publication was also subject to a period of public comment. On behalf of The Sedona

Conference, I thank both the membership and the public for all of their contributions to the *Primer*.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
May 2024

TABLE OF CONTENTS

I. INTRODUCTION 168

II. OVERVIEW OF BIOMETRIC RECOGNITION SYSTEMS 169

- A. Biometric Modalities and Purpose 169
- B. Biometric Recognition Systems Overview 171
- C. Common Biometric Modalities 174
  1. Fingerprint Recognition 176
  2. Facial Recognition 177
  3. Iris Recognition 179
  4. Voice Recognition 181

III. BIOMETRIC SYSTEM BENEFITS AND DRAWBACKS 183

- A. Benefits 183
- B. Drawbacks 186

IV. U.S. BIOMETRIC PRIVACY LEGAL LANDSCAPE 195

- A. Overview 195
- B. State Biometric Privacy Laws 199
  1. Biometric/Covered Information Definition. 199
  2. Exemptions from Biometric Regulation 201
  3. Notice and Consent Requirements 202
  4. Sale and Disclosure of Biometric Data 205
  5. Retention of Biometric Data 206
  6. Enforcement and Penalties 207
  7. Security 208

V. SYSTEM SELECTION AND DESIGN 210

- A. Biometric Modality 211
- B. System Design and Accuracy 212
- C. Security and Integrity 215
- D. Privacy and Nondiscrimination 219

I. INTRODUCTION

This *U.S. Biometric Systems Privacy Primer* ("*Primer*") provides a general introduction to biometric systems and a summary of existing U.S. laws regulating the collection, use, and sharing of the biometric information these technologies collect.

This *Primer* is written as a resource for lawyers, judges, legislators, and other policymakers. It provides a general guide to the relationships among the technical, legal, and policy aspects of biometric systems—with a particular focus on the privacy and related concerns these systems may raise.

As Part II explains, the *Primer* focuses primarily on biometric recognition systems (which include both identity verification and identification systems) by private organizations. While the *Primer* generally limits its discussion to private-sector applications, it acknowledges—and, in several places, analyzes—the overlap between public and private applications, including the risks raised by what we term "function creep."

II. OVERVIEW OF BIOMETRIC RECOGNITION SYSTEMS

A. Biometric Modalities and Purpose

The term "biometrics" is used generally to encompass biological or behavioral characteristics that are unique to a person and allow for identification and/or verification of that individual. Biometric recognition systems record a unique physical characteristic—or combination of characteristics—from an individual and compare that stored record to a later-acquired record of the same attribute, using software to determine whether the two records "match" each other within the parameters of a prescribed statistical range set by the system.

The public and private use of biometric technology is expanding dramatically. Biometric technologies have become more robust and advanced, substantially reducing error rates through advances in artificial intelligence (AI), including neural networks. As a result, biometrics has developed into a tool for quick and relatively reliable identification or authentication in a broad range of contexts from border control to unlocking smartphones. These techniques are rapidly replacing traditional passwords as a security measure, with newest facial recognition technology enabling identification in less than one second.[1]

The growth of biometric technology is due, in part, to the potential for biometric systems to offer a faster, simpler, more secure, and more user-friendly alternative to knowledge-based security systems, such as passwords and physical tokens. This is because biometric systems rely on unique, persistent physical features that, for most applications, a person must physically present to confirm identity.

[1] SOODAMANI RAMALINGAM ET AL., FUNDAMENTALS AND ADVANCES IN 3D FACE RECOGNITION, IN BIOMETRIC-BASED PHYSICAL AND CYBERSECURITY SYSTEMS 125–62 (Mohammad S. Obaidat et al. eds., 2019).

Critics of biometric technologies and academics studying these issues have raised privacy, security, and civil liberties concerns in connection with these systems. Some biometric features, such as a person's face, gait, and even fingerprints, are difficult or impossible to keep private, which creates the risk that biometric data can be collected with relative ease and without consent. Even where a person consents to collection, the persistence of biometric features creates heightened concern over unauthorized access to, and use of, that information because the underlying physical characteristics are not easily changed. Well-designed biometric systems convert persistent physical characteristics into proprietary templates that are unusable outside of each system. Yet some privacy advocates have voiced concerns that government and law enforcement collection could use biometric information to track a person across multiple systems.[2]

Some state and local governments, as well as private organizations, have implemented regulatory and policy responses and proposals to try to find a balance that protects individual rights while allowing for the use and growth of biometric technology given its many potential benefits. For example, as we discuss below, some local governments have banned any police use of facial recognition technology, and others have adopted ordinances restricting both private and public use of some biometrics for surveillance. Several states have taken up biometric privacy legislation, and industry groups are increasingly

[2] *See, e.g.*, *Biometrics,* ELEC. FRONTIER FOUND., https://www.eff.org/issues/biometrics (last visited Feb. 2, 2024); Ann Cavoukian et al., *Privacy and Biometrics for Authentication Purposes: A Discussion of Untraceable Biometrics and Biometric Encryption*, *in* ETHICS AND POLICY OF BIOMETRICS, ICEB 2010, LECTURE NOTES IN COMPUTER SCIENCE 14 (Ajay Kumar & David Zhang eds., 2010).

advocating for best practices guidelines and other forms of self-regulation.

B. *Biometric Recognition Systems Overview*

The term "biometrics" is used across multiple disciplines to describe an array of technologies and processes ranging from identity or verification systems to biological processes like the statistical analysis of biological data. The lack of consensus over how to define "biometrics," and even what biological characteristics the term should encompass, is reflected in the differing legal definitions included in the data privacy and related laws discussed below in Part IV.

For purposes of this *Primer*, we focus on a set of technologies related to identifying individuals that fit the International Standards Organization's (ISO) definition for biometric recognition: "automated recognition of individuals based on their biological and behavioral characteristics."[3] This definition encompasses the two most common biometric processes: biometric verification (sometimes called "authentication") and biometric identification.

Verification compares an existing template of a biometric identifier to a newly submitted template to verify a person's identity, for example, using a finger scan or face template to unlock a mobile phone or clock into one's workplace. This process is referred to as 1:1 matching because the software compares the newly submitted information only with the stored information of the claimed identity.[4]

[3] ISO/IEC 2382-37:2022 *Information technology — Vocabulary — Part 37: Biometrics*, ISO, https://standards.iso.org/ittf/PubliclyAvailableStandards/ (last visited May 10, 2024).

[4] ANIL K. JAIN ET AL., INTRODUCTION TO BIOMETRICS, 10–11 (2011).

Identification compares a newly submitted biometric template to a database of stored templates to identify a person.[5] This process is used to prevent and detect alias or duplicate enrollments, whether accidental or intentional—called "scrubbing" for double identity holders—and by law enforcement to search for matches against criminal databases for background checks or in criminal investigations, among others.[6] Private commercial entities have similarly used facial recognition systems to identify individuals in a variety of contexts, including for security purposes.[7] This process is referred to as 1:n matching because the software compares the newly submitted information with a database containing the stored information of multiple other records.

Most biometric recognition systems follow a basic operating model that includes the following components:[8]

Acquisition and Enrollment: Software captures a raw data sample of a particular physical feature from an individual. Some biometric modalities typically require direct contact with a device to scan the feature. For example, finger scans capture a 2D image of the friction ridges present on the subject's finger pad. Others, such as facial recognition, can be acquired from a real-time camera image or by scanning existing other sources, such

[5] *Id.* at 11–12.

[6] Due to the complexity of additional issues that arise in the context of law enforcement and national security, this *Primer* focuses on the use of biometrics in private and commercial applications.

[7] *See, e.g.*, Tom Chivers, *Facial recognition . . . coming to a supermarket near you*, GUARDIAN (Aug. 4, 2019), https://www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties.

[8] JAIN, *supra* note 4, at 3–10; BIOMETRIC SYSTEMS: TECHNOLOGY, DESIGN AND PERFORMANCE EVALUATION 9–14 (James Wayman et al. eds., 2005) [hereinafter BIOMETRIC SYSTEMS].

as government ID or even social media postings and other publicly available photographs.

Data Extraction: The software then uses an algorithm to convert the raw sample into a digital biometric template that is, usually, a mathematical or symbolic representation of the raw sample reflecting the unique landmarks derived from the subject's sample.

Liveness Detection: Liveness detection is a security countermeasure, used in some biometric recognition systems, that can be deployed to distinguish a biometric trait presented by a live person from an artificial submission of data. The type of liveness detection used will vary based on the biometric modality. Examples of liveness detection include pulse rate, blood flow, muscle contractions, electrical responses from human tissue, and three-dimensional variations in how the subject repositions between successive captures.[9]

Alias/Duplicate Check: Where an enrollment database is used, the operator may search that database for potential matches at enrollment to determine if the enrollment is unique. This is one example of the use of 1:n matching for the purposes of creating a 1:1 verification system.

Data Storage: The system retains a database of enrolled templates to search and compare, or the subject may carry its template in a secure form. The software typically associates each template with an identifier. In some cases, such as a digital electronic identification, the record with the enrolled template is placed on a phone or smartcard and is carried by the subject.

Data Matching: Software uses a computer algorithm to determine whether the new template is sufficiently similar to the

[9] JAIN, *supra* note 4, at 272–78; *see also* Abdenour Hadid et al., *Biometrics Systems Under Spoofing Attack: An Evaluation Methodology and Lessons Learned*, 32 IEEE SIGNAL PROCESSING MAG. (Sept. 2015), at 20.

enrolled template(s) from the database or a personally carried medium to be considered a "match" for the purposes of the system's design and purpose. After a matching algorithm compares the similarities between the enrolled template or templates and the one presented for authentication, the resulting output can either be used to validate a claimed identity for verification purposes, or to rank matches across multiple identities for identification purposes. The threshold of similarity can be calibrated by the system designer to balance the risks of false rejection and false acceptance to find the optimum balance of accuracy for the specific use case involved.[10]

System Parameters: Some systems allow the end-user/operator to define or modify the threshold requirements for determining when a new sample potentially "matches" the existing record or records based on the purpose of the system use and the accuracy of the technology.[11]

C. Common Biometric Modalities

The field colloquially described as "biometrics" continues to advance, with developers modifying existing technology and developing new ways to verify or identify individuals based on biological, physical, and behavioral characteristics. In addition, biometric systems increasingly use more than one characteristic, such as combining facial recognition with a finger scan, to take advantage of the different benefits of each and to increase the accuracy, security, and convenience of a system. Concerns about the risks of the use of various biometric characteristics for either identification or verification may change based on

[10] JAIN, *supra* note 4, at 9–10.

[11] ILEANA BUHAN & PIETER HARTEL, THE STATE OF THE ART IN ABUSE OF BIOMETRICS (2005).

whether a biometric system uses one or a combination of characteristics.[12]

Behavioral biometrics extend the use of biometric characteristics to create a unique profile of a distinctive behavior or combination of behaviors ranging from how a person holds a device, swipes a screen, or types on a keyboard to build a user profile for authenticating the person's identity.[13] These patterns often are combined with other information such as a person's IP address and/or location to identify suspicious authentication attempts that the system either blocks or triggers the requirement for an additional authentication method.

This section analyzes four of the physical characteristics most often used in biometric recognition systems to illustrate how different characteristics, and combinations of characteristics, offer distinctive benefits and pose different risks[14] The four characteristics we include—fingerprint, facial, iris, and voice recognition—generally illustrate the range of benefits and risks of using other characteristics, such as vein and gait recognition, though the use of existing biometric characteristics and the addition of new characteristics continue to evolve.

These benefits and risks vary to some extent for each characteristic. Incorporating multiple biometric characteristics and connecting one or more characteristics with other information further complicates the risk-benefit analysis of a biometric system. That calculus also depends on many other variables

[12] JAIN, *supra* note 4, at 209–12.

[13] *See* INT'L BIOMETRICS+IDENTITY ASS'N, BEHAVIORAL BIOMETRICS, https://www.ibia.org/download/datasets/3839/Behavioral (last visited May 10, 2024).

[14] *See, e.g.*, WORLD BANK GROUP, TECHNOLOGY LANDSCAPE FOR DIGITAL IDENTIFICATION 18 (2018), https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf (identifying face, iris, and fingerprint recognition as "primary biometrics").

discussed below. This section illustrates the perhaps basic, but often overlooked, point that not all biometric characteristics are the same and underscores the importance of carefully considering those differences when selecting and designing biometric systems for different applications as well as whether a biometric system is the appropriate tool in the first instance.

1. Fingerprint Recognition

The science of forensic fingerprint analysis was codified by Sir Francis Galton in the late nineteenth century, culminating in the 1892 publication of his landmark treatise *Finger Prints*.[15] Galton cataloged unique characteristics, collectively called "minutiae," that collectively represented the various structures evident in a person's fingerprint. To systematize the process of fingerprint analysis into something that can be performed efficiently by software, modern computerized systems eschew the identification of nearly all of the various structures altogether and do not attempt to perform pattern matching on images. Instead, most commercial fingerprint-based authentication systems rely on mapping only one type of minutiae. Although fingerprint analysts have identified as many as 150 different types of minutiae, only the points where ridges either terminate or bifurcate are considered salient for the purposes of automated recognition systems.[16]

During the enrollment phase, a subject places its finger onto a scanning device. Different manufacturers use a variety of competing sensor technologies, including optical, capacitance, pressure, thermal, or ultrasound. Whatever sensor technology is used generates an image of the fingerprint, but this image needs

[15] FRANCIS GALTON, FINGER PRINTS (1892).

[16] Fed. Bureau Investigation, *Fingerprint Recognition*, https://ucr.fbi.gov/fingerprints_biometrics/biometric-center-of-excellence/files/fingerprint-recognition.pdf (last visited May 10, 2024).

to be processed before it can be used to identify minutiae points. First, the grayscale image is converted to a pure black-and-white image with no intermediate grays and is "thinned" to reduce each ridge down to the width of a single pixel. The system then identifies minutiae points by their orientation and coordinates on an x/y plane.[17] This coordinate information is stored as a "template" and is assigned to a particular user identity or account in the system in question.

During the matching phase, a subject presents its finger to a scanning device to be processed in the same way, and the resulting template is compared to the stored template to determine statistical similarity. If a sufficient number of data points are found in common, the scans are considered to match.

The threshold of similarity required to be deemed a "match" can be calibrated by the system designer or, in some instances, the system user to balance the risks of false rejection and false acceptance to find an appropriate matching threshold for the purpose and technology involved.

2. Facial Recognition

Generally speaking, facial recognition technologies can be divided into two distinct categories, which in turn consist of numerous competing subcategories.

The first category ("Category 1") includes approaches (such as the Principal Component Analysis, or "Eigenfaces," method) that identify distinguishing relative differences between images within a given set. The system first develops an average of all the face images in its dataset. Then, the system compares each

[17] Lukasz Wieclaw, *A Minutiae-Based Matching Algorithms in Fingerprint Recognition Systems*, 13 J. MED. INFORMATICS & TECHS. 65 (2009); Ravi. J et al., *Fingerprint Recognition Using Minutia Score Matching*, 1(2) INT'L J. ENG'G SCI. & TECH. 35 (2009).

individual face image in that base set to the average, subtracting out the common elements they share and assigning mathematical weights to those variances. These mathematical representations of how a given face differs from the average in the set are called "eigenfaces," named after the concept of "eigenvectors" in linear algebra. New images are processed in the same way and are ranked based on how closely their eigenface transformations align with those that have already been calculated. If a certain characteristic combination of eigenfaces is substantially similar to a known image, then there is a mathematical basis to conclude the two images are visually similar.[18]

The second category ("Category 2") includes approaches (such as measurements of facial geometry) that identify distinguishing features of each subject's face. This model-based face recognition approach enables matching for facial images that do not share the same pose or orientation by constructing a facial graph from key landmarks such as corners of the eyes, tip of the nose, corners of the mouth, and chin.[19]

Category 1 technologies described above are "template-based" approaches that distinguish individual faces from a given, closed, set of data points. These approaches generally depend on comparing templates within a specific defined dataset and are amenable to security protections in their design that minimize the risk that the data could be used outside of the specific application.[20]

Category 2 methods create facial models that do not depend on replicating the orientation and lighting of the enrolled

[18] Matthew Turk & Alex Pentland, *Eigenfaces for Recognition*, 3 J. COGNITIVE NEUROSCIENCE 71 (1991).

[19] JAIN, *supra* note 4, at 122–24.

[20] Yi C Feng et al., *A Hybrid Approach for Face Template Protection*, 6944 SPIE PROC: BIOMETRIC TECH. FOR HUM. IDENTIFICATION V (2008).

template and can potentially be used outside the original enrolled setting. These technologies are feature-based approaches that begin with measurements of specific facial features and their relationship to one another on a given face. Once a prominent orienting facial landmark (typically, the center of the eyes) is identified, the software crops out nonfacial components (such as hair) to isolate the relatively unchanging central features. The software then performs "intensity normalization" to convert certain facial features determined to be useful for discriminating between different faces into numerical vectors.[21]

In both categories of facial recognition technology, a visual image of a subject's face is processed to standardize and equilibrate the visual details. Further processing is performed on the standardized data to identify and extract the facial features relevant to the approach the system uses and store a mathematical representation of the significant features: eyes, nose, mouth, etc. (the "template"). During the matching phase, the same process is repeated, and the resulting mathematical representation is compared to the stored template. If a sufficient mathematical similarity (as prescribed by the system owner) is found, the scans are considered to match. The administrators of such systems can configure the threshold level of confidence for a match to be accepted and thereby balance the rate of false positives to false negatives based on the use case.

3. Iris Recognition

The iris is a thin diaphragm in the middle of the eye, situated behind the cornea and in front of the lens. The iris is composed of a complex set of muscles, tissue, blood vessels, and other biological structures that collectively have a distinct visual

[21] R. Sivapriyan et al., *Analysis of Facial Recognition Techniques*, 57 MATERIALS TODAY: PROC. 2350 (2022), https://doi.org/10.1016/j.matpr.2022.01.296.

appearance. Although it is unknown whether the iris is biologically unique between individuals, it has been found to be distinctive enough for use in biometric systems.[22]

One advantage to using an iris recognition system is that the eye muscles react to light, which enables the scanning system to confirm that the eye is in fact present at the time of scanning (liveness detection), which can guard against the risk of an attacker replaying a recording to the system in place of the actual subject.[23]

Comparing two iris scans is a complex geometric challenge that requires the software to isolate the information describing the biological structures of the iris from the noisy information resulting from how the subject's head was oriented at the time of the scan, the degree to which ambient light caused the iris to expand or contract, and other circumstantial differences. In other words, the software must be sophisticated enough to discriminate between the information attributable to the subject's fundamental biology from the information incidental to the circumstances of the scan.

A typical iris recognition system begins by scanning the subject's eye with near infrared light to take several two-dimensional monochromatic images (although the pigmentation of the iris is a distinctive characteristic that humans use to recognize one another's eyes, the color is not relevant to the processing described below and is not captured). The software selects the best of these images and discards the others. The chosen image is then cropped to isolate only the iris from the rest of the image (excluding the pupil, eyelids, eyelashes, and

[22] Richard Wildes, *Iris Recognition*, *in* BIOMETRIC SYS: TECH., DESIGN & PERFORMANCE EVAL., *supra* note 8, at 65–68; JAIN, *supra* note 4, at 141–45, 170–71.

[23] Wildes, *supra* note 22, at 67.

other features). The cropped image is then processed to "unwrap" the conical shape of the iris onto a rectangular shape of fixed dimensions.

The software then encodes the coordinates measured from the unwrapped iris, using algorithms to mathematically calculate a binary code called an "iris signature" that contains the coordinate information. This signature is stored as the enrolled template. To authenticate a subject, the same process is repeated to generate a binary iris code to be compared to the template.[24]

4. Voice Recognition[25]

Voice recognition technology proceeds from the assumption that each person's vocal tract is biologically unique, and therefore attributes of the speaker's voice are particular to that tract. The acoustic patterns of the speaker's voice are directly affected by the physical characteristics of the speaker's vocal tract, mouth, nasal cavities, jaw, tongue, larynx, and other biological features.[26]

Unlike some of the other biometric traits discussed above, the physical features of the speaker's vocal tract are known to change over time and are affected by the speaker's age, mood, health, and emotional state. Additionally, voice patterns are not as distinctive to an individual as other biometric traits. Nevertheless, there are certain circumstances (such as telephonic communications) where the speaker's voice may be the only feature presented. Consequently, there are situations where voice

[24] *Id.* at 73–86; JAIN, *supra* note 4, at 144–45.

[25] As discussed in Part IV, several biometric information privacy statutes use the term "voiceprint," which may be distinct from "voice recognition."

[26] M. M. Kabir et al., *A Survey of Speaker Recognition: Fundamental Theories, Recognition Methods and Opportunities*, 9 IEEE ACCESS *79236* (2021).

recognition is the only biometric modality available to authenticate a person's identity.[27]

Voice recognition technology can be "text dependent" (where the speaker has to say a certain passphrase to be recognized and authenticated) or "text independent" (where the speaker can say anything, and the recognition may run in the background of a voice interaction). A typical voice recognition system begins by sampling a section of the speaker's audio and mapping the audio signal's quality, duration, intensity dynamics, and pitch. Depending on the technology used, different statistical state-mapping models are applied to classify the vocal characteristics. The resulting template is a set of vector states representing the characteristic sound forms derived from the audio sample.

During the matching process, the same process described above is repeated on a new audio sample and compared to the enrolled template or templates. The software compares the vector states to determine a statistical likelihood that the two samples come from the same speaker.[28]

[27] Fed. Bureau Investigation, *Speaker Recognition*, https://ucr.fbi.gov/fingerprints_biometrics/biometric-center-of-excellence/files/speaker-recognition.pdf (last visited May 10, 2024).

[28] Clark D. Shaver & John M. Acken, *A Brief Review of Speaker Recognition Technology*, PROC. 6TH INT'L MULTI-CONF. ON COMPLEXITY, INFORMATICS & CYBERNETICS: IMCIC 2015, at 172, http://archives.pdx.edu/ds/psu/19320.

III. BIOMETRIC SYSTEM BENEFITS AND DRAWBACKS

A. Benefits

Biometric systems can provide a variety of operational and security benefits across different settings. Most prominently, biometric technology can allow for enhanced security and protection of information, including sensitive personal information, through the use of biometric data as an access gateway in place of passwords or personal information (e.g., social security numbers) that can be forgotten, stolen, or shared.[29] To realize these benefits, designers of biometric recognition systems typically use characteristics that meet the following criteria:

Robust: Characteristics that are relatively unchanging on an individual over time;

Distinctive: Characteristics that exhibit significant variation across individuals within the overall population;

Available: All individuals in the population can be expected to have this characteristic;

Accessible: The characteristic can be measured or scanned electronically; and

Acceptable: Individuals do not generally object to having it measured or scanned.[30]

The growth of biometric technology is due, in part, to the potential for biometric systems to provide more secure, faster, cheaper, simpler, frictionless, and more user-friendly alternatives to other forms of information security. In "real world" scenarios, humans routinely rely on biological features to identify one another. Known associates can be recognized in one-on-one interactions by face or voice, while government-issued

[29] Irfan Iqbal, *Biometrics: Security Issues and Countermeasures*, 4 INT'L J. SCI. & RES. 2229 (2015).

[30] BIOMETRIC SYSTEMS, *supra* note 8, at 3–4.

identification cards provide photographs to facilitate the official verification of one's identity to a stranger. The use of biometric technology provides a mechanism to adapt this process into an electronic realm.

Proponents of biometric identification and authentication technologies note that it offers significant security advantages over other methods of information security. For example, reliance on passwords introduces a range of risks—from the use of weak or easily guessable passwords, to the ease with which passwords can be shared among other users in ways that reduce the security of the overall system and limit the ability to reliably identify individual users. From a security standpoint, biometrics are preferable over passwords because they aim to tie the authentication process directly to the actual subject's identity, rather than a password or token that can be forgotten, lost, or swapped. The aspects that make biometric-based security more secure are also aligned with ease of use.[31]

Instead of relying on a user to remember and protect different passwords, the person physically presents their persistent physical features to an electronic system to gain access. Because the templating technology in each system is often proprietary, the individual templates derived from persistent biological or behavioral features cannot be easily replicated even with access to a publicly available feature, like a person's face. Whereas a person who uses the same "password123" in multiple systems is exposed in all of them when that password is leaked, a person who is authenticated into multiple systems with a biometric,

[31] David Kalat, *You Can't Change Your Fingerprints, But Do You Need To? The Evolution of Biometric- and Password-Based Authentication Security—Part I*, 5 PRATT'S PRIV. & CYBERSECURITY L. REP. 137 (2019); David Kalat, *You Can't Change Your Fingerprints, But Do You Need To? The Evolution of Biometric- and Password-Based Authentication Security—Part II*, 5 PRATT'S PRIV. & CYBERSECURITY L. REP. 217 (2019).

depending on the engineering of the affected systems, would not necessarily be exposed in all of them even if a template from one were to be leaked.[32]

Biometric recognition systems also play a prominent role in Multi-Factor Authentication (MFA). MFA is a security control that requires two or more forms of authentication to confirm identity. MFA has long been recognized as a best practice for data security, and federal and state regulators increasingly require it. For example, beginning in 2021, all federal agencies are required by an executive order to use MFA, and the New York Department of Financial Services Cybersecurity Regulation explicitly requires MFA in some circumstances.[33]

While all forms of MFA increase security, the Cybersecurity and Infrastructure Security Agency (CISA) recently released a fact sheet describing how phishing and similar attacks undermine several common types of MFA, including SMS (Short Message Service, i.e., standard text messages) and voice messages, and calling on organizations to implement "phishing-resistant" forms of MFA.[34] CISA noted that the only widely available form of phishing-resistant MFA is the Fast ID Online/Web Authentication standard developed by the FIDO Alliance and published by the World Wide Web Consortium ("FIDO2").[35] The FIDO2 standard uses either separate physical tokens or biometrics to confirm a user's identity.

[32] *Id.*

[33] *See* Exec. Order No. 14028, 86 C.F.R. 26633 (2021); 23 N.Y. FIN. SERV. LAW § 550.12 (McKinney 2023).

[34] CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, IMPLEMENTING PHISHING-RESISTANT MFA 3–4 (2022), https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

[35] *Id.*; *How FIDO Works*, FIDO ALL., https://fidoalliance.org/how-fido-works/ (last visited May 10, 2024).

The Federal Trade Commission (FTC) has also identified phishing-resistant MFA as an element of the reasonable security required for organizations that collect consumer data. In two recent settlements with companies over lax security practices, the FTC ordered both organizations to adopt MFA methods and specifically prohibited using telephone or SMS-based authentication.[36]

B. *Drawbacks*

Critics of biometric technologies and academics studying these issues have voiced concerns that the reliable and persistent link to an individual that makes biological characteristics (like face, iris, fingerprint, and voiceprint) useful for recognition also can be viewed as an intrusion into one's personal space and privacy—and a challenge to the autonomous control of personal information.[37]

Many automated systems, not just biometric ones, collect, use, aggregate, and share data in ways that are often poorly understood or opaque. As a result, even well-designed systems behaving appropriately can give rise to unease among the system's users. For example, people may feel alarmed when they think that a system or an entity "knows" more about them than they knowingly or intentionally disclosed. Similarly, privacy advocates have raised concerns about the potential for entities that collect biometric data for one purpose to use or share that

[36] Decision and Order at 6, Drizly, LLC, FTC Docket No. C-4780 (Jan. 10, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Decision-and-Order.pdf; Decision and Order at 5–7, Chegg, Inc., FTC Docket No. C-4782 (Jan. 25, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Decision-and-Order.pdf.

[37] *See, e.g.*, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 11 (Joseph Pato & Lynette Millett, eds., 2010); ELEC. FRONTIER FOUND., *supra* note 2.

data in an unexpected way.[38] Such concerns may be compounded by the reality that some biological features, like a person's face, are often publicly available, potentially facilitating the identification of an individual or the aggregation of their data without the subject's knowledge.

Consequently, some privacy advocates have argued that compromised biometric information from one system could be used to steal a person's identity across multiple systems that rely on the same biometric feature, or that biometric features could be used to combine data about an individual, de-anonymize it, or share it with multiple entities.[39] The following list identifies and briefly explains some of the key privacy and related concerns that have been raised in the collection and use of biometric information.

Persistent Identification. Biometrics are derived from physiological or biological characteristics that are generally immutable and unique to each individual. Critics of biometric systems are therefore concerned that the collection of biometric information for one application could result in a persistent link between that data and a given individual. Such a connection could allow an individual's data to be associated with their actual identity or could result in an association between data and an individual that is permanent and can never be severed by the user.

This concern is heightened by the risk that a persistent biological characteristic could be aggregated with other sources of personal information to form a more detailed profile of an

[38] *See, e.g.*, IDENTIFICATION FOR DEVELOPMENT, A PRIMER ON BIOMETRICS FOR ID SYSTEMS (2022) 31–32 (ID4D).

[39] *Id.*

individual.[40] Any collection of personal information raises this risk. But unlike information linked by a name, a credit card number, or an IP address, for example—where the link to an individual could be broken—the relatively immutable nature of the biological characteristics used in biometric systems raises concerns that the link may be unchangeable, i.e., data will be permanently associated with one's actual identity.

The proliferation of biometric systems in both private and public settings has coincided with rapid advancement in technical capabilities as well as decreasing costs of the hardware and software components. As a result, technology could develop in ways that permit combining more and better biometric data and other information in ways that compromise individual privacy to a greater extent than any single application. It also raises questions about whether biometric technology is being implemented where increased security and identity verification is required, and with the appropriate biometric security and privacy concerns in mind.

Security. Advocates of biometric technologies argue that such systems offer improved security to verify identity because the biological characteristics used are intimately connected to an individual and often must be physically presented for verification.[41] Biometric systems are not, however, immune from compromise.

Biometric systems approximate whether a new template (i.e., biometric input) sufficiently matches the existing one. Attackers can spoof a system by using techniques such as downloading or printing a person's photo, using a fake silicone

[40] AI NOW INSTITUTE, REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS 7–8 (Amba Kak ed., September 1, 2020), https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions.

[41] Iqbal, *supra* note 29.

fingerprint, or using a 3D mask. Such attacks are known as presentation attacks.[42]

Moreover, recent research has demonstrated the possibility of generating both "master prints" and "master faces" that match the partial fingerprints and faces of multiple people and could therefore theoretically give access to a large number of user accounts for multiple individuals.[43] At present, this risk is remote and limited to systems that use multiple enrollments for the same biometric.

The security of stored biometric information is itself a key consideration. If that information has the potential to be used across multiple systems, compromise of it creates a far greater security risk than a compromised password or other identifier that can be changed.[44]

Publicly Accessible Characteristics. Certain biometric information can be collected without the knowledge of the individual. For example, facial recognition or voiceprint technology can be used without the individual's knowledge or consent. Other modalities that generally require direct interaction with the collection device (e.g., fingerprint placed onto a finger scanning device) may still present some risk of capture through indirect means (e.g., lifting a fingerprint from an item touched by

[42] *See* Hadid et al., *supra* note 9.

[43] *See* Aditi Roy et al., *MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems*, 12(9) IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY 2013 (2017), https://ieeexplore.ieee.org/document/7893784; Ron Shmelkin et al., *Generating Master Faces for Dictionary Attacks with a Network-Assisted Latent Space Evolution*, 2021 16TH IEEE INT'L CONF. ON AUTOMATIC FACE & GESTURE RECOGNITION (2021), https://ieeexplore.ieee.org/document/9666968.

[44] *See* A PRIMER ON BIOMETRICS FOR ID SYSTEMS, *supra* note 38.

the individual) that allow for the covert collection of information.[45]

Secondary Information. Templates from some biometric systems can contain secondary information that could be harvested and used beyond the individual's knowledge or consent. For example, some systems claim to be able to detect emotions and other information from both static and live facial images.[46]

Tracking and Surveillance. Identifying individuals by means of biometric information expands the ability to track the movement, activity, and behavior of those individuals. This is particularly the case with biometric information that can be implemented surreptitiously—most notably, facial recognition technologies.[47]

Function Creep. Function creep involves the reuse of sensitive information beyond the purpose for which it was originally collected. Function creep can occur with benevolent intent. For example, in Australia, a biometric database originally designed to prevent cross-border criminal activity was used to identify individuals who lost other forms of identification in brushfires and provide them aid.[48] But it may also compound potential

[45] *See, e.g.*, YAMILA LEVALLE, BYPASSING BIOMETRIC SYSTEMS WITH 3D PRINTING AND 'ENHANCED' GREASE ATTACKS, DREAMLAB TECHS. (2020), https://dreamlab.net/media/img/blog/2020-08-31-Attacking_Biometric_Systems/WP_Biometrics_v5.pdf.

[46] *See, e.g.*, *TechDispatch #1/2021 – Facial Emotion Recognition*, EUR. DATA PROT. SUPERVISOR (May 26, 2021), https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12021-facial-emotion-recognition_en.

[47] *See* ELEC. FRONTIER FOUND., *supra* note 2.

[48] Justin Hendry, *Services Australia put face matching to work for bushfire relief payments*, ITNEWS (June 5, 2020), https://www.itnews.com.au/news/services-australia-put-face-matching-to-work-for-bushfire-relief-payments-548978.

concerns about identity theft, tracking, the collection or sharing of personal information, and misidentification, particularly as the use of biometrics evolves and becomes more predominant.

Individuals who have consented to the collection of their biometric identifiers as a secure method for building access at their workplace, for example, may not have provided consent for the use of their biometric information to identify their whereabouts in the building, assess their health, or evaluate their emotional state at work. An individual who has consented to the use of facial geometry for a mobile application's photo filter may not have consented to the use of that biometric information as a personal identifier.

Function creep also can affect security. Using biometric data for new purposes often means increased access, storage points, and potential disclosure of that data. Likewise, the quality and integrity of biometric data require examination when function creep arises—the integrity of biometric data suitable for one purpose (e.g., home security) may not be suitable for a new purpose (e.g., criminal identification by law enforcement) and may result in misidentification or security flaws.[49]

The potential for private biometric systems to share information with law enforcement and national security agencies intensifies these concerns. In 2015, the FBI announced that it would start to retain fingerprints submitted for routine background checks in its searchable criminal database.[50] A series of U.S. House and Senate investigations into law enforcement access to private biometric databases have highlighted the sometimes blurred lines between private and public use of biometric

[49] *See* A PRIMER ON BIOMETRICS FOR ID SYSTEMS, *supra* note 38, at 31–32.

[50] Jennifer Lynch, *FBI Combines Civil and Criminal Fingerprints into One Fully Searchable Database*, ELEC. FRONTIER FOUND. (Sept. 18, 2015), https://www.eff.org/deeplinks/2015/09/little-fanfare-fbi-ramps-biometrics-programs-yet-again-part-1.

information and even prompted legislation.[51] These and other examples demonstrate the ease with which private biometric information can be obtained and shared with law enforcement.[52]

Discrimination and Bias. Critics of biometric systems and other algorithm-based decision systems have noted patterns of discrimination against certain groups, which can result in perpetuating and exacerbating existing discriminatory structures or processes.[53] Among biometric modalities, facial recognition has received the most attention in this area because facial features used for identification more often correlate with salient demographic features such as race, sex, and age than other biometric modalities such as fingerprints and irises.[54]

[51] *See* Letter from Sen. Edward J. Markey to Founder and CEO of Clearview AI, Hoan Ton-That (June 8, 2020), https://www.markey.senate.gov/download/clearview-ai-protests-letter; Fourth Amendment Is Not For Sale Act, 117th Cong. § 1265 (2021).

[52] *See, e.g.*, Nicol Turner Lee & Caitlin Chin-Rothmann, P*olice Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color*, BROOKINGS (Apr. 12, 2022), https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

[53] *See, e.g.*, Davide Castelvecchi, *Is Facial Recognition Too Biased to Be Let Loose?*, NATURE (Nov. 18, 2020) https://www.nature.com/articles/d41586-020-03186-4. For a broader discussion of these issues, *see* CHRISTIANE WENDEHORST & YANIC DULLER, BIOMETRIC RECOGNITION AND BEHAVIOURAL DETECTION: ASSESSING THE ETHICAL ASPECTS OF BIOMETRIC RECOGNITION AND BEHAVIOURAL DETECTION TECHNIQUES WITH A FOCUS ON THEIR CURRENT AND FUTURE USE IN PUBLIC SPACES, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs (2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf.

[54] Christian Rathgeb et al., *Demographic Fairness in Biometric Systems: What Do the Experts Say?* 41(4) IEEE TECH. & SOC'Y MAG. 71, (Dec. 2022), https://ieeexplore.ieee.org/document/9975333.

In spite of the substantial attention that these issues have received, there is no single accepted definition of what constitutes "fairness" for biometric systems (or algorithms more generally).[55] From a technical performance perspective, it is relatively straightforward to measure and quantify how a system performs on a specific metric across different demographics.[56] For example, the National Institute of Standards and Technology (NIST) has engaged in ongoing performance testing comparing several facial recognition algorithms against trained human reviewers. This Facial Recognition Verification Testing program, with some notable exceptions, has reported higher error rates for some demographic groups for both verification (1:1 matching) and identification (1:n matching), although the studies indicate that the systems are improving over time.[57]

The rapid evolution of biometric systems promises to eventually make these systems highly accurate across all demographics. Even where a biometric system meets a set of technical standards for accuracy and nonbias in a test setting, it may exhibit flaws in real-world conditions, and/or the testing scenario may fail to adequately consider the operational and social aspects of real-world applications that can introduce inaccuracies or bias.

Transparency. The risk of discrimination is exacerbated by the frequent lack of transparency in the deployment of these systems and the alleged use of privately created "watch list"

[55] *Id.*

[56] *Id.*

[57] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NAT'L INST. STANDARDS & TECH. (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

databases.[58] Individuals often have no way of knowing that a private system has flagged their biometric information (most often facial templates created from surveillance camera footage) or no opportunity to contest it.[59] This lack of transparency and procedural protections heightens the accuracy and bias risks identified above because many systems are less accurate for people of color and women.[60]

[58] *See* AI NOW INSTITUTE, *supra* note 40, at 11; Anshul Kumar Singh & Charul Bhatnagar, *Biometric Security System for Watchlist Surveillance*, 46 PROCEDIA COMPUT. SCI. 596 (2015).

[59] Written Testimony of Meredith Whittaker to U.S. House Committee on Oversight and Reform, Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy 4 (Jan. 15, 2020), https://www.congress.gov/116/meeting/house/110380/witnesses/HHRG-116-GO00-Wstate-WhittakerM-20200115.pdf.

[60] In 2021, Apple was sued by a black man who was misidentified as a shoplifter by one of its retail store's facial recognition security systems. *See* Kim Hart, *Facial recognition surges in retail stores*, AXIOS (July 19, 2021), https://www.axios.com/facial-recognition-retail-surge-c13fff8d-72c6-400f-b680-6ae2679955d4.html.

IV. U.S. BIOMETRIC PRIVACY LEGAL LANDSCAPE

A. Overview

In the U.S., biometric-specific regulation falls roughly into two phases. The first began in 2008 when Illinois passed the groundbreaking Biometric Information Privacy Act (BIPA).[61] Texas adopted a similar law in 2009.[62] In the second wave, several state and local governments passed laws targeting biometric information,[63] and a growing number of states have passed comprehensive consumer data privacy laws that specifically protect biometric information, often including it within a category of highly sensitive personal information.[64] Several other states include biometric information among the types of

[61] 740 ILL. COMP. STAT. 14/1–99 (2023). BIPA provides for a private right of action, permitting "aggrieved" individuals to assert claims for violations of the statute. *Id*. at 14/20.

[62] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2023) (Capture or Use of Biometric Identifier). Unlike BIPA, The Texas statute does not provide for a private right of action.

[63] *See, e.g.*, WASH. REV. CODE § 19.375.020 (2023) (Enrollment, disclosure, and retention of biometric identifiers; effective 2017); N.Y COMP. R. & REGS. Tit. 22, §§ 1201–1205 (McKinney 2023) (Biometric Identifier Information; effective 2021); PORTLAND, OR., CITY CODE ch. 34, §§ 10.010–10.050 (2022) (Digital Justice; Prohibit the use of Face Recognition Technologies in Places of Public Accommodation by Private Entities in the City of Portland; enacted 2020, effective 2021).

[64] *See, e.g.*, California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2023) (amended by the California Privacy Rights Act, by vote in 2020, effective 2013, to address biometric information); Colorado Consumer Protection Act, COLO. REV. STAT. §§ 6-1-713, 6-1-713.5 (2023); Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1301-6-1-1313 (2023) (effective July 1, 2023); Maryland Personal Information Protection Act, MD. CODE ANN., COM. LAW §§ 14-3501 to 14-3508 (LexisNexis 2023) (amended 2018); Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575 to 59.1-585 (2023) (effective 2023); Tennessee Information Protection Act, Tenn. Pub. Acts 408 (effective July 1, 2025).

covered information in their data protection and breach notification laws.[65] Numerous states are considering biometric privacy legislation.[66]

At the federal level, members of both the House and Senate have introduced several unsuccessful legislative proposals to regulate biometric privacy, including through general data privacy laws.[67] The FTC's general consumer protection authority

[65] *See, e.g.,* Arkansas Personal Information Protection Act, ARK. CODE ANN. §§ 4-110-101 to 4-110-108 (2023) (amended to address biometric data in 2019); DEL. CODE ANN. tit. 6, § II-12B-100-104 (2023) (Computer Security Breaches); IOWA CODE §§ 715C.1-2 (2023) (Personal Information Security Breach Protection); VT. STAT. ANN. Tit. 9, §§ 2430-2445 (2023) (Protection of Personal Information); WIS. STAT. § 134.98 (2023) (Notice of unauthorized acquisition of personal information).

[66] *See, e.g.,* S.B. 1238, 2003 Leg., 1st Sess. (Ariz. 2023) (biometrics identifiers; collection; retention; disclosure); Kentucky Biometric Identifiers Privacy Act, H.B. 483, 2023 Gen. Assemb., Reg. Sess. (Ky. 2023); H.B. 0033 and S.B. 0169, 2023 Gen. Assemb., Reg. Sess. (Md. 2023) (Commercial Law – Consumer Protection – Biometric Data Privacy); H.B. 63, 193d Gen. Ct., 2023 Reg. Sess. (Mass. 2023) (An Act to protect biometric information); S.B. 195, 193d Gen. Ct., 2023 Reg. Sess. (Mass. 2023) (An Act to protect personal biometric data); S.B. 30, 193d Gen. Ct., 2023 Reg. Sess. (Mass. 2023) (An Act relative to protecting sensitive information under the security breach law); S.B. 954 & H.B. 2532, 2023 Leg., 93d Reg. Sess. (Minn. 2023) (A bill for an act relating to private data; establishing standards for biometric privacy; establishing a right of action); Biometric Information Privacy Act, H.B. 1047 & H.B. 1225, 102d Gen. Assemb., 1st Reg. Sess. (Mo. 2023); Biometric Privacy Act, A.B. 1362 & S.B. 4457, 2023-2024 Leg., 246th Reg. Sess. (N.Y. 2023); S.B. 2390, 2023-2024 Leg., 246th Reg. Sess. (N.Y. 2023) (Relates to prohibiting private entities from using biometric data for any advertising, detailing, marketing, promotion, or any other activity that is intended to be used to influence business volume, sales or market share, or to evaluate the effectiveness of marketing practices or marketing personnel); H.B. 121, 2023 Gen. Assemb., 77th Sess. (Vt. 2023) (An act relating to enhancing consumer privacy).

[67] *See, e.g.,* Facial Recognition and Biometric Technology Moratorium Act of 2021, S. 2052, 117th Cong. (2021); National Biometric Information Privacy

over data privacy and security encompasses biometric information, and the FTC recently issued a policy statement directed to the "increasing use of consumers' biometric information" and warning that false or unsubstantiated claims about the accuracy or efficacy of biometric information technologies or about the collection and use of biometric information may violate the FTC Act.[68] Sector-specific laws, most prominently the Healthcare Insurance Portability and Accountability Act (HIPAA), also regulate some biometric information and/or practices related to that information.[69]

Government acquisition and use of biometric information is governed broadly by federal law. At the state and local levels, a growing number of ordinances regulate the acquisition of surveillance technologies and, more recently, ban the use of facial recognition. Recent proposals to expand the use of biometric systems by federal agencies have come under increased scrutiny and have even been reversed in some prominent cases.[70]

Act of 2020, S. 4400, 116th Cong. (2020); American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

[68] *See* Press Release, Fed. Trade Comm'n, FTC Warns About Misuses of Biometric Information and Harm to Consumers: Agency Issues Policy Statement Addressing Emerging Technologies That Might Harm Consumers and Violate the FTC Act (May 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers.

[69] *See* 45 C.F.R. § 164.512.

[70] For example, the Internal Revenue Service reversed its decision to require taxpayers to verify their identities using a private facial recognition service, and the Department of Homeland Security rescinded a proposal to expand the use of biometric verification systems for people applying for immigration benefits. *See* Kimberly Adams and Jesus Alvorado, *About-Face: IRS to stop using ID.me to identify taxpayers*, MARKETPLACE (Feb. 8, 2022), https://www.marketplace.org/shows/marketplace-tech/about-face-irs-to-stop-using-id-me-to-identify-taxpayers; Saira Hussain, *Victory! Biden Administration Rescinds Dangerous DHS Proposed Rule to Expand Biometrics Collection*,

The rapid evolution of the legal landscape in this area means that any summary of existing laws risks becoming outdated even before it is published. Nonetheless, a clear trend has emerged toward increased regulation of biometric information and systems and specifically to treat biometric information as sensitive personal information. To date, with the exception of some primarily local and county-level ordinances, U.S. biometric privacy laws do not entirely prohibit the private use of biometric technologies and/or collection, storage, and use of biometric information. Instead, these laws impose varying notice, consent, storage, and security requirements and limits on the sale, disclosure, and reuse of biometric information.

Notably, recent laws and proposed legislation uniformly treat biometric information as protected information, with some, including California's consumer data privacy law, requiring heightened protections.[71] A related set of laws and proposals require fairness, accountability, and transparency in the development and use of algorithms generally, including those used in biometric systems.[72] These developments all underscore the critical need to pay close attention to the legal and regulatory requirements both when deciding whether to adopt a biometric

ELEC. FRONTIER FOUND. (June 30, 2021), https://www.eff.org/deeplinks/2021/06/victory-biden-administration-rescinds-dangerous-proposed-rule-expand-biometrics.

[71] *See, e.g.*, CAL. CIV. CODE § 1789.140 (West 2023) (defining "sensitive information" to include "The processing of biometric information for the purpose of uniquely identifying a consumer").

[72] *See, e.g.*, *Legislation Related to Artificial Intelligence*, NAT'L CONF. OF STATE LEGISLATURES, https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx (Jan. 31, 2023) ("General artificial intelligence bills or resolutions were introduced in at least 17 states in 2022, and were enacted in Colorado, Illinois, Vermont and Washington. Colorado, Illinois and Vermont created task forces or commissions to study AI.").

system and to ensure continued compliance for existing systems.

The following summary of existing U.S. biometric privacy laws highlights the most common requirements and key differences, with a focus on Illinois's BIPA. BIPA is the leading model for biometric-specific legislation and, because it contains a private right of action, is the most extensively litigated.

B. State Biometric Privacy Laws

1. Biometric/Covered Information Definition

The rapidly evolving nature of biometric technology and the challenges in defining "biometric" have led to legal disputes concerning the definition of "biometrics." Definitions under operative and proposed state statutes vary, and litigation has often centered on these questions. For example, BIPA defines biometric "identifiers" as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, and defines biometric "information" broadly to include any information based on an individual's biometric identifier that is "used to identify an individual." The Illinois statute expressly excludes certain data elements from the definition of biometric "identifiers" or "information" (such as writing samples, photographs, tattoo descriptions, information captured in a health care setting or under HIPAA).

The Virginia Consumer Data Privacy Act (VCDPA) similarly defines biometric information as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."[73]

[73] VA. CODE ANN. § 59.1-575 (2023). The Connecticut Data Privacy Act provides the same definition of "biometric data" as the Virginia law. *See*

California's law uses a different model. The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), defines biometric information broadly as any "physiological, biological or behavioral characteristics" that "is used or is intended to be used singly or in combination with each other or other identifying data, to establish individual identity."[74] The law expressly includes imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted (faceprint, a minutiae template, voiceprint), and keystroke patterns, gait patterns, and sleep, health, or exercise data.[75] This derivative approach extends the law to a newer set of applications that use unique individual traits or behaviors that might not be covered under narrower definitions. It also creates flexibility for the law to encompass future applications.

The CPRA amendments to the CCPA also include biometric information processed "for the purpose of uniquely identifying a consumer" within the new category of "sensitive personal information" for which the law creates additional consumer rights.[76]

How to apply these definitions to newer technologies and different applications—e.g., AI machine-learning systems for facial analysis or recognition that do not use facial geometry, or speech recognition technologies that can understand human speech—and the scope of the exceptions to BIPA is the subject of debate.

CONN. GEN. STAT. § 42-515(4) (2023) (effective July 1, 2023); *see also* Tennessee Information Protection Act, 2023 Tenn. Pub. Acts 408 (same; effective July 1, 2025).

[74] CAL. CIV. CODE § 1798.140 (West 2023).

[75] *Id.*

[76] *Id.* § 1798.140(c) (West 2023).

Competing concerns about ambiguity and clarity in each of these models animate debate not only about effective legislation, but also compliance. This lack of clarity creates substantial risk for organizations that use applications that incorporate biological and behavioral features.

2. Exemptions from Biometric Regulation

Many biometric privacy laws, like other consumer privacy laws, include exemptions for regulated sectors like finance and healthcare that have sector-specific laws regulating the privacy and data security of personal information, including biometrics. For instance, BIPA excludes financial institutions or their affiliates that are subject to Title V of the federal Gramm-Leach-Bliley Act (GLBA), as well as information subject to HIPAA and information collected, used, or stored in a healthcare setting.[77] Many laws also make exceptions for uses that are pursuant to a valid warrant or subpoena or in court proceedings.[78]

Washington's law provides for GLBA and HIPAA exemptions and also carves out use by a law enforcement officer acting within the scope of his or her authority.[79] The Washington law also applies only where the enrollment of the biometric data is for a "commercial purpose," notably exempting from coverage any use "in furtherance of a security purpose."[80] This would seem to carve out using biometric information to authenticate a user's identity as part of a security program.

The exemptions in the Texas law are narrower, carving out only voiceprint data retained by a financial institution or an affiliate of a financial institution under GLBA from the application

[77]· *See* 740 ILL. COMP. STAT. 14/10, 14/25(b), 14/25(c) (2023).

[78]. *See id.* 14/25(a).

[79]. *See* WASH. REV. CODE § 19.375.020(7), 19.375.040 (2023).

[80]. *Id.* § 19.375.020(7).

of the statute.[81] The Texas statute also applies only where the data is captured for a "commercial purpose."[82]

California's CCPA includes similar exemptions for federal sector-specific privacy laws and also exempts from coverage any personal information, including biometric information, collected from publicly available sources.[83] But the law excludes from that exemption publicly available "biometric information collected by a business about a consumer without the consumer's knowledge."[84]

3. Notice and Consent Requirements

Most biometric privacy laws require notice and consent prior to use and/or disclosure, or allow consumers to opt out afterwards or from future disclosures. As with any new regulation, there are concerns about compliance with and enforcement of these procedures.[85]

[81] TEX. BUS. & COM. CODE § 503.001(e) (West 2023).

[82] *Id.* § 503.001(b) and (c).

[83] CAL. CIV. CODE § 1798.140(o) (West 2023).

[84] *Id.*

[85] Although currently there is no comprehensive federal biometric data privacy law, the FTC recently settled an enforcement action under Section 5 of the Federal Trade Commission Act against a company related to its use of facial recognition technology. Decision and Order, Everalbum, Inc., FTC Docket No. C-4743 (May 6, 2021). According to the FTC's complaint, the company violated Section 5's prohibition of "deceptive acts or practices in or affecting commerce" by allegedly (1) promising to delete users' images if they deactivated their accounts, but in fact retaining the images and (2) suggesting on its website that it would only apply facial recognition technology to users' images with users' consent, but actually enabling the technology by default without many users' consent. *See* Press Release, Fed. Trade Comm'n, FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology (May 7, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology.

For example, BIPA requires written notice that biometric identifiers or information are being collected or stored, including notification of the "specific purpose and length of term" for the collection and storage. BIPA also requires a written release from the user prior to the collection or receipt of the biometric identifiers or information.[86]

As noted above, the CCPA as amended by CPRA lists biometric information as a special subcategory of personal information, called "sensitive personal information."[87] The law imposes several requirements on businesses that collect all forms of personal information, including that a business provide notice of what information it collects, whether it sells or shares that information, the length of time it intends to retain that information, and consumers' rights with regard to that information.[88] For sensitive personal information, a business also must

[86] 740 ILL. COMP. STAT. 14/15(a), (b) (2023).

[87] CAL. CIV. CODE § 1798.140(c) (West 2023).

[88] *E.g.*, *id.* § 1798.100(a) (business that controls the collection of personal information must inform consumers at or before the point of collection regarding, e.g., categories of information collected, purposes of collection, length of time the business intends to retain each category of personal information); *id.* § 1708.105(b) (business shall disclose consumer's right to request the deletion of personal information); *id.* § 1798.106 (business shall disclose consumer's right to request correction of inaccurate personal information); *id.* § 1798.121(a) (business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in 1798.121 must notify consumers of use or disclosure and that consumers have the right to limit the use or disclosure of their sensitive personal information); *see id.* § 1791.130 (other provisions regarding Notice, Disclosure, Correction, and Deletion Requirements); § 1791.135 (additional provisions regarding disclosure and consent in the context of Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information); *see also, e.g.*, *id.* § 1798.110(c) (information required to be disclosed to consumers upon request).

disclose the purposes for the collection.[89] The CCPA further requires that collection, use, and retention of personal information be "reasonably necessary and proportionate" to achieve those purposes.[90] The CCPA limits some notice obligations when a consumer's sensitive personal information is being used for certain permitted purposes, including ensuring security and integrity and verifying a consumer's information.[91] This arguably could permit a business to use biometric information for authentication purposes without providing consumers a notice of their right to limit those uses, but only if the business uses the biometric information solely for such purposes and the business meets the statute's other notice and use requirements.[92]

Like the CCPA, the VCDPA includes biometric data within a category labeled "sensitive information." But the VCDPA goes further than California by prohibiting collection and processing of biometric data unless a business obtains "freely given, specific, informed, and unambiguous agreement" from the consumer.[93]

Colorado's Privacy Act mirrors Virginia's heightened consent requirement and also specifically prohibits obtaining consent by: (1) "[a]cceptance of a general or broad terms of use"; (2) "[h]overing over, muting, pausing, or closing a given piece of content"; and (3) and "[a]greement obtained through dark patterns."[94]

[89] *Id.* § 1798.140(c).

[90] *Id.* § 1798.100(a).

[91] *See id.* §§ 1798.121(a), 1798.140(e)(2), 1798.140(e)(4), 1798.140(e)(5), 1798.140(e)(8).

[92] *See id.*; *see also, e.g.*, *supra* note 64.

[93] VA. CODE ANN. § 59.1-575 (2023).

[94] COLO. REV. STAT. § 6-1-1303 (2023) (effective July 1, 2023).

The Washington law requires disclosure given "through a procedure reasonably designed to be readily available to affected individuals" prior to enrolling a biometric in a database.[95] The law specifies that the "exact notice and type of consent required to achieve compliance . . . is context-dependent" but is something less than affirmative consent.[96] The Washington law also requires consent for new uses or disclosures where a biometric is enrolled or disclosed for a commercial purpose in a manner "that is materially inconsistent with the terms under which the biometric identifier was originally provided."[97]

4. Sale and Disclosure of Biometric Data

Current and proposed laws address the sale and disclosure of biometric data by prohibiting or restricting the sale or profiting from biometrics as well as placing restrictions on their disclosure. For example, BIPA requires notice and prior consent for any disclosure of biometric data to a third party.[98] Moreover, BIPA prohibits "private entit[ies] in possession of a biometric identifier or biometric information" from selling, leasing, trading, or "otherwise profit[ing]" from a person's biometric identifiers or biometric information.[99] The scope and application of this provision, however, remains unclear. For example, some argue that a private entity that sells a "biometric device" or hosts such data for a fee is "otherwise profiting" from a person's biometrics, while others contend such indirect "profiting" not involving the sale of biometric information is outside the scope of

[95] WASH. REV. CODE § 19.375.020(2) (2023).

[96] *Id.*

[97] *Id.* § 19.375.020(5).

[98] 740 ILL. COMP. STAT. 14/15(d) (2023); *see also* WASH. REV. CODE § 19.375.020(3) (2023) (permitting disclosure where necessary to provide a product or service explicitly requested by the individual).

[99] 740 ILL. COMP. STAT. 14/15(c) (2023).

BIPA and prohibiting it would substantially curtail or eliminate the ability of companies to provide biometric technology or data hosting.

The CCPA lists biometric information as a category of sensitive personal information with heightened protections. A business that collects biometric information must "[p]rovide a clear and conspicuous link on the business' internet homepages" that will permit the consumer, or a person authorized by the consumer, to limit the use or disclosure of their information.[100] Consumers have the right to limit the use and disclosure of sensitive personal information to those purposes "necessary to perform the services or provide the goods reasonably expected by an average consumer" and for other specific purposes defined in the statute.[101]

5. Retention of Biometric Data

As discussed above, biometric data generally is considered personal information that may pose privacy and security concerns when collected and retained. Some biometric laws address retention requirements by imposing an upper limit on the retention period, pegged to the purposes or services for which the biometrics were collected.[102] Considerations for such laws

[100] CAL. CIV. CODE § 1798.135 (West 2023).

[101] *Id.* § 1798.121; *see also id.* § 1798.140(e)(2) (security and integrity), (4) (short-term, transient use), (5) (performing certain services on behalf of the business, including verifying customer information), (8) (verifying or maintaining the quality and safety of the business's service or device).

[102] For example, BIPA requires a retention schedule and guidelines for destroying biometrics, both of which must be publicly available and allow for retention until the "initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with the private entity, whichever occurs first." 740 ILL. COMP. STAT. 14/15(a) (2023). The Texas law requires retention within a "reasonable period of time" but then caps that period at a year after there is no

include whether there should be exceptions for the specified retention periods (for example, for security, recordkeeping, or law enforcement purposes), what "publicly available" means, and how narrowly to define the initial purposes for the collection.

6. Enforcement and Penalties

Existing biometric privacy laws generally take one or both of two approaches to enforcement of the statute: (1) providing for a private right of action, and/or (2) enforcement by state attorneys general.

BIPA provides a private right of action, allowing individuals to bring claims in court alleging their biometric data was collected, disclosed, or retained in violation of BIPA.[103] California provides a private right of action and statutory damages for the unauthorized access and exfiltration, theft, or disclosure of certain types of personal information, including unique biometric data if obtained together with a person's name.[104] Other states, like Texas and Washington, restrict enforcement to their respective state attorneys general.[105]

longer a valid reason for maintaining the biometric. TEX. BUS. & COM. CODE § 503.001(c)(3) (West 2023). Where the biometric serves the purpose of employee identification, then the biometric must be destroyed within a year after the employment relationship is terminated. *Id*. The Washington statute provides that the entity "may retain the biometric identifier no longer than is reasonably necessary to: (i) Comply with a court order, statute, or public records retention schedule specified under federal, state, or local law; (ii) Protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability; and (iii) Provide the services for which the biometric identifier was enrolled." WASH. REV. CODE § 19.375.020(4)(b)(i)-(iii) (2023).

[103] 740 ILL. COMP. STAT. 14/20 (2023).

[104] CAL. CIV. CODE § 1798.150 (West 2023).

[105] WASH. REV. CODE § 19.375.030(2) (2023); TEX. BUS. & COM. CODE § 503.001(d) (West 2023).

These biometric privacy laws also provide for monetary penalties and other compensation. BIPA, for example, provides that the prevailing party "may recover" the greater of a specified liquidated damages or actual damages, as well as reasonable attorneys' fees and costs.[106] The statute of limitations for a BIPA claim is five years,[107] and claims under sections 15(b) and (d) accrue with each collection and disclosure of a person's biometric identifier or information,[108] leading to potentially staggering statutory damages. Other states provide a statutory cap per violation.[109]

7. Security

The current and proposed biometric-specific privacy laws typically impose general standards for data security. For example, BIPA and the Texas law require the storage, transmission, and protection from disclosure "using the reasonable standard of care within the private entity's industry" and "in a manner that is the same as, or more protective than, the manner in which the private entity stores, transmits, and protects other confidential and sensitive information."[110] The Washington law requires "reasonable care."[111]

[106] BIPA provides that a prevailing party "may recover" for each violation the greater of liquidated damages of $1,000 (negligent violations) or $5,000 (intentional or reckless violations) or the party's "actual damages." 740 ILL. COMP. STAT. 14/20(1) and (2) (2023). BIPA also provides that a prevailing party "may recover" reasonable attorneys' fees and costs. *Id*. 14/20(3).

[107] Tims v. Blackhorse Carriers, Inc., 216 N.E.3d 845 (Ill. 2023).

[108] Cothron v. White Castle Sys., Inc., 2023 IL 128004 (Ill. 2023).

[109] For example, Texas caps civil penalties at $25,000 per violation. TEX. BUS. & COM. CODE § 503.001(d) (West 2023).

[110] 740 ILL. COMP. STAT. 14/15(e) (2023); TEX. BUS. & COM. CODE § 503.001(c)(2) (West 2023).

[111] WASH. REV. CODE § 19.375.020(4)(a) (2023).

General privacy laws that encompass biometrics also require a baseline level of security. For example, California's law permits private rights of action where a data breach results from a business's "violation of the duty to implement and maintain reasonable security procedures and practice appropriate to the nature of the information."[112]

The general trend in data security laws is toward more specific requirements, though there is debate whether that approach is appropriate given the rapidly evolving security threat landscape. For example, the NY SHIELD Act, which includes "biometric information" in its definition of "private information" regulated under the statute, requires reasonable safeguards to protect the security, confidentiality, and integrity of private information, including its disposal.[113] Likewise, the VCDPA requires data controllers to conduct and document a data protection assessment prior to processing biometric data.[114]

[112] CAL. CIV. CODE § 1798.150 (West 2023).

[113] Stop Hacks and Improve Electronic Data Security (SHIELD) Act, N.Y. GEN. BUS. LAW § 899-bb (McKinney 2023).

[114] VA. CODE ANN. § 59.1-578 (2023).

V. SYSTEM SELECTION AND DESIGN

The legal issues identified above illustrate some of the risks posed by the use of biometric systems, but in most U.S. jurisdictions, existing laws address only a relatively small subset of the issues these systems raise or are perceived to raise. In addition, biometric systems incorporate advanced technologies, including algorithms, machine learning, and artificial intelligence, that also have come under increased regulatory scrutiny.[115]

More broadly, the collection of biometric information generally, and some biometric modalities in particular, like facial recognition, may pose reputational risks beyond legal liability. As a result, organizations considering implementing biometric systems and professionals advising those organizations should consider not only existing legal requirements and the likelihood that those requirements will change, but also the broader reputational risks that could arise from using these systems.

The process of selecting or designing biometric recognition systems presents organizations the opportunity to make intentional choices that can mitigate the risks these systems pose to users and the organizations implementing them. This section identifies several general considerations organizations should consider, including:

Biometric Modality: Each biometric modality offers different benefits and poses different risks that should be assessed in determining whether a system fits a specific application, including the legal, security, and privacy risks it poses relative to other modalities.

System Design and Accuracy: Accuracy depends on the entire system, not only the algorithm used in it. While generally

[115] *See, e.g.*, Alex Engler, *The EU and U.S. are starting to align on AI regulation*, BROOKINGS (Feb. 1, 2022), https://www.brookings.edu/blog/techtank/2022/02/01/the-eu-and-u-s-are-starting-to-align-on-ai-regulation.

speaking, biometric systems across all modalities are increasingly accurate, the actual performance of each system will vary substantially depending on how it is configured and used.

Privacy and Nondiscrimination: Biometric information generally is treated as protected and sometimes sensitive information that implicates user privacy and discrimination concerns, which should be assessed and mitigated.

Security and Integrity: Protecting biometric data requires both security and integrity. A key element of both aspects is mitigating the risk that a biometric template could be reused across different systems and/or reverse-engineered to identify the original biological feature used to generate it.

A. Biometric Modality

Biometric systems offer different benefits and pose some distinct risks compared to traditional identity verification methods. When deciding whether to use a biometric system by itself or in combination with other recognition methods, it is important to consider whether the distinctive features of biometric systems are necessary and suited to the application and the business objective.

It is equally important to recognize that each biometric modality offers a different mix of benefits and risks. For example, people's faces are a fundamentally public feature, commonly visible and exposed. This fact, coupled with the ability for technology to effectively perform facial recognition on photographs or surveillance video, regardless of whether the subject purposefully engaged in the recognition process, gives rise to a broad range of privacy concerns.[116] Those same features,

[116] Privacy concerns regarding facial recognition will be addressed in a forthcoming companion publication, The Sedona Conference, *Commentary on Notice and Consent Principles for Facial Recognition Technology*.

however, also offer distinctive benefits, including the ability to conduct remote identity verification.[117]

Biometric systems built around finger scans or iris recognition typically require the active participation of the subject to perform any biometric recognition. The addition of "liveness detection" features to such systems can further ensure that the subject is knowingly present as a participant in each biometric recognition event. In addition to being relatively private, irises and fingers are examples of features whose rich biological complexity mean that templates can be derived from them that extract only a relatively small fraction of the available biological information. This limited extraction of biological detail can help in designing templates that cannot be usefully repurposed outside of the original system.

As discussed above, biometric systems increasingly incorporate more than one modality. Among other things, a multimodal system can provide benefits including increased security, higher accuracy, and reduced bias. At the same time, by collecting two or more biometric features, such systems increase privacy, security, and related risks.

B. System Design and Accuracy

The accuracy of each biometric system varies significantly, largely depending on what aspect of system performance is measured. For example, a system may perform well when measuring the overall percentage of correct identifications but poorly when measuring its ability to correctly identify a single individual across multiple different photos. Accuracy also depends on quality of the hardware and software associated with

[117] *Id.*

the system, as well as how a system is configured and used in a specific application.[118]

The following list identifies and briefly describes the most significant factors that can affect the accuracy of biometric systems. These factors operate together to determine the accuracy of a given biometric system.[119]

Input Image Quality: The quality of the input (such as an image or audio) used to create the biometric template at the enrollment phase and of the probe data or image used to verify or identify a person directly affects the accuracy of the system. For example, a face recognition system that requires a subject to position its face within a prescribed zone on a high-definition camera will have a higher accuracy than one based on low-resolution surveillance video.

Aging: Some biometric characteristics (most notably facial features, but also voice) change over time, reducing the accuracy of the system.

Architecture and Training Data: The accuracy of algorithms used across different biometric systems can vary significantly and can be influenced by the quality, quantity, and diversity of the data used to train the system. As discussed, different demographic groups may experience different rates of accuracy from the same systems and algorithms.

[118] Generally speaking, the accuracy of biometric systems using the most common modalities of fingerprint, face, and iris have improved dramatically during the last several years, with several facial recognition systems performing more accurately than trained human reviewers in the ongoing Facial Recognition Verification Testing (FRVT) program conducted by NIST. *See NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, *supra* note 57.

[119] *See generally*, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES, *supra* note 37; A PRIMER ON BIOMETRICS FOR ID SYSTEMS, *supra* note 38, at 74.

Skill/Training/Experience of Human Examiner: In systems where a human is involved in the process, the skill, training, and experience (including implicit biases) of each individual examiner can strongly influence the results and either reduce or increase the overall accuracy.

Search Parameters: Biometric systems often permit users to define the parameters of the search in ways that can influence accuracy by, for example, calibrating the system to require a relatively closer match to the probe image or, conversely, in 1:n identification systems requiring that the system return a set number of matches regardless of confidence level.

One basic measure of the accuracy of a biometric system focuses on the rate of false matches ("false positives") and the rate of false nonmatches ("false negatives"). Each time a system captures a person's biometric, the resulting template will be different and can be different to varying degrees. The algorithm used in the data matching process therefore must estimate whether the new template is sufficiently similar to the stored one.

This means that calibrating a system's algorithm to accept a greater range of variability in the new template to reduce the number of false negatives will increase the number of false positives, and vice versa. The desired balance will vary depending on the specific technology and its individual implementation. For example, configuring a system to prioritize efficiency and access may require accepting a larger number of false positive identifications by permitting the system to accept a larger variation in templates. By contrast, prioritizing security requires accepting a larger number of false negatives to ensure that the system accepts only very closely matched templates.[120]

[120] *See Biometric recognition and authentication systems: Measuring performance*, NATIONAL CYBER SECURITY CENTRE, https://www.ncsc.gov.uk/collection/biometrics/measuring-performance (last visited May 10, 2024).

ISO recognizes three kinds of biometric system evaluations: technology, scenario, and operational. NIST evaluations have documented increasing accuracy on technical evaluations for the top-performing systems in major modalities but also substantial differences among systems.[121] Scenario and operational testing are less common but are important to identify how systems work under the actual conditions in which a system operates. Even systems that incorporate algorithms that perform well under NIST's technical evaluations may perform less well in real-world conditions.[122] Independent scenario and operational testing of facial recognition systems has demonstrated that accuracy depends on the entire system configuration, including the quality of the equipment used to acquire images and the conditions under which they were created.[123]

C. *Security and Integrity*

Well-designed biometric systems emphasize process integrity as much as secrecy to ensure that the chain of custody from sample capture, comparison, and returning results are protected from tampering or manipulation, even by an imposter armed with stolen or publicly captured biometric data. It is impossible to comprehensively define the specific measures that meet the "reasonable security" standard that most biometric laws require. Nonetheless, as many of these laws treat biometric

[121] *See NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, *supra* note 57.

[122] *See* YEVGENIY SIROTIN & ARUN VEMURY, DEMOGRAPHIC VARIATION IN THE PERFORMANCE OF BIOMETRIC SYSTEMS: INSIGHTS GAINED FROM LARGE-SCALE SCENARIO TESTING, DHS SCIENCE AND TECHNOLOGY (2021), https://www.dhs.gov/publication/demographic-variation-performance-biometric-systems.

[123] *See* Yevgeny Sirotin, *'Bias' in face recognition: some facts*, LINKEDIN (Oct. 16, 2019), https://www.linkedin.com/pulse/bias-face-recognition-some-facts-yevgeniy-sirotin-phd/.

data as sensitive, it is critical to develop an appropriate security program addressing the collection, storage, and use of biometric information. Multiple authorities, including ISO, a leading international standards body, identify the following elements for biometric information security that entities could consider adopting in whole or in part in developing their programs for biometric information security:[124]

Security: It should be computationally infeasible to reverse a protected template back to the original biometric characteristic; well-designed systems use proprietary templates and algorithms that are not interoperable across systems.

Diversity: If the protected template is obtained by an attacker, it should be impossible to use it in a different database or system.

Revocability: If a protected template is compromised, it should be straightforward to revoke it and replace it with a new protected template based on the same biometric characteristic.

Performance: The protection scheme used to achieve the previous three principles should not materially degrade the system's false acceptance or false rejection rates.

One of the distinctive security challenges raised by biometric recognition systems is that the process of comparing stored templates to newly submitted input data is a process that requires direct access to the data in the template. Consequently, certain data protection techniques that rely on keeping sensitive data encrypted (for example, the use of hash functions, which are

[124] JAIN, *supra* note 4, at 286–87; *see also* ISO/IEC 24745:2022, *Information Security, Cybersecurity and Privacy Protection—Biometric Information Protection*, INT'L STANDARDS ORG. (2022), https://www.iso.org/standard/75302.html (collapsing these into three security requirements for secure biometric systems: i) unlinkability and renewability; ii) irreversibility; and iii) performance preservation).

commonly used to protect passwords in an encrypted format) are inapplicable to biometric recognition systems. Instead, a well-designed biometric recognition system will deploy other techniques, in keeping with the principles above, to provide comparable protections.[125]

Securing a biometric system involves protecting both the algorithm used to create biometric templates as well as the templates the algorithm generates using "reasonable" security practices, which may include encrypted storage, appropriate access controls, and/or access logging and monitoring.[126] In addition, consideration should be given to segregating the algorithm used to create biometric templates from the templates themselves, as doing so may lower the risks that both aspects will be disclosed in a security incident, and thus the risk that the incident could allow an attacker to impersonate an individual.[127]

Perhaps most important in the biometric context, consideration should be given to whether the algorithm itself can and should be designed in a way such that it holds no value outside of the current system. One of the most common objections leveled against the use of biometric systems is that theft of a biometric template will irrevocably compromise a person's identity because it is impossible to change the underlying physical feature. A biometric system that uses a unique algorithm may ensure that if the algorithm is exfiltrated from that system, it cannot be used to reverse-engineer the biometric attributes of templates from another system.[128]

[125] Anil K. Jain et al., *Biometric Template Security*, EURASIP J. ON ADVANCES IN SIGNAL PROCESSING (2008).

[126] *See* Iynakaran Natgunanathan, et al., *Protection of Privacy in Biometric Data*, 4 IEEE ACCESS 880 (2016).

[127] *Id.*

[128] *See* A PRIMER ON BIOMETRICS FOR ID SYSTEMS, *supra* note 38, at 27–29; ISO/IEC 274745, *supra* note 124.

For the new and existing or enrolled templates, consideration should be given to employing security measures designed to protect against the injection of unauthorized templates.[129] In addition to the general measures just identified, a system's security might be further enhanced by including a method to validate the template against the specific algorithm that was used to create the template. Doing this may ensure that if an unauthorized template is injected into the biometric system, it cannot be used to validate unauthorized credentials, as the injected template would not validate against the specific biometric system algorithm. Note that if biometric system algorithms are designed such that they are proprietary to a given system and dissimilar to other system algorithms, then exfiltration of a protected template itself potentially has no value outside of the existing system and cannot be used on its own to reverse-engineer the biometric attributes of an individual.[130]

Integrating data integrity principles into the design of a biometric system also potentially ensures much greater security. Ensuring data integrity means establishing chain of custody and including data validation steps such as checksums when protected templates are created.[131] Data integrity implemented at the time of protected template creation may ensure that templates are not useful outside of their biometric systems and therefore cannot be used to reverse-engineer the specific biometric data points used to create the template without the corresponding algorithm. Data integrity also can affect system accuracy, specifically as it relates to the balance between false positives and false negatives, which is dependent on the use of

[129] ISO/IEC 274745, *supra* note 124.

[130] A PRIMER ON BIOMETRICS FOR ID SYSTEMS, *supra* note 38.

[131] ISO/IEC 247745, *supra* note 124.

the biometric system (verification, or 1:1 matching, vs. identification, or 1:n matching).

D. Privacy and Nondiscrimination

In general, organizations that are selecting or designing biometric recognition systems should consider how best to protect individual privacy when the biometric data is collected from subjects, when the biometric data is used for its intended purpose, and at any subsequent decision point when new purposes are considered. Each of these steps represents distinct moments of risk and may have different answers. For example, an organization that is collecting biometric data carefully and responsibly, and using it for an appropriate purpose, may find that subsequent reuse of the same data may implicate new privacy concerns or dangers.

The modality selection and system design considerations outlined above can mitigate many of these concerns. For example, a modality such as a finger scan is far more difficult to use to publicly identify a person without their consent than facial or gait recognition. Likewise, using proprietary templates that are difficult to reverse-engineer protects individuals against the risk of identity theft in the case of unauthorized disclosure.

As noted above, an increasing number of jurisdictions impose specific legal requirements to protect biometric information. Most of these laws include consent requirements for obtaining biometric data and restrict how that data can be used and shared. They also impose specific retention requirements and, in some jurisdictions, like California, provide consumers with specific rights.

Organizations should also consider how their systems may directly or indirectly discriminate against different demographic groups. The risks here can arise in different ways, ranging from a system that is less accurate for different races, genders, and ages to applications that are or may be deployed in ways that disproportionately affect specific demographic groups.

The Sedona Conference Commentary on Privilege Logs

A Project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)

Author:

The Sedona Conference

Drafting Team Leaders:

Adam Gajadharsingh
Meghan A. Podolny

Drafting Team:

Toni Baker
Travis Bustamante
MaryBeth Gibson
Nathaniel Giddings
Jennifer Scullion
Hon. Thomas Vanaskie (ret.)
Margot Want

Steering Committee Liaisons:

Rebekah Bailey
Andrea D'Ambra
Tessa Jacob
Sandra Metallo-Barragan
Claudia T. Morgan

Staff editor:

David Lumia

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 1. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

This publication may be cited as follows:

> The Sedona Conference, *Commentary on Privilege Logs*, 25 SEDONA CONF. J. 221 (2024).

PREFACE

Welcome to the final, May 2024 version of *The Sedona Conference Commentary on Privilege Logs ("Commentary")*, a project of The Sedona Conference Working Group 1 on Electronic Document Retention and Production (WG1). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The intent of this *Commentary* is to offer tools and strategies for both responding and requesting parties to mitigate the considerable burdens and competing interests that can be associated with privilege logs, consistent with Federal Rule of Civil Procedure 1's mandate "to secure the just, speedy, and inexpensive determination of every action" while also ensuring that parties have the ability to obtain discoverable evidence. Its primary conclusions include addressing format, timing, and anticipated issues early in the case to help reduce costly discovery disputes later; excluding certain categories of documents from the logging process; considering whether alternative formats to a "traditional" privilege log might be appropriate to the specific needs of the case; affirming that the burden is on the responding party to support its privilege claims; and recognizing that the concept of proportionality is integral to the privilege logging process. The *Commentary*'s appendices include examples of various privilege log formats that provide a visual representation of each format's strengths and weaknesses.

This project was a topic of dialogue at the Working Group 1 Midyear and Annual meetings in 2021, the Midyear Meeting in

2022 and the Midyear Meeting in 2023. Previous drafts of the *Commentary* were published for member comment in 2022 and 2023 and for public comment in February 2024. Where appropriate, the comments received during the public comment period have been incorporated into this final version.

On behalf of The Sedona Conference, I thank drafting team leaders Adam Gajadharsingh and Meghan Podolny for their leadership and commitment to the project. I also recognize and thank drafting team members Toni Baker, Travis Bustamante, MaryBeth Gibson, Nathaniel Giddings, Jennifer Scullion, Hon. Thomas Vanaskie (ret.), and Margot Want for their dedication and contributions, and Steering Committee liaisons Rebekah Bailey, Andrea D'Ambra, Tessa Jacob, Sandra Metallo-Barragan, and Claudia Morgan for their guidance and input.[1]

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; patent remedies and damages; patent litigation best practices; trade secrets; data security and privacy liability; and other "tipping point" issues in the law. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

[1] We also acknowledge the contributions of those who served on the Privilege Logs Brainstorming Group: Kelly Atherton, James Canaday, Todd Itami, Nichole Sterling, Hon. Becky R. Thorson, and Florence Yee.

Kenneth Withers
Deputy Executive Director
The Sedona Conference
May 2024

TABLE OF CONTENTS

EXECUTIVE SUMMARY 228

I. APPLICABLE RULES, PUBLICATIONS, AND INITIATIVES 238

- A. The Requirements and Goals of Rule 26(b)(5) 238
- B. Other Relevant Federal Rules 242
  1. Federal Rule of Civil Procedure 1 242
  2. Federal Rule of Civil Procedure 29 242
  3. Federal Rule of Civil Procedure 45 243
  4. Federal Rule of Evidence 502 245
- C. Federal District and State Local Rules and Standing Orders 246
- D. Evaluation by the Judicial Conference Advisory Committee for Civil Rules 249

II. BURDENS AND CHALLENGES WITH PRIVILEGE LOGGING 251

- A. The Descriptive Narrative 253
- B. Subject Matter 257
- C. Identifying Privileged Parties 259
- D. Basis of Privilege 262
- E. Substantial Volume 263
- F. Timing Pressures 269
- G. Motion Practice 272

III. METHODOLOGIES TO MITIGATE BURDENS 274

- A. Privilege Log Exclusions for Categories Requiring Less/No Substantiation 274
- B. Alternative Construction of Logs 279
  1. Categorical logs 279
  2. Metadata logs 286

3. Metadata-plus-topic logs 292

4. Different logs for different, nontraditional sources 294

C. Early Conferences to Discuss Privilege Logging Issues 295

IV. RESOLVING PRIVILEGE LOG DISPUTES.......................... 302

A. Preliminary communications to narrow issues 302

B. Formal conference 303

C. In camera review 304

V. CONCLUSION 307

APPENDIX A: INTRODUCTION TO WIDGETS EXEMPLARS AND EXAMPLE PRIVILEGE LOGS.................................... 309

A-1 TRADITIONAL PRIVILEGE LOG EXEMPLAR 310

A-2 CATEGORICAL PRIVILEGE LOG EXEMPLAR 311

A-3 METADATA PRIVILEGE LOG EXEMPLAR 312

A-4 METADATA-PLUS-TOPIC EXEMPLAR PRIVILEGE LOG..... 313

APPENDIX B: DESCRIPTIONS OF PRIVILEGE LOG FIELDS........ 314

APPENDIX C: FACT PATTERN FOR WIDGETS EXEMPLARS AND EXEMPLAR DOCUMENTS....................................... 325

EXECUTIVE SUMMARY

When a party withholds otherwise responsive documents in discovery based on the attorney-client privilege, work-product doctrine, or some other protection,[2] it must satisfy the requirements of the relevant jurisdiction for explaining the bases for withholding production. This *Commentary* focuses primarily on cases in federal courts and, therefore, the Federal Rules of Civil Procedure, but where helpful, some state rules and cases are referenced.

The operative rule for withholding otherwise discoverable information based on the assertion of a privilege or protection is Federal Rule of Civil Procedure 26(b)(5)(A). This Rule provides two primary requirements for a responding party to withhold information as privileged—the party must (1) "expressly make the claim" and (2) describe the nature of the information in such a way that allows the receiving party to assess the claim. This Rule, however, does not specify *how* the responding party must satisfy its obligation. This ambiguity has led to responding parties employing a variety of approaches to substantiate their assertions of privilege, with courts and commentators noting that some forms of substantiation can be more problematic, including being less informative, than others.[3]

[2] Unless stated otherwise herein, references to "privilege" are intended to include the attorney-client privilege, work product doctrine, common-interest doctrine, governmental deliberative process privilege, and any other potential privilege, doctrine, or protection a party may assert as a basis for withholding relevant documents, in whole or in part, in discovery.

[3] *See, e.g.*, Chevron Corp. v. Weinberg Grp., 286 F.R.D. 95, 99 (D.D.C. 2012) ("For entry after entry, one part of the description for a particular category is exactly the same. This raises the term 'boilerplate' to an art form, resulting in the modern privilege log being as expensive to produce as it is useless."). *See also* The Sedona Conference, *Commentary on Protection of Privileged ESI*, 17 SEDONA CONF. J. 95, 155 (2016) ("[T]he current method used

Rule 26(b)(5) does not explicitly require the creation and exchange of a privilege log, nor does it define what information must be provided.[4] However, the most common tool parties have used to satisfy their obligation under Rule 26(b)(5) is a "traditional" privilege log.[5] Generally speaking, a traditional privilege log is a table providing the following information about each withheld document: Privilege Log ID Number; Bates Number (if partially produced); Date; Author (for documents) or From/Sender (for communications like email); Recipients (To/CC/BCC); Privilege Asserted; Privilege Narrative/ Description; and possibly Filename or Email Subject.[6] This

by most parties for identifying privileged documents and for creating privilege logs appears to be a broken process."); Report of the Special Committee on Discovery and Case Management in Federal Litigation of the New York State Bar Association, June 23, 2012, at 73, https://nysba.org/app/uploads/2020/02/Discovery-and-Case-Management-Final-Report.pdf ("Most commercial litigation practitioners have experienced the harrowing burden the privilege log imposes on a party in a document-intensive case, especially one with many e-mails and e-mail strings.").

[4] As the Committee Notes indicate, "The rule does not attempt to define for each case what information must be provided when a party asserts a claim of privilege or work product protection." FED. R. CIV. P. 26 advisory committee's note to 1993 amendment.

[5] This *Commentary* uses the term "traditional privilege log" or "traditional log" to refer to a document-by-document log that typically includes factual information about a document, as well as a narrative description of basis for claiming privilege over the withheld document.

[6] "'[T]he customary contents of a privilege log' include 'a description of the type of document[,] . . . its topic, date, the writer and recipient, and an explanation as to why the matter is deemed to be privileged (which privilege was being invoked and on what grounds).'" 3d Eye Surveillance, LLC v. United States, 155 Fed.Cl. 355, 361 (Fed. Cl. Aug. 27, 2021) (alterations in original) (quoting Yankee Atomic Elec. Co. v. United States, 54 Fed. C. 306, 309 (2002)); *see* Trudeau v. N.Y. State Consumer Prot. Bd., 237 F.R.D. 325, 335 (N.D.N.Y. 2006) (requiring log to contain: "(1) the identity of each person listed as author and their role in preparing the documents; (2) the identity of

traditional privilege log is arguably the most thorough and, therefore, defensible method for "expressly describing" the bases for withholding documents as privileged.[7] It is also typically the most costly and burdensome to prepare.

Most of the elements of a traditional log can be generated fairly easily for electronically stored information ("ESI"), assuming metadata[8] exists for the document, by exporting relevant fields from a document review platform into a spreadsheet. Determining the Privilege Asserted and crafting a custom Privilege Narrative/Description, however, requires

each recipient, the role in which they received the documents and whether they are a party or non-party; (3) a more elaborate description of the specific document, or specific portion of the document, which is claimed to be protected by any privilege, without revealing the substance of the privileged communication; (4) identify any bate stamp number or any other identifiable notation; and, (5) identify the type of privilege being asserted (i.e., attorney-client privilege, work product, deliberative process, executive privilege).").

[7] *See generally In re* Imperial Corp. of Am. v. Shields, 174 F.R.D. 475, 478 (S.D. Cal. 1997) ("That format has been, undoubtedly will, and should remain, the traditional format. However, that paradigm is not rigid and inflexible."); Apple Inc. v. Samsung Elecs. Co., 306 F.R.D. 234, 237 (N.D. Cal. 2015) ("In the Ninth Circuit, a privilege log must identify (a) the attorney and client involved, (b) the nature of the document, (c) all persons or entities shown on the document to have received or sent the document, (d) all persons or entities known to have been furnished the document or informed of its substance, and (e) the date the document was generated, prepared, or dated." (internal citation and quotes omitted)); Benson v. Rosenthal, No. CV 15-782 Section "H" (2), 2016 WL 1046126, at *9 (E.D. La. Mar. 16, 2016) (requiring "basic information, including the author, recipient, date and general nature of the document").

[8] Metadata is "the generic term used to describe the structural information of a file that contains data about the file, as opposed to describing the content of a file." The Sedona Conference, *The Sedona Conference Glossary: eDiscovery and Digital Information Management, Fifth Edition*, 21 SEDONA CONF J. 263, 337–38 (2020). For example, metadata might include the author of an electronic document, or the date it was last modified.

analysis for each document and, depending on the complexity of the document, can take significant time to draft a defensible custom privilege description. As a result, including these elements can increase the amount of time, and thus burden, associated with creating a traditional privilege log, particularly if a responding party (the party preparing the privilege log) is withholding a large number of documents on the basis of privilege.[9] With the proliferation of ESI in discovery, this situation presents more frequently and can result in the responding party withholding thousands or tens of thousands of documents based on claims of privilege. The time and cost incurred in the effort to form descriptive sentences for each entry on these voluminous logs, as is frequently conducted for traditional privilege logs, can be burdensome.[10] Nevertheless,

[9] Unitedhealth Grp. Inc. v. Columbia Cas. Co., No. CV 05-1289 (PJS/SRN), 2010 WL 11537514, at *26 (D. Minn. Aug. 10, 2010) ("Because many of the document requests at issue in this motion specifically call for privileged or work product protected discovery, and because of the sheer breadth of the requests and estimated volume of responsive documents, the cost and burden of a document-by-document privilege log would be staggering.").

[10] *See* Auto. Club of N.Y., Inc. v. Port Auth. of N.Y. & N.J., 297 F.R.D. 55, 60 (S.D.N.Y. 2013) (quoting Committee Note to Local Rule 26.2: "With the advent of electronic discovery and the proliferation of e-mails and e-mail chains, traditional document-by-document privilege logs may be extremely expensive to prepare, and not really informative to opposing counsel and the Court."); First Horizon Nat'l Corp. v. Certain Underwriters at Lloyd's, No. 2:11-CV-02608-SHM-DKV, 2013 WL 11090763, at *7 (W.D. Tenn. Feb. 27, 2013) (quoting FED. R. CIV. P. 26 advisory committee's notes to the 1993 amendment: "Details concerning time, persons, general subject matter, etc., may be appropriate if only a few items are withheld, but may be unduly burdensome when voluminous documents are claimed to be privileged or protected."); EPAC Techs., Inc. v. Harpercollins Christian Publ'g, Inc., No. 3:12-CV-00463, 2018 WL 3628890, at *1 (M.D. Tenn. Mar. 29, 2018) (citing FED. R. CIV. P. 26 advisory committee's note to 1993 amendment that document-by-document log may be unduly burdensome when voluminous documents

the responding party has a legal obligation to satisfy the requirements of Rule 26(b)(5). This *Commentary* does not propose shifting the responding party's obligations to the requesting party. Rather, this *Commentary* provides options for how responding parties can reduce the burden of satisfying their obligations and how parties can engage in constructive discussions to minimize disputes.

The privilege logging process can also raise issues for the requesting party (i.e., the party receiving the privilege log). These issues typically relate to the amount and nature of information on the privilege log. Specifically, a privilege log with fewer details can impair the requesting party's ability to understand the assertion of privilege, leaving the party to guess as to whether (or not) privilege properly attaches to the withheld documents.[11] Additionally, a responding party may intend to produce its privilege log only after it substantially completes its productions or on a "rolling basis."[12] This delay

are claimed to be protected); *see also* First Horizon Nat'l Corp. v. Houston Cas. Co., No. 2:15-cv-2235, 2016 WL 5867268, at *6 (W.D. Tenn. Oct. 5, 2016) (must establish undue burden with specificity and articulate explicitly why production of an itemized and descriptive privilege log is unduly burdensome); Mfrs. Collection Co., LLC v. Precision Airmotive, LLC, No. 3:12-CV-853-L, 2014 WL 2558888, at *3 (N.D. Tex. June 6, 2014); Patriot Rail Corp. v. Sierra R.R., No. 2:09-CV-0009 TLN AC, 2016 WL 1213015, at *2 (E.D. Cal. Mar. 29, 2016); Tyco Healthcare Group LP v. Mut. Pharm. Co., No. 07-1299 (SRC)(MAS), 2012 WL 1585335, at *4 (D.N.J. May 4, 2012).

[11] Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251, 265 (D. Md. 2008) ("In actuality, lawyers infrequently provide all the basic information called for in a privilege log, and if they do, it is usually so cryptic that the log falls far short of its intended goal of providing sufficient information to the reviewing court to enable a determination to be made regarding the appropriateness of the privilege/protection asserted without resorting to extrinsic evidence or *in camera* review of the documents themselves.").

[12] The term "rolling basis" typically means that instead of producing all documents by a single date certain (e.g., thirty days after the request for

may impair the requesting party's ability to perform a timely analysis of the assertions of privilege and, if privilege is determined to have been improperly asserted, make use of the later-produced documents earlier in the litigation.

Not surprisingly, the competing interests—and countervailing burdens and rights—of requesting and responding parties in discovery can lead to disputes about how and when a responding party will substantiate its assertions of privilege, and if a privilege log is used, whether the form and content of that privilege log are sufficient. This *Commentary* outlines the burdens that can be associated with privilege logs for *both* responding and requesting parties and presents tools and strategies that can mitigate them. However, one size does not fit all, and litigants and the courts should consider the specific needs of their case, as well as any specific requirements of specific courts or judges, when deciding which of the recommendations in this *Commentary*, if any, should be employed.

Consistent with Federal Rule of Civil Procedure 1, which encourages parties "to secure the just, speedy, and inexpensive determination of every action,"[13] as well as *The Sedona Conference Cooperation Proclamation*,[14] which encourages parties to work together to resolve discovery issues, this *Commentary*

production is received), a party will produce portions of documents in tranches over time. *See, e.g.*, O'Donnell/Salvatori Inc. v. Microsoft Corp., 339 F.R.D. 275, 276 (W.D. Wash. 2021) ("Microsoft produced documents to ODS on a rolling basis, per the Court's order, making productions on May 17, July 2, August 9, and August 19, 2021."); Gugino v. City of Buffalo, No. 21-CV-283V(F), 2021 WL 5239901, at *3 (W.D.N.Y. Nov. 10, 2021); Urban Air Initiative, Inc. v. Env't Prot. Agency, 442 F. Supp. 3d 301, 312 (D.D.C. 2020).

[13] FED. R. CIV. P. 1.

[14] *The Sedona Conference Cooperation Proclamation*, 10 SEDONA CONF. J. 331 (2009 Supp.), *available at* https://thesedonaconference.org/publication/The_Sedona_Conference_Cooperation_Proclamation.

outlines how parties and, if necessary, the courts can cooperatively address the burdens—to the responding parties, the requesting parties, and the courts—associated with privilege logs. The primary conclusions and recommendations in this *Commentary* are as follows:

1. Because not all cases are the same, the methods by which a responding party may satisfy its requirements under Rule 26(b)(5) depend on the case, including the procedures set forth in local rules or standing orders.[15] The parties should address privilege log format, timing, and anticipated issues, as well as contemplate procedures for seeking court assistance in resolving any privilege disputes, early in their case to help reduce costly discovery disputes later. Consistent with the Rule revisions being evaluated by the Advisory Committee on Civil Rules,[16] which this *Commentary* supports, this discussion should begin as part of the Rule 26(f) conference and be incorporated into the Rule 16(b) scheduling order, to the extent the parties have sufficient information at that time.
2. Parties should discuss whether certain categories of documents, such as communications between a client and its outside litigation counsel about the litigation after a complaint has been filed, can be excluded from a privilege log in the first instance. This *Commentary* supports such exclusions as an

[15] *See* Oracle USA, Inc. v. Rimini St., Inc., No. 2:10-CV-00106-LRH-VCF, 2020 WL 5750850, at *4 (D. Nev. Sept. 25, 2020) (a traditional document-by-document log is not mandated by Rule 26(b)(5) and privilege logs in general are simply one of the ways a party may satisfy its obligation).

[16] *See infra* Section I.D.

effective and appropriate way to mitigate privilege logging burdens in most cases.

3. Parties should discuss whether a "metadata plus topic log," or another alternative format, should be employed in their case. This *Commentary* takes the position that a "metadata plus topic log" is a preferred format over the traditional privilege log because it generally is more effective in satisfying the requirements of Rule 26(b)(5) while also mitigating the burdens associated with narrative descriptions. However, alternative formats may vary in effectiveness depending on the documents and factors at issue in each case.

4. Acknowledging that practical burdens exist in the privilege logging process does not mean that the responding party's legal burden of supporting its privilege claims should shift to the requesting party. Consistent with the Federal Rules, the onus is on the responding party to satisfy the requirements of Rule 26(b)(5) and not on the requesting party to justify why those requirements should be met. Although the responding party maintains the legal burden of supporting its privilege claims, this *Commentary* suggests ways that burden can be minimized.

5. The 2015 Amendments to the Federal Rules of Civil Procedure brought the concept of proportionality in discovery to the fore, and in 2018, The Sedona Conference stated that proportionality should be considered and applied to all aspects of discovery,

including the preparation of privilege logs.[17] This *Commentary* does not alter the 2018 Principle.[18]

[17] The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1 (2018). The Sedona Conference has also touched upon privilege logging issues in several prior publications: *The Sedona Conference Cooperation Proclamation*, 10 SEDONA CONF. J. 331 (2009 Supp.) (discussing how cooperation is consistent with zealous advocacy and Rule 1, this proclamation encourages parties to work together to resolve discovery issues and its principles are equally applicable to privilege logs); The Sedona Conference, *Commentary on Protection of Privileged ESI*, 17 SEDONA CONF J. 95, 154–67, 172, 188–89 (2016) (discussing the history of privilege logging and logging practices, while addressing privileges and protection issues, including recommending processes, tools and technologies to reduce the cost and burden of logging); The Sedona Conference, *Commentary on Rule 45 Subpoenas to Non-Parties, Second Edition*, 22 SEDONA CONF J. 1, 60, 82 (2021) (providing an overview of Rule 45 subpoenas to non-parties, the Commentary also discusses the requirement to provide a privilege log to comply, and notes that logging can be a factor in the burden to non-parties and in shifting expenses); The Sedona Conference, *Commentary on the Effective Use of Federal Rules of Evidence 502(d) Orders*, 23 SEDONA CONF J. 1 (2022).

[18] Practitioners should be aware, however, that the application of proportionality to privilege logs continues to be disparately examined by courts after undertaking varying levels of analysis. Some courts directly apply the Rule 26(b)(1) proportionality factors. *See, e.g.*, First Horizon Nat'l Corp. v. Houston Cas. Co., No. 2:15-CV-2235-SHL-DKV, 2016 WL 5867268, at *6 (W.D. Tenn. Oct. 5, 2016) (applying the Rule 26(b)(1) proportionality standard, citing the proportionality factors, and concluding that a traditional document-by-document log, rather than a "categorical log" was proportional); Finger v. Jacobson, No. CV 17-2893, 2019 WL 7557821, at *1 (E.D. La. May 10, 2019) (finding the privilege log "proportional to the needs of the case given the parties' relevant access to the requested materials," may also "aid in resolving the issues in this litigation, the burden or expense does not outweigh its likely benefit," and noting it had no evidence of "any of the other proportionality factors under Rule 26" available as evidence") (internal citations omitted). Other courts discuss whether a privilege log is proportional without any explicit reference to the Rule 26(b)(1) factors. *See,*

e.g., Las Brisas Condo. Homes Condo. Ass'n, Inc. v. Empire Indem. Ins. Co., No.: 2:21-cv-41-KCD, 2023 WL 2788873, *2 (M.D. Fla. Mar. 8, 2023) (agreeing that itemized privilege logs are "not always necessary" because "Rule 26 requires proportionality"); U.S. Bank Nat'l Ass'n v. Triaxx Asset Mgmt., 18-CV-4044-BCM, 2021 WL 1968325, at *5 (S.D.N.Y. Mar. 31, 2021); Norton v. Town of Islip, No. CV043079PKCSIL, 2017 WL 943927, at *8 (E.D.N.Y. Mar. 9, 2017) (determining whether a categorical privilege log is appropriate, courts consider whether its justification is "directly proportional to the number of documents withheld" but not evaluating any of the Rule 26(b)(1) factors); 3rd Eye Surveillance, LLC v. United States, No. 15-501C, 2021 WL 3828654, at *3 (Fed. Cl. Aug. 27, 2021) (ordering revised privilege descriptions to better articulate common interest doctrine claims but stating "the burden of identifying and logging each and every communication between counsel to the parties to the [joint defense agreement] over six years . . . is not proportional to the needs of the case"); *In re* Snap Inc. Sec. Litig., No. CV1703679SVWAGRX, 2018 WL 7501294, at *1 (C.D. Cal. Nov. 29, 2018) (concluding that the logging of documents dated after commencement of the litigation was not proportional to the needs of the case, but no evaluation of the Rule 26(b)(1) factors). Although the drafting team was unable to find a court outright rejecting application of proportionality to privilege logs, one case appears to do so in dicta. *See* Main St. Am. Assurance Co. v. Savalle, No. 3:18CV02073(JCH), 2021 WL 1399685, at *3 (D. Conn. Apr. 14, 2021) (drawing a distinction between whether "the information sought by the subpoena" is disproportional to the needs of the case versus whether "creating the privilege log" is somehow disproportionately burdensome).

I. APPLICABLE RULES, PUBLICATIONS, AND INITIATIVES

A. The Requirements and Goals of Rule 26(b)(5)

Rule 26(b)(5) governs how a party must make a privilege assertion, stating as follows:

> (5) Claiming Privilege or Protecting Trial-Preparation Materials.
>
> > (A) *Information Withheld.* When a party withholds information otherwise discoverable by claiming that the information is privileged or subject to protection as trial-preparation material, the party must:
> >
> > > (i) expressly make the claim; and
> > >
> > > (ii) describe the nature of the documents, communications, or tangible things not produced or disclosed—and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim.[19]

The Committee Notes provide more detail on the goals of Rule 26(b)(5), stating that the Rule "provides a procedure for a party that has withheld information on the basis of privilege or protection as trial-preparation material to make the claim so that the requesting party can decide whether to contest the claim and the court can resolve the dispute."[20]

The Federal Rules of Civil Procedure do not explicitly require "a privilege log," nor do they provide a defined list of the information that must be provided.[21] Although they are

[19] FED. R. CIV. P. 26(b)(5).

[20] FED. R. CIV. P. 26 advisory committee's note to 2006 amendment.

[21] As the Committee Notes indicate, "The rule does not attempt to define for each case what information must be provided when a party asserts

silent regarding format, practitioners have regularly used traditional privilege logs as the mechanism by which parties comply with Rule 26(b)(5)(A) (and Rule 45(e)(2)(A)).[22] Practically speaking, the format of a privilege log can allow a party to "expressly make a claim" of privilege or protection in a way that "describes the nature" of the withheld document "in a manner that, without revealing information itself privileged or protected," allows "other parties to assess the claim."[23]

One of the possible repercussions for not satisfying the requirements of the Rule is waiver of the privilege or protection. When waiver is found, it generally is imposed as a sanction for bad-faith, abusive, or recalcitrant behavior with respect to production of an insufficient log (or providing of no log whatsoever).[24] Thus, parties may be reluctant to diverge from

a claim of privilege or work product protection." FED. R. CIV. P. 26 advisory committee's note to 1993 amendment.

[22] Caudle v. Dist. of Columbia, 263 F.R.D. 29, 35 (D.D.C. 2009) ("A privilege log has become an almost universal method of asserting privilege under the Federal Rules."); *see also* Courtland Co., Inc. v. Union Carbide Corp., No. 2:19-CV-00894, 2021 WL 665532, at *1 (S.D.W. Va. Feb. 12, 2021); Ho v. Ernst & Young, LLP, No. C05-04867 JF HRL, 2008 WL 205595, at *1 (N.D. Cal. Jan. 24, 2008). For an example of a traditional log, *see* Appendix A.1.

[23] *See* FED. R. CIV. P. 26(b)(5).

[24] *See, e.g.*, Evergreen Trading, LLC v. United States, 80 Fed. Cl. 122, 126 n.2 (2007) ("While an inadequate privilege log may be the basis for disallowing a privilege, such a finding is in the nature of a sanction and, at least in the first instance, should be weighed in terms of the intent of the party producing the defective log and against the harm caused by disclosure of what might otherwise be privileged documents." (citations omitted)); Burlington N. & Santa Fe Ry. Co. v. U.S. Dist. Ct. for Mont., 408 F.3d 1142, 1149 (9th Cir. 2005) (rejecting a per se waiver rule, but finding waiver when a sophisticated litigant produced a log five months after the expiration of the Rule 34 time limit); Muro v. Target Corp., 250 F.R.D. 350, 360 (N.D. Ill. 2007) ("[B]lanket waiver is not a favored remedy for technical inadequacies in a privilege log.") (citing Am. Nat'l Bank & Trust Co. of Chi. v. Equitable Life

traditional privilege logs out of concern that if a court finds the associated description insufficient, the privilege will be waived.[25] A more common result, however, is that a court will require the responding party to provide more detailed information to substantiate the assertion of privilege, or order in camera review.[26]

Assurance Soc'y of U.S., 406 F.3d 867, 879 (7th Cir. 2005) (holding that Magistrate Judge abused his discretion by finding that defects in privilege log merited a sanction of blanket waiver, absent a finding of bad faith); E.B. v. N.Y. City Bd. of Educ., No. CV 2002-5118 (CPS)(MDG), 2007 WL 2874862 (E.D.N.Y. Sept. 27, 2007) (holding waiver not an appropriate sanction after delay in producing privilege log).

[25] *See, e.g.*, Meade v. Gen. Motors, LLC, 250 F. Supp. 3d 1387, 1396 (N.D. Ga. 2017) (finding claims of privilege waived where multiple iterations of the privilege log were found inadequate); Neelon v. Krueger, No. 12-CV-11198-IT, 2015 WL 1037992, at *4 (D. Mass. Mar. 10, 2015) (affirming magistrate judge's ruling that categorical privilege log provided inadequate detail and waived privileges and protections as to specific group of documents); *In re* Rivastigmine Patent Litig., 237 F.R.D. 69, 87 (S.D.N.Y. 2006) (finding the vast majority of the categorical justifications provided by the plaintiffs were inadequate, and all corresponding documents must be produced in their entirety); McNamee v. Clemens, No. 09 CV 1647(SJ), 2013 WL 6572899, at *3 (E.D.N.Y. Sept. 18, 2013) (finding the "exceedingly unhelpful" document descriptions resulted in an inadequate privilege log and holding the responding party had waived his claims of privilege by failing to timely produce an adequate log); Maxus Energy Corp. v. YPF, S.A., Nos. 16-11501, 18-50489, 2021 WL 3619900 (D. Del. Aug. 16, 2021) (questioning the confidentiality and privilege applicable to documents withheld in three categories on a categorical privilege log, rejecting the responding party's request for a "redo" with a traditional privilege log, and requiring production).

[26] *See, e.g.*, Johnson v. Ford Motor Co., 309 F.R.D. 226, 234–35 (S.D.W. Va. 2015) ("When a party provides an inadequate or untimely privilege log, the Court may choose between four remedies: (1) give the party another chance to submit a more detailed log; (2) deem the inadequate log a waiver of the privilege; (3) inspect in camera all of the withheld documents; and (4) inspect in camera a sample of the withheld documents.") (quoting Nationwide Mut. Fire Ins. Co. v. Kelt, Inc., No. 6:14–cv–749–Orl–41TBS, 2015

From a responding party's perspective, the goal of a privilege log is to satisfy its burden under Rule 26(b)(5) without waiving privilege over protected information by, for example, disclosing privileged content. From a requesting party's perspective, the privilege log must provide sufficient information to understand the assertion of privilege and evaluate whether there is a good-faith basis to believe nonprivileged documents have been improperly withheld.

A privilege log is not the only option, however, for expressly making a privilege claim.[27] Nor is there a "monolithic form of

WL 1470971, at *9 (M.D. Fla. Mar. 31, 2015)); Coventry Cap. US LLC v. EEA Life Settlements Inc., Civ. A. No. 17 Civ. 7417 (VM) (SLC), 2020 WL 7383940, at *8 (S.D.N.Y. Dec. 16, 2020) (ordering responding party to provide names of attorneys involved in any of the categorical logged communications), *objections overruled*, 2021 WL 961750 (S.D.N.Y. Mar. 15, 2021); EPAC Techs., Inc. v. HarperCollins Christian Publ'g, Inc., Case No. 3:12-cv-00463, 2018 WL 3628890, at *1 (M.D. Tenn. Mar. 29, 2018) (finding categorical log insufficient because of party's failure to provide metadata for each document included within a category and ordering party to amend it); *In re* Aenergy, S.A., 451 F. Supp. 3d 319, 325 (S.D.N.Y. 2020).

[27] *See, e.g.*, Oracle USA, Inc. v. Rimini St., Inc., No. 2:10-CV-00106-LRH-VCF, 2020 WL 5750850, at *5 (D. Nev. Sept. 25, 2020) (privilege log not needed because discussion of category and volume of documents at hearing, along with declarations, was sufficient); Koumoulis v. Indep. Fin. Mktg. Grp., Inc., 29 F. Supp. 3d 142, 150-51 (E.D.N.Y. 2014) (finding no abuse of discretion where the court allowed plaintiffs to use a declaration to satisfy Federal Rule 26(b)(5)(A)); Genesco, Inc. v. Visa U.S.A., Inc., 302 F.R.D. 168, 191–94 (M.D. Tenn. 2014) (plaintiff's counsel submitted affidavits and other documents in lieu of log, and court determined that only certain documents needed to be logged); Fifty-Six Hope Road Music, Ltd. v. Mayah Collections, Inc., No. 2:05-cv-01059-KJD-GWF, 2007 WL 1726558, at *6-8 (D. Nev. June 11, 2007) (endorsing certification in lieu of generating a full privilege log that: (1) attested to the sufficiency of the privilege review; and (2) provided a reasonable estimate of the number of withheld documents, while providing log for any purportedly privileged documents that were shared with third parties).

privilege logs."[28] Simply put, expressly claiming the privilege in a manner or format different from the traditional privilege log (described in the Executive Summary and an exemplar attached as Appendix A.1) is permissible so long as the responding party satisfies its burden to substantiate its assertion of privilege.

B. *Other Relevant Federal Rules*

There are several other Federal Rules that touch on the assertion of privilege.

1. Federal Rule of Civil Procedure 1

As discussed in this *Commentary*, the time, expense, and effort required to create a traditional privilege log can be in tension with Federal Rule of Civil Procedure 1, which requires the rules to "be construed, administered, and employed by the court and the parties to secure the *just, speedy, and inexpensive* determination of every action and proceeding,"[29] particularly with the proliferation of ESI, which can result in parties withholding hundreds or thousands of documents based on an assertion of privilege. This *Commentary* recommends that litigants and the courts be mindful of Rule 1 in discussing how to address and resolve privilege log issues.

2. Federal Rule of Civil Procedure 29

Rule 29 states that "[u]nless a court orders otherwise, the parties may stipulate that . . . other procedures governing or

[28] Securitypoint Holdings, Inc. v. United States, No. 11-268C, 2019 WL 1751194, at *2 (Fed. Cl. Apr. 16, 2019) (citing Deseret Mgmt. Corp. v. United States, 76 Fed. Cl. 88, 91 (2007)); Patriot Rail Corp. v. Sierra R.R., No. 2:09-CV-0009 TLN AC, 2016 WL 1213015, at *2 (E.D. Cal. Mar. 29, 2016) (refraining from opining on log format as long as it permits court and parties to assess the claim of privilege).

[29] FED. R. CIV. P. 1 (emphasis added).

limiting discovery be modified."[30] Many of this *Commentary*'s proposals provide options for negotiation between the parties. While local rules and standing orders should be considered, parties should explore opportunities under Rule 29 to stipulate as to what they are willing to accept in connection with privilege logging, including the content and format, and the court should abide by the terms of that agreement. To avoid disputes, stipulations reached under Rule 29 should be in writing.

3. Federal Rule of Civil Procedure 45

Rule 45(d)(3)(A)(iii) requires the court to quash a subpoena, "on timely motion," where it "requires disclosure of privileged or other protected matter, if no exception or waiver applies . . . ." But a non-party seeking to quash a subpoena because it requires disclosure of privileged materials must substantiate its assertion of privilege.[31]

Pursuant to Rule 45(e)(2), a subpoena recipient asserting privilege must "(i) expressly make the claim; and (ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information

[30] FED. R. CIV. P. 29.

[31] *See, e.g.*, Brown v. Tax Ease Lien Servicing, LLC, No. 3:15-CV-208-CRS, 2017 WL 6940735, at *4 (W.D. Ky. Aug. 21, 2017) ("Because [the non-party] makes merely a blanket assertion of the privilege without providing a privilege log or other means of identifying the affected documents, this ground in support of its motion to quash is unpersuasive.") (internal citations omitted); Dong Gun Shin v. Infinity Ins. Co., No. 1:18-cv-1954-SCJ, 2018 WL 8951202, at *2 (N.D. Ga. Oct. 1, 2018) (declining to quash a subpoena where, *inter alia*, the non-party and related party had not submitted a privilege log such that the court could not "determine whether the contents of the file sought by [the requesting party] are protected by the attorney-client privilege"); *In re* Kidd, No. 3:20-cv-00800 (KAD), 2020 WL 5594122, at *13 (D. Conn. Sept. 18, 2020) (affirming denial of motion to quash due to absence of privilege log).

itself privileged or protected, will enable the parties to assess the claim." Although a non-party is required to satisfy its burden under Rule 45(e)(2)(A), some courts have permitted non-parties to substantiate their assertions of privilege through other, less burdensome means than a traditional privilege log.[32] It is also not uncommon for a subpoenaing party and a responding non-party to agree that a privilege log is not required. However, a non-party's failure to satisfy its burden may result in the non-party waiving privilege, so non-parties should be diligent in complying with relevant rules.[33]

[32] *See, e.g.*, Lake as Tr. of Richard D. Lake Revocable Living Tr. Dated Aug. 24, 2011 v. Charlotte Cty. Bd. of Cty. Commissioners, Case No. 2:20-cv-809-JLB-NPM, 2021 WL 2351178, at *2 (M.D. Fla. June 9, 2021) ("[R]ather than require [the non-parties] to produce privilege logs of withheld or redacted materials, they may categorically withhold or redact privileged communications, and must provide a certification by both the subpoenaed party and [the plaintiff] that none of the withheld or redacted documents were distributed to or reviewed by anyone other than [the plaintiff], [plaintiff]'s counsel, [the non-parties], or their respective staffs.").

[33] *See, e.g.*, *In re* Grand Jury Subpoena, 274 F.3d 563, 575-76 (1st Cir. 2001) ("[A]lthough [Rule 45] does not spell out the sufficiency requirement in detail, courts [consistently] have held that the rule requires a party resisting disclosure to produce a document index or privilege log . . . [or be] deemed to waive the underlying privilege claim.") (internal citations omitted); Schaeffer v. City of Chicago, 19 C 7711, 2020 WL 7395217, at *3 (N.D. Ill. Dec. 15, 2020); Mosley v. City of Chicago, 252 F.R.D. 445, 449 (N.D.Ill. 2008); Williamson v. Recovery Ltd. P'ship, 2:06-cv-292, 2016 WL 4920773, at *2 (S.D. Ohio Sept. 15, 2016); Ensminger v. Credit L. Ctr., LLC, 19-2147-JWL, 2019 WL 6327421, at *4 (D. Kan. Nov. 26, 2019) (rejecting a non-party's argument that he need not comply with a subpoena because it would be burdensome to create a privilege log: "While the court recognizes there are resources involved in creating and evaluating a privilege log, the court does not find it so burdensome as to constitute good cause for granting a protective order"); Meyer v. Bank of Am., N.A., No. 2:18-CV-218, 2018 WL 6436268, at *6 (S.D. Ohio Dec. 7, 2018) (finding universe of 2,700 potentially privileged communications not unduly burdensome, given "(1) the amount in controversy in this case, (2) the importance of the issues at stake, and (3)

Consistent with the Sedona Principles and Rule 1, the party and non-party should confer about potential means of reducing the burden on the non-party associated with preparing a privilege log.[34] If a non-party attempts to substantiate its assertion of privilege through an alternative to a traditional privilege log, it must be mindful that it still carries the burden to provide sufficient information to the requesting party to substantiate the privilege assertions.[35]

4. Federal Rule of Evidence 502

Federal Rule of Evidence 502 clarifies privilege waiver rules in the federal courts and sets out mechanisms whereby parties

the fact that the discovery Plaintiffs requested here is, at least, of 'moderate relevance' to their claims and defenses . . . .") (internal citations omitted); *but see* Dell Inc. v. DeCosta, 233 F. Supp. 3d 1, 3 (D.D.C. 2017) (quashing a subpoena, in part, served on the party's former counsel because it "would impose an undue and disproportionate burden on [former counsel] to prepare a privilege log [for] thousands of documents").

[34] *See* The Sedona Conference, *Commentary on Rule 45 Subpoenas to Non-Parties, Second Edition*, 22 SEDONA CONF. J. 1, 82 (2021) ("The party issuing a subpoena should seek to minimize the burden of privilege claims on the non-party. For example, the issuing party and the non-party may agree to exclude some potentially privileged and protected information from the subpoena based upon dates, general topics, or subjects. To minimize the burden on the non-party, the subpoenaing party should consider alternatives to the traditional privilege log.").

[35] *See, e.g.*, Swasey v. W. Valley City, No. 2:13-CV-768 DN, 2016 WL 6947022, at *2 (D. Utah Jan. 15, 2016) (ordering a non-party to "provide more specificity" regarding roughly 200 emails over a roughly four-year period that the non-party grouped into a single category on its privilege log); *In re* Motion for Protective Ord. for Subpoena Issued Stein L. Firm, No. CV 03-9354 JSL (VBK), 2006 WL 8444493, at *5 (D.N.M. Feb. 10, 2006) (finding waiver where, *inter alia*, "[t]he privilege log that the [non-party] produced listed fourteen categories of documents in summary fashion without the detail that [Rule 45] requires").

can obtain further protections against the waiver of attorney-client privilege and work-product protections.[36]

Rule 502 is comprised of several sections. Rule 502(d), in particular, provides that with a court order, the production of privileged material, whether inadvertent or otherwise, is not a waiver in the case, nor in any other federal or state proceeding, even involving other parties. [37]

C. Federal District and State Local Rules and Standing Orders

While the Federal Rules do not provide specific direction on how a responding party can satisfy its burden to substantiate its assertion of privilege, some federal District Courts have adopted local rules that do so.[38]

For example, the local rules for the U.S. District Court for the Southern and Eastern Districts of New York state, "[W]hen asserting privilege on the same basis with respect to multiple documents, it is presumptively proper to provide the

[36] FED. R. EVID. 502. *See also* The Sedona Conference, *Commentary on Protection of Privileged ESI*, 17 SEDONA CONF. J. 95, 103–04 (2016); The Sedona Conference, *Commentary on the Effective Use of Federal Rule of Evidence 502(d) Orders*, 23 SEDONA CONF J. 1 (2022).

[37] Additional information regarding Rule 502 can be found in The Sedona Conference's *Commentary on the Effective Use of Federal Rule of Evidence 502(d) Orders,* 23 SEDONA CONF J. 1 (2022).

[38] For a compilation survey of various local rules adopted for privilege logs, *see, e.g.*, Lawyers for Civil Justice, Privilege and Burden: The Need to Amend Rules 26(b)(5)(A) and 45(e)(2) to Replace "Document-By-Document" Privilege Logs with More Effective and Proportional Alternatives, 1, 7-10 (Aug, 4, 2020), *available at* https://www.uscourts.gov/sites/default/files/20-cv-r_suggestion_from_lawyers_for_civil_justice_-_rules_26_and_45_privilege_logs_0.pdf.

information required by this rule by group or category."[39] As another example, the U.S. District Court for the District of Connecticut Local Civil Rule 26(e) explicitly states that parties need not log "written or electronic communications between a party and its trial counsel after commencement of the action and the work product material created after commencement of the action."[40]

Some states have also enacted their own rules governing privilege logging. Recently, New York State adopted revised Uniform Rules for the New York Supreme Court and County Court that require parties to "meet and confer at the outset of the case" and affirmatively includes the use of categorical logs in the privilege log discussions.[41] These changes to the State Courts Uniform Rules were adopted and influenced from similar rules in the New York State Supreme Court's Commercial Division.[42] Additionally, the Commercial Division Rules require the responding party to certify "with specificity those facts supporting the privileged or protected status of the information included within the category" and "describe the steps taken to identify the documents so categorized, including but not limited to whether each document was reviewed or

[39] S.D.N.Y. CIV. R. 26.2(c). *See generally* Assured Guar. Mun. Corp. v. UBS Real Estate Secs. Inc., No. 12 CIV. 1579 (HB) (JCF), No. 12 CIV. 7322 (HB) (JCF), 2013 WL 1195545, at *9 (S.D.N.Y. Mar. 25, 2013).

[40] D. CONN. R. 26(e).

[41] N.Y. COMP. CODES R. & REGS. tit. 22 § 202.20-a.

[42] David Ferstendig, *Significant Amendments to Uniform Rules*, NYSBA (Feb. 8, 2021), https://nysba.org/significant-amendments-to-uniform-rules/; David Ferstendig, *Amendments to Uniform Rules*, NYSBA (Mar. 23, 2021), https://nysba.org/amendments-to-uniform-rules/.

some form of sampling was employed, and if the latter, how the sampling was conducted."[43]

Some judges also provide standing orders on what they expect of privilege logs, or what may be excluded from privilege logs. As an example, one judge in the Northern District of Ohio states, "Where the [discovery] dispute involves claims of attorney-client privilege or attorney work product, it is not necessary, unless I order otherwise, to prepare and submit a privilege log."[44] A standing order for a judge in the Middle District of Florida requires the production of privilege logs containing specific information, including "the degree of confidentiality with which the information was treated."[45]

Some courts have developed model orders and programs to explore alternative methods for complying with Rule 26(b)(5). For example, the U.S. Court of Appeals for the Seventh Circuit's Electronic Discovery Committee has a model privilege log order that encourages metadata-only logging, with the option for categorical logging for certain categories that a party deems burdensome to provide on a metadata-only log.[46] This

[43] N.Y. CT. R. 202.70, Rule 11-b(b)(1); *see* Hon. John M. Facciola & Jonathan M. Redgrave, *The Facciola-Redgrave Framework*, 4 FED CTS. L. REV. 20, 47 (2009) (advocating for production of an affidavit by the responding party that attests "to the facts that support the privileged or protected status of document and ESI within that category").

[44] Judge Carr Civil Cases – Case Management Preferences, https://www.ohnd.uscourts.gov/judge-carr-civil-cases-case-management-preferences (last visited May 16, 2024).

[45] Standing Order of Judge Kidd on the Procedure for Assertion of Privilege, www.flmd.uscourts.gov/sites/flmd/files/documents/flmd-standing-order-re-procedure-for-assertion-of-privilege-6-19-mc-42-orl-ejk.pdf (last visited May 16, 2024).

[46] Seventh Circuit Council on eDiscovery and Digital Information, *Model Discovery Plan and Privilege Order*, EDISCOVERY COUNCIL.COM,

Commentary explores these formats in Section III.B and the Appendices. In addition, the U.S. District Court for the Southern District of New York's Pilot Program for Complex Civil Cases makes an explicit recognition that communications with party counsel and work product created after the commencement of an action did not need to be logged.[47]

D. *Evaluation by the Judicial Conference Advisory Committee for Civil Rules*

In mid-2020, the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States began to consider whether to implement changes to Rule 26(b)(5) to address the competing interests of requesting and responding parties in the privilege logging process. As stated in one Advisory Committee report, in some cases privilege logs "imposed considerable burdens," which "escalated as digital communications supplanted other means of communication. The volume of material potentially subject to discovery escalated, and the cost of preparing a privilege log for all of them also escalated. Nevertheless, there were also regular objections that these very expensive and voluminous lists did not really provide the needed information."[48] A Discovery Subcommittee was formed to investigate the issue and received

https://www.ediscoverycouncil.com/content/model-discovery-plan-and-privilege-order (last visited May 16, 2024).

[47] U.S. Dist. Court S.D.N.Y., *In re* Pilot Project Regarding Case Management Techniques for Complex Civil Cases, at 6 (Nov. 1, 2011), https://www.nysd.uscourts.gov/sites/default/files/pdf/Complex_Civil_Rules_Pilot_14.11.14.pdf.

[48] Committee on Rules of Practice and Procedure, Report of the Advisory Committee on Civil Rules, at 3 (Dec. 9, 2022), included in the Committee on Practice and Procedure, Meeting Agenda Book, at 205 (Jan. 4, 2023), https://www.uscourts.gov/sites/default/files/2023-01_standing_committee_meeting_agenda_book_final_0.pdf.

more than 100 written comments, taking a variety of positions.[49] The Advisory Committee issued a report after its October 5, 2021, meeting, noting the "recurrent and stark divide" between plaintiff and defense bars regarding proposed logging formats, the specificity element, costs, and timing of privilege logs.[50]

Ultimately, the Advisory Committee concluded that trying to amend Rule 26(b)(5)(A) to provide an all-purpose solution for every case was not feasible. Instead, the Committee unanimously recommended revising Rule 16(b) and Rule 26(f) to require litigants to discuss issues regarding "the timing and method for complying with Rule 26(b)(5)(A)" in the 26(f) conference and 16(b) scheduling order.[51] This *Commentary* supports encouraging early discussion among parties, promoting negotiation and agreement where possible, or seeking early court intervention when negotiation fails.

[49] Comments on Privilege Logging Practice, https://www.uscourts.gov/sites/default/files/comments_on_privilege_log_practice.pdf.

[50] Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Advisory Committee on Civil Rules, at 17 (Dec. 14, 2021), https://www.uscourts.gov/sites/default/files/advisory_committee_on_civil_rules_-_december_2021_0.pdf.

[51] Report of the Advisory Committee on Civil Rules, at 5, 8 (Dec. 9, 2022), Meeting Agenda Book, at 207, 210 (Jan. 4, 2023), https://www.uscourts.gov/sites/default/files/2023-01_standing_committee_meeting_agenda_book_final_0.pdf.

II. BURDENS AND CHALLENGES WITH PRIVILEGE LOGGING

In evaluating whether the creation of a privilege log in a certain manner would be "unduly" burdensome, some courts look to the scope of a document request and the relevancy of the requested information.[52] Courts often reject conclusory, unparticularized statements regarding the burden of producing a privilege log and require some showing related to "the injurious consequences of insisting upon compliance."[53] This *Commentary* does not seek to define what rises to the level of being "unduly" burdensome in the privilege logging process. Rather, it acknowledges that, to varying degrees, burdens and challenges can exist for both the responding party and requesting party. This Section of the *Commentary* identifies and discusses those burdens and challenges, while Section III provides various mitigation strategies parties should consider to address these burdens and challenges.

Asserting privilege and substantiating that claim with a privilege log can be a complex process that often requires a significant investment of time, money, and business resources. For traditional logs, a review for privilege is often done either (a) as part of the initial relevance/responsiveness review or (b) through a separate privilege review. In the latter case, the potentially privileged documents have been identified either during the initial relevance/responsiveness review or through application of a privilege screen, such as keyword searching

[52] *See, e.g.*, Food Delivery Holding 12 S.a.r.l. v. DeWitty and Assocs. CHTD, 538 F. Supp. 3d 21, 31 (D.D.C. 2021).

[53] Garcia v. E.J. Amusements of N.H., Inc., 89 F. Supp. 3d 211, 216 (D. Mass. 2015) (citing New England Compounding Pharm., Inc. Prod. Liab. Litig., 2013 WL 2058483, at *6 (D. Mass Nov. 13, 2013)); *see also Food Delivery Holding*, 538 F. Supp. 3d at 31 ("The Court will not simply assume that creation of a privilege log would be unduly burdensome absent evidence from DeWitty on the issue.").

and/or machine-learning tools. Typically, at the first level of privilege review, the reviewing attorney selects coding fields within a document review platform that provide information to support the assertion of privilege, particularly as it relates to the Privilege Asserted and Privilege Narrative/Description fields. Those coded fields, as well as certain document metadata, are exported and combined to computer-generate an initial privilege log entry for each document. This initial privilege log entry is then, in most cases, reviewed by senior level attorneys to ensure accuracy, perhaps on a sampling basis in larger data sets. This process usually occurs after the first-level review has completed, in part because information discovered later in the review helps to further inform the legal team's awareness of the extent and scope of privileged documents. Additionally, because privilege determinations can prove to be thorny, the review of the privilege log entries is usually conducted by more experienced (and thus, more expensive) attorneys.

Apart from the multiple layers of review often required for potentially privileged documents, the burdens of privilege logging are most pronounced in the creation of descriptive narratives, which identify the subject matter and privileged parties involved, as well as the basis for the privilege being asserted. Narrative descriptions, therefore, require an attorney to analyze the contents of each document (some of which can be lengthy and unfamiliar to the reviewer) and craft a privilege description that provides enough detail to substantiate the privilege claim without disclosing the privileged information itself. This is frequently a time-intensive process, which can present significant burdens and costs to responding parties.

The burdens of creating privilege logs are borne by responding parties. For requesting parties, the challenges lie in evaluating the privilege log, particularly if the log is voluminous or contains deficient descriptions that do not allow the party to assess the validity of the asserted privilege claims.

These challenges faced by the parties are often exacerbated by factors such as the enormous volume of ESI in modern litigation, timing pressures in discovery, and the potential for costly motions practice when the parties cannot resolve privilege log disputes on their own.

A. The Descriptive Narrative

As discussed above, Rule 26(b)(5)(A) does not define what is required to "expressly make the claim" of privilege or how specific and detailed the description must be to "enable other parties to assess the claim" of privilege. This ambiguity has resulted in the descriptive narrative becoming one of the more contentious aspects of privilege logs, with the responding party and requesting party often having divergent views regarding the level of specificity required.

In general, a descriptive narrative is a sentence describing the type of document, the fact of legal advice sought or rendered, the confidential nature of the communication,[54] and the general subject matter of the legal advice.[55] For logs without independent fields identifying the specific names of communicants, those descriptive sentences include the identities of the clients or attorneys (or third-party agents) involved in the communications. For documents withheld for work-product protection, the narrative may describe the type of document, the identities of the preparer and recipient(s) of the document, and the nexus to anticipated or pending litigation.

From the requesting party's perspective, a descriptive narrative that fails to provide sufficient information hinders its

[54] To the extent the information is not available in other fields, such as the sender and recipient fields.

[55] *See* Appendix A.1 for examples of descriptive narratives in a traditional log.

review of the privilege log and determination of whether privilege attaches to the withheld document(s). For example, the descriptive narrative may be too generic to identify clearly whether the communication in a given log entry concerns legal as opposed to business advice, or it may conflict with other information in the privilege log for the same entry. In short, insufficient details in a log shift the burden to the requesting party to initiate a discovery conference and, possibly, motion practice to get the information it needs, all of which adds to cost and time expended for both parties.

From the responding party's perspective, the creation of the descriptive narrative can be a significant undertaking, often requiring a good deal of time and deliberation. The attorney preparing the log entry typically needs to determine the document type (e.g., an email chain, memorandum, summary, compilation, or report), the affiliation of each communication participant (e.g., an attorney, client, representative, or non-party), the directional flow of the communication (e.g., seeking legal advice, providing legal advice, memorializing a conversation with counsel, or providing information to enable the rendering of legal advice), and the subject matter of the communication. As to this last component, counsel needs to define a description regarding the referenced topic without disclosing the actual advice sought or provided.

It is possible to generate such a description by creating and using single or multichoice coding fields in a review platform to denote, for example, the purpose of the communication or the subject matter of the legal advice. Once selected, these fields can be exported outside of the review platform in a report, such as in an Excel workbook. Those multiple fields can then be concatenated (an Excel-specific formula that merges text content from multiple cells into a single cell) into a string sentence.[56] However, such effort requires reviewers to take additional time to think about and select each element that best ties to each logged document.[57] Unlike a single choice field in document review (i.e., Responsive or Not Responsive; or Not Privileged, Redact for Privilege, or Withhold for Privilege),

[56] Some practitioners and technologists are exploring the use of tools utilizing artificial intelligence to assist in the generation of narrative descriptions. However, such technologies may require substantial upfront costs depending on data volume and vendor pricing or are otherwise inaccessible to certain litigants. In addition, there is significant attorney time required to draft narrative descriptions to train the technology on a sample of documents, sample the results, and validate the accuracy of the generated narratives. The use of such technologies may someday be helpful in reducing the time and potentially overall cost of creating privilege logs, but certain barriers to accessing and leveraging these technologies exist. Nevertheless, as these options evolve, they may become more valuable in reducing the burdens of the privilege logging process.

[57] Although no comprehensive studies have been done on the amount of time required to create the narrative descriptions for privilege logs, it is axiomatic that making several field selections or "clicks" for a privileged document will take longer than making only two (e.g., Responsive and Withhold for Privilege). Further, the menu of choices under each field that is required to form the descriptive sentence makes privilege log coding similar in complexity to issue coding and provides multiple ways for reasonable minds to differ when compared to a binary choice. Additional layers of complexity also increase the efforts required to quality control those varying decision points for consistency. The burden of privilege log coding increases as the number of privileged documents in the otherwise producible population increases. *See* Robert Keeling, *Document Review: You're Doing it Wrong Cognitive Psychology and the Attorney's Mental Plate*, 42 U. ARK. LITTLE ROCK L. REV. 257, 270, 277 (2020) (observing that "an individual can handle only so much information on his or her mental plate, and that these limitations have very real implications for document review" and finding a correlation between a higher number of issue tags document reviewers were required to choose from and a higher overturn rate.); *see also* American Psychological Association, *Multitasking: Switching Costs* (Mar. 20, 2006), https://www.apa.org/research/action/multitask (summarizing research on the impact to productivity when humans switch between complex tasks).

privilege log coding typically requires separate fields for each of the descriptive elements listed above. Each field then requires multiple menu choices in order to accommodate the variety of privileged communications that may be responsive in a complex discovery matter.[58]

Moreover, while the concatenated string approach may be useful in certain circumstances in which document metadata is not informative and the choices for the concatenated string are few and straightforward (e.g., lawyer markups of internal drafts of various policies over the years), this approach takes additional time and consideration where the documents are not easily described by a few common strings. Absent a case where the concatenation choices are few and easily explain the withheld documents, the additional effort required to string together a descriptive sentence to provide information beyond what is identifiable from the document's metadata will not only be more time consuming than a metadata-plus privilege log, but the additional words contained in the descriptive sentence may not provide significantly more insight than the document's own metadata would provide.[59]

Given the additional time and expense associated with creating these descriptive narratives, as well as the fact that much of the same information contained in these descriptions can be exported from the metadata of withheld documents,

[58] Responding parties may wish to provide reviewers with limited menu choices for each field to reduce decision making time and inconsistent coding across a large team of reviewers. However, limiting choices for each field may result in a lengthy log with many documents that have similar entries, which in turn may prompt a challenge that the log is not sufficiently detailed.

[59] *See* Sections III.B.2 and III.B.3, discussing the merits of metadata and metadata-plus-topic logs as alternative means to traditional logs in appropriate circumstances.

alternatives to logging that do not involve such a descriptive narrative offer a more efficient way for a responding party to satisfy its burden, though, as discussed in Section III.2.B, more information may be required for the responding party to meet its burden. As stated throughout this *Commentary*, alternative privilege log formats may be helpful in addressing the tension between specificity and burden.

B. Subject Matter

As stated above, the descriptive narrative also contains the general subject matter of the legal advice. The extent to which courts require subject-matter descriptions and their required level of specificity varies, although the touchstone appears to be whether the details provided are useful to assess the claim of privilege.[60] For example, the Second Circuit and Third Circuit

[60] *See, e.g.*, Johnson v. Ford Motor Co., 309 F.R.D. 226, 233 (S.D.W. Va. 2016) (noting that "courts have not been entirely consistent about the level of detail that is necessary to comply with Rule 26(b)(5)(A)"); Spilker v. Medtronic, Inc., No. 4:13-CV-76-H, 2015 WL 1643258, at *6 (E.D.N.C. Apr. 13, 2015) ("'When a party relies on a privilege log to assert these privileges [i.e., attorney-client privilege and work product protection], the log must as to each document . . . set [ ] forth specific facts that, if credited, would suffice to establish each element of the privilege or immunity that is claimed.'" (quoting Rohlik v. I–Flow Corp., No. 7:10–CV–173–FL, 2012 WL 1596732, at *4 (E.D.N.C. May 7, 2012))); Neuberger Berman Real Estate Income Fund, Inc. v. Lola Brown Trust, 230 F.R.D. 398, 406 n.14 (D. Md. 2005); Pham v. Hartford Fire Ins. Co., 193 F.R.D. 659, 662 (D. Colo. 2000). However, in the context of the assertion of a common-interest privilege, some courts have held that it is sufficient to identify only the parties to the communication on the theory that the fact that the documents are discoverable material is enough to show that the subject matter is relevant to the parties' claims and defenses to support application of the common interest doctrine. *See, e.g.*, Elat v. Ngoubene, Civ. Case No. PG-11-2931, 2013 WL 4478190 (D. Md. Aug. 16, 2013) ("It is immaterial that Defendants did not state the documents' general subject matter because, as discoverable material in this case is necessarily 'relevant to a[] party's claim or defense,' these communications also must be 'relevant

have held that "cursory" descriptions, such as "Fax Re: DOL Findings," "Fax: Whistleblower article," "daily log entries," or "notes/correspondence," are insufficient.[61] By contrast, privilege logs that specifically state that the document includes communications of legal advice on an issue generally pass muster.[62]

As responding parties have moved toward automating drafts of privilege logs from document review databases, some have included metadata filenames, email subject, document titles, and file paths in the logs. This information can be useful and in some cases may be sufficient to illustrate the "general subject matter" sought by the 1993 Advisory Committee Notes. Other times, however, generic subject lines or titles will not be

to a[] party's claim or defense,' i.e., communications that would be covered by the common interest rule, if it applies." (alterations in original)).

[61] *See* United States v. Constr. Prods. Research, Inc., 73 F.3d 464, 473-74 (2d Cir. 1996); R.J. Reynolds Tobacco v. Philip Morris, Inc., 29 F. App'x 880, 882 (3d Cir. 2002); *see also In re* Gen. Instrument Corp. Sec. Litig., 190 F.R.D. 527, 530 (N.D. Ill. 2000) (finding descriptions such as "Explanation re: Primestar Relationship," "NLC Employee Stock Options," and "Filing with SEC," were not "even marginally specific" to allow assessment of claims of privilege); Norton v. Town of Islip, CV 04-3079 (PKC) (SIL), 2017 WL 943927, *4 (E.D.N.Y. Mar. 9, 2017) (finding descriptions insufficient where they were largely limited to unadorned phrases such as "Norton Litigation," "Law Enforcement," and "Litigation").

[62] *See, e.g.*, Spilker v. Medtronic, Inc., No. 4:13-CV-76-H, 2015 WL 1643258, at *6 (E.D.N.C. Apr. 13, 2015) (finding log sufficient where it provided descriptions such as "Memo made at direction of counsel and sent to counsel for purpose of seeking legal advice regarding medical procedure," and "Email requesting advice of counsel regarding FDA request" to be sufficient); *but compare* RBS Citizens, N.A. v. Husain, 291 F.R.D. 209, 218 (N.D. Ill. 2013) (finding insufficient the following description: "Document containing non-responsive and privileged analysis re loan facilities including NBB based in part on and reflecting advice of counsel"); *see also* Vaughan v. Celanese Americas Corp., No. 3:06CV104-W, 2006 WL 3592538, at *3 (W.D.N.C. Dec. 11, 2006).

sufficient to substitute for information needed to assess the basis for the claim of privilege, particularly where the filenames are vague, cryptic, or technical and cannot be explained even by the author/witness.[63] On the other hand, including email subjects, filenames, and/or document titles raises another burden concern. The responding party must assess whether these fields, either alone or combined, reveal sensitive privileged content requiring additional protection through redaction.

In these scenarios, the custom descriptions may become extensive, each taking time to craft the information needed to support the elements of each privilege/doctrine claimed throughout the entire document, which further underscores the importance of consulting with adversaries about privilege log format.

From the requesting party's perspective, if a privilege log fails to provide sufficient information regarding the subject matter of a withheld document that would allow it to understand the nature of each document and assess the privilege claim, it can impact the privilege log review. This is further discussed in Sections II.C (identifying the source of the privilege), II.E (assessing privilege claims amidst increasing volumes of documents), II.F (resolving disputes in time to use the information in the litigation) and II.G (motion practice).

C. *Identifying Privileged Parties*

The descriptive narrative also often incorporates identification of the privileged parties who generated or received the withheld document, or whose legal advice or requests for legal advice are reflected within. For corporate or

[63] Johnson v. Ford Motor Co., 309 F.R.D. 226, 233–34 (S.D.W. Va. 2016) (finding log insufficient when it included "enigmatic file names" that the author of the document could not understand, such as "DI_UA.xls," "Appendix 1 Ford.pdf," "Appendix 14 Toyota.pdf," and "Charts.xls").

institutional parties, there may be questions as to who is included within the definition of the "party" within the ambit of privilege and who is a non-party. Where there is a request to provide the job title or role for individuals listed on the log, that request can become complex if the documents on the log span a long period of time, because this causes a greater likelihood of corporate position changes within the pool of communicants on the log and the fact that information such as job titles going back in time are often not available. Potential courses of action could include agreement that all non-parties will be unambiguously identified (such as by providing email addresses on the privilege log itself), agreement that a responding party will provide this information for specific party individuals upon request, or agreement to provide only the current titles for individuals.

Parties typically identify attorneys and other privileged parties on the log, either by designating attorneys with an asterisk or "Esq.," or by providing a separate list of all individuals whose involvement they assert give rise to the privilege or protection.[64] In-house attorneys representing corporations or institutions may wear multiple hats. Asserting privilege based on in-house attorneys may give rise to a question of whether they were providing business or legal advice in the communication, and parties should be prepared to provide additional substantiation where the in-house attorney is the only legal personnel identified and the log entry does not otherwise provide sufficient information for the requesting party to understand the assertion of privilege.

There may also be communications on the log for which no attorney is listed, and so additional facts about that communication may have to be gathered to determine the

[64] *In re* Haynes, 577 B.R. 711, 737 (Bankr. E.D. Tenn. 2017).

privilege status. While it may be reasonable to withhold a communication between nonattorneys memorializing and/or reflecting the advice of counsel, additional investigation may be necessary to substantiate the assertion of privilege. Although courts recognize that a document may be privileged even if an attorney is not a direct sender or recipient of the correspondence, without some other indicia on the log indicating these documents were prepared for the purpose of obtaining legal advice or in anticipation of litigation, disputes can arise.[65] In addition, email communications without attorneys on the to/from/cc of the metadata may contain counsel communications farther down the email chain (i.e., when nonattorneys forward attorney advice), which may require explanation on the log.

From the requesting party's perspective, a responding party may not have met its obligations when privilege logs fail to adequately identify or explain the roles of the individuals involved in a document and their effect on the privilege claim. For example, when name normalization is used,[66] Listservs are

[65] *See, e.g.*, United States v. Davita, Inc., 301 F.R.D. 676, 682 (N.D. Ga. 2014) ("Thus, the lack of attorneys on either side of an otherwise confidential corporate communication is not fatal to a claim of privilege. The Court, rather, must examine the claims of privilege individually to ascertain whether the documents are entitled to attorney-client protection."); Koumoulis v. Indep. Fin. Mktg. Grp., Inc., 295 F.R.D. 28, 43 (E.D.N.Y. 2013); Norton v. Town of Islip, CV 04-3079 (PKC) (SIL), 2017 WL 943927 (E.D.N.Y. Mar. 9, 2017). Some privileges do not depend on the direct involvement of an attorney (e.g., deliberative process, executive privilege, legislative privilege, etc.), and the absence of an attorney from the log entry provided for such privileges does not necessarily give rise to a justified privilege challenge.

[66] A name normalization tool converts various iterations of email addresses into a single (normalized) name format, rather than require a global "find and replace" for the myriad of ways an email name presents. For example, jsmith@abccorp.com; joe.smith@abccorp.com;

present, or the privilege log contains a large number of individuals, the requesting party often must spend significant amounts of time attempting to discern the basis for the claims of privilege—e.g., whether individuals listed in a log are "outsiders" or lower-level employees whose access to or involvement in the communication may preclude a claim of privilege or give rise to waiver.

D. Basis of Privilege

Responding parties must identify the privilege(s) or protection(s) (i.e., attorney-client privilege, work product, etc.) on which they are withholding each document or category of documents. However, merely identifying the nature of the claimed privilege(s) may not in every instance fulfill the requirement of providing information necessary for the responding party to substantiate the assertion of privilege.[67] For example, it may be necessary to add information to log entries to substantiate claims of work-product protection (e.g., identifying the specific litigation for which the document was

joe@abccorp.com; jmith@gmail.com all normalize on the privilege log to "Smith, Joe." Name normalization has a manual component, and therefore, is an additional burden on the responding party. Before undertaking this effort, the parties should discuss whether the requesting party prefers name normalization, as requesting parties may find it unhelpful.

[67] Harper v. Auto-Owners Ins. Co., 138 F.R.D. 655, 664 (S.D. Ind. 1991) (requiring that the log list, for each separate document, the authors and their capacities, the recipients and their capacities, the subject matter of the document, the purpose for its production, and a detailed, specific explanation of why the document is privileged or immune from discovery); Resolution Trust Corp. v. Diamond, 137 F.R.D. 634, 641–42 (S.D. N.Y. 1991) (finding an index including date, addressor, addressee, document type, and grounds for nondisclosure insufficient).

prepared) or the common-interest doctrine (e.g., the nature of common interests between communicants on the log entry).[68]

E. Substantial Volume

Since the addition of Federal Rule 26(b)(5) in 1993, there has been a tremendous rise in the volume of email and other electronic forms of communications, which, along with the increased ease of transmitting privileged information, has increased the number of documents potentially subject to a claim of privilege. Where a responding party desires to assert privilege over a large number of documents, the time required to complete a traditional privilege log necessarily increases, as does the burden of preparing individualized narrative descriptions for the increased volume of documents.[69] For instance, a party withholding hundreds of documents can typically prepare a defensible privilege log within a week or

[68] *See*, *e.g.*, Pritchard v. Dow Agro Scis., 263 F.R.D. 277, 293 (W.D. Pa. 2009) (requiring that log specify whether the claim is one for factual versus opinion work product); Companion Prop. & Casualty Ins. Co., Civ. A. No. 3:15-cv-01300-JMC, 2016 WL 6539344, *3 (D.S.C. Nov. 3, 2016) (ordering party to provide additional information regarding specific anticipated litigation(s) for the documents withheld on the basis of work-product protection for categorical log); 3d Eye Surveillance, LLC v. United States, 155 Fed. Cl. 355, 362-363 (Fed. Cl. Aug. 27, 2021) (requiring description of the common interests shared among participants to communications claimed to fall within common-interest privilege).

[69] Southern District of New York Committee Note to Local Civil Rule 26.2 ("[W]ith the advent of electronic discovery and the proliferation of e-mails and e-mail chains, traditional document-by-document privilege logs may be extremely expensive to prepare, and not really informative to opposing counsel and the Court."). The Sedona Conference has acknowledged previously that preparation of a privilege log in a complex matter can "consume hundreds of thousands of dollars, or more." The Sedona Conference, *Commentary on the Protection of Privileged ESI*, 17 SEDONA CONF. J. 95, 103 (2016).

two, but a party withholding thousands or tens of thousands of documents as privileged could potentially need months to prepare a defensible privilege log.[70]

The opinion in *Hopson v. Mayor & City Council of Baltimore* aptly describes this challenge and the need for flexible solutions to address it:

> If, indeed, the common law of privilege is not frozen in antiquity, but rather is flexible and adaptable to changing circumstances, then it must be elastic enough to permit reasonable measures to facilitate production of voluminous electronically stored information during discovery without imposing on the parties unreasonable burdens on their human and fiscal resources. The

[70] Increasing volumes of ESI have led many litigants to look for solutions to streamline responsiveness review. Responsiveness review burdens can be alleviated, at least in part, through Technology Assisted Review ("TAR") and other artificial intelligence ("AI") tools. *See* Da Silva Moore v. Publicis Groupe, 287 F.R.D. 182, 191-92 (S.D.N.Y. Feb. 24, 2012) (analyzing the limitations of keyword searches to identify responsive documents and approving technology-assisted review). TAR uses algorithms to identify potentially responsive documents, reducing the volume of documents needing document-by-document human review. However, the application of TAR and other AI technologies to privilege review has proved to be a more vexing problem. This is in part because the privilege analysis is often more nuanced and difficult to recognize than a simple responsiveness binary choice. *See, e.g.*, Ellen Murphy et al., *Lessons From 'Michael Cohen v. United States': Criminal Defendants Should Not Be at the Mercy of Technology for Privilege Review*, N.Y. L.J., Jan. 14, 2019 (noting that TAR is "almost unheard of as the sole tool for privilege review"). *See also* NICHOLAS PACE AND LAURA ZAKARAS, WHERE THE MONEY GOES: UNDERSTANDING LITIGANT EXPENDITURES FOR PRODUCING ELECTRONIC DISCOVERY (2012) (ebook), *available at* https://www.rand.org/pubs/monographs/MG1208.html, (stating that 73 percent of the cost of producing electronically stored information was allocated to human review for responsiveness and privilege, and that while responsiveness could be addressed by emerging tools, privilege review likely could not).

> unavoidable truth is that it is no longer remarkable that electronic document discovery may encompass hundreds of thousands, if not millions, of electronic records that are potentially discoverable under Rule 26(b)(1). In this environment, to insist in every case upon "old world" record-by-record pre-production privilege review, on pain of subject matter waiver, would impose upon parties costs of production that bear no proportionality to what is at stake in the litigation, and mark a dramatic retreat from the commendable efforts since the adoption of Rule 26(b)(2) to tailor the methods and costs of discovery to fit the case at hand . . . . [C]ourts cannot insist upon such painstaking and costly review unless they are willing to allow enough time to do so reasonably. It is unlikely that courts are going to embrace the notion of years-long timetables to allow parties to assemble and review voluminous electronic information prior to production during discovery.[71]

Consistent with the foregoing, this *Commentary* recommends that litigants discuss the expected volume of privileged documents early in the case and the implications of that volume on the format and timing for the production of privilege logs, to the extent that information is reasonably available.

While the time-intensive process of identifying, logging, and conducting quality-control review of a large number of documents as privileged imposes an obvious burden on the responding party, it also can impose a burden on the requesting party. Whereas counsel may be able to more easily analyze a log of a few hundred documents, it takes a significant amount of time to assess privilege logs containing thousands of documents

[71] Hopson v. Mayor & City Council of Baltimore, 232 F.R.D. 228, 243–44 (D. Md. 2005).

and determine which entries require further clarification or reflect documents that may not, in fact, be privileged.

One advancement in technology that has attempted to address the proliferation of emails is the use of email thread identification and suppression, also known as "email threading." Email threading is the technical process of recombining emails that comprise an email discussion, including replies and forwards. Email threading identifies inclusive emails[72] within a given document set, and email thread suppression is the process whereby noninclusive emails within email threads are removed (suppressed) from a review set to reduce the overall review population without removing any unique content. In many cases, email thread suppression may be used to reduce the volume of documents that the responding party must review, and to the extent the emails are privileged, subject to an additional review for privilege logging. This, in turn, can increase the speed of review.

To avoid later disputes, it is recommended that parties discuss early in the case whether threading will be used for review. This includes not just for review but also for logging, because there is a lack of consensus among courts that have addressed in the context of email chains (i.e., one document that contains multiple emails) whether it is sufficient to log the top-level email or whether each component email in the chain must

[72] Inclusive emails are emails containing content that is not present in its entirety in any other email in the set of emails being analyzed. Generally those are the last-in-time email in any branch of the thread, as well as any email with an attachment that is not also attached to a later-in-time email that contains the full content of the earlier email. Noninclusive emails are all emails that are not categorized as inclusive. The Sedona Conference, *The Sedona Conference Glossary: eDiscovery and Digital Information Management, Fifth Edition*, 21 SEDONA CONF J. 263, 381 (2020).

be individually logged.[73] While one practice is to reflect on the privilege log only the top-level email information (while having the description accurately reflect the assertion of privilege over the entire chain), some court decisions endorse the position that every email in the chain must be separately logged. The drafters of this *Commentary* are not aware of any decision addressing whether emails suppressed from review through email thread identification technology must be separately logged. These decisions assessing the need to individually log emails in an email chain would logically be applied to the question of whether individual emails suppressed via threading also need to be individually logged. Courts reaching decisions consistent with the *Rhoads Industries v. Building Materials Corp. of America* cases require logging of each individual email in a chain as a

[73] Practitioners should be aware that courts have taken different approaches on whether each message in the chain must be logged or if one entry will suffice. A few courts, despite acknowledging the increased burden, have required parties to log each message in the chain, even if the metadata of the earlier-in-time email is not available because the message was not separately collected and would need to be populated manually with the date and email participant information. *Compare, e.g.,* United States v. Davita, Inc., 301 F.R.D. 676, 684–85 (N.D. Ga. 2014) (collecting cases where threading was prohibited), recons. in part, 1:07-CV-2509-CAP-JSA, 2014 WL 11531065 (N.D. Ga. May 21, 2014); Universal Serv. Fund, 232 F.R.D. 669, 674 (D. Kan. July 26, 2005) (requiring each email in chain to be logged while acknowledging that "requiring each e-mail within a strand to be listed separately on a privilege log is a laborious, time-intensive task for counsel"); Hillsdale Env't Loss Prevention, Inc. v. U.S. Army Corps of Engineers, No. CIV.A. 10-2008-CM, 2011 WL 1102868, at *4 (D. Kan. Mar. 23, 2011) (requiring each email in a chain or strand be listed on the privilege log and explaining that "[t]o hold otherwise 'would [permit] stealth claims of privilege which, by their very nature, could never be the subject of a meaningful challenge by opposing counsel or actual scrutiny by a judge; this, in turn would render Fed. R.Civ.P. 26(b)(5) a nullity'").

separate document being withheld.[74] On the other side of the question, courts reaching the decision consistent with *Muro v. Target* allow multiple emails in the same chain to be logged as a single entry, provided that all the parts of the communication in the email chain were properly privileged, or nonprivileged portions were otherwise produced.[75]

Absent clear guidance from the court, parties should consider several factors when discussing email threading. When objective information in the log is populated only from top-level email metadata, the potential remains that responsive communications (from suppressed emails in the chain) will be withheld on the basis of privilege without being disclosed on the log. In that case, the direct involvement of an attorney in a suppressed email may not be reflected if metadata is used to

[74] Rhoads Indus., Inc. v. Bldg. Materials Corp. of Am. (Rhoads I), 254 F.R.D. 216, 222 (E.D. Pa. 2008); Rhoads Indus., Inc. v. Bldg. Materials Corp. of Am. (Rhoads II), 254 F.R.D. 238 (E.D. Pa. 2008) (clarifying the scope of court's earlier order regarding which emails were privileged). *See also* N.L.R.B. v. Interbake Foods, LLC, 637 F.3d 492, 503 (4th Cir. 2011) (remanding for district court to assess privilege with respect to each email in the string).

[75] *See* Muro v. Target Corp., 250 F.R.D. 350, 362–363 (N.D. Ill. 2007), *aff'd*, 580 F.3d 485 (7th Cir. 2009) (finding that requiring separate entries for multiple emails in the same string risks forcing parties to disclose privileged information); EPAC Technologies, Inc. v. Thomas Nelson, No. 3:12-cv-00463, 2015 WL 13729725, at *5 (M.D. Tenn. Dec. 1, 2015) ("The Magistrate Judge, however, finds persuasive the standard set forth in Phillips v. C.R. Bard, Inc., 290 F.R.D. 615, 641–42 (D. Nev. 2013) whereby email threads are not required to be separately itemized on privilege logs, but nonprivileged portions of e-mail chains should be produced."); Dawe v. Corr. USA, 263 F.R.D. 613, 621 (E.D. Cal. 2009) (using the first email in a chain to determine privilege); Williamson v. S.A. Gear Company, Inc., Case No. 3:15-cv-365-SMY-DGW, 2017 WL 10085017, at *1 (S.D. Ill. June 6, 2017) ("If applicable, the parties are not required to include separate entries for multiple e-mails within the same string.").

generate and populate the privilege log.[76] This leaves the requesting party guessing at whether any attorney was involved at all, or whether non-parties are included in the suppressed emails. This is one area where parties can negotiate alternatives to providing information regarding communicants of noninclusive emails in the absence of individually logging suppressed emails to address such concerns.

The time required to separately log each lesser included email in a thread can be laborious. Although certain threading tools attempt to parse metadata and text of a document to identify names of senders and recipients on lesser included emails, those tools are not always available or accurate. Without those tools, this can only be achieved through manual effort.

Given the burden of logging each member of an email thread separately, it would be reasonable for the parties to negotiate a single log entry for the inclusive emails within an email thread. The parties should discuss email threading and its implications on the information that will be reflected in the privilege log, and whether it may be helpful to provide additional information about the metadata of suppressed emails, early in the case and before privilege logs are created and produced.

F. Timing Pressures

Parties often have competing interests with respect to the timing of privilege log productions. Common options include producing one log after all documents have been produced, or

[76] Consider a privileged email between an attorney and her nonattorney client, which is then forwarded by the client to a nonattorney company employee. The metadata on the log for the later-in-time inclusive email would reflect only the communication between the nonattorney client and employee. If email threading is used, the original communication with the attorney may be suppressed from review and production and not accounted for on the log (absent negotiation on how to reflect it).

"rolling" privilege logs produced sequentially after a set number of days after the production of a tranche of documents. Because preparing a privilege log can be time consuming and expensive, and perhaps because litigants hope to settle the case before those costs are incurred, some responding parties may prefer to place the effort at the end of discovery. Though Rule 26 does not contain an explicit timing requirement for providing a privilege log, parties are encouraged to discuss the expected timing of serving a privilege log and plan to give themselves sufficient time to address privilege log challenges with the court before the close of discovery, if necessary. Moreover, parties should consider whether their jurisdiction requires serving logs contemporaneous with productions.[77]

From the requesting party's perspective, receiving a privilege log only after all productions have been completed can be problematic for several reasons. First, putting off the logging process risks delaying depositions, summary judgment, and trial, especially where a requesting party challenges the responding party's assertion of privilege over a large number of documents, or where the documents withheld largely implicate contentious privilege disputes. Even with properly prepared and detailed logs, issues related to privilege logs often take significant time and effort to identify, work through, and present to the court (if unable to resolve without intervention). This is especially true when logs produced at the very end of discovery are facially deficient or where the parties have

[77] Courts may have their own standing orders providing expectations on when privilege logs are to be served. For example, one court in the Middle District of Florida orders that privilege logs shall be served simultaneously with the response to written discovery requests in which the documents are withheld on the basis of privilege. *See* https://www.flmd.uscourts.gov/sites/flmd/files/documents/mdfl-hoffman-standing-order-regarding-privilege-logs.pdf (June 17, 2019).

reached an impasse as to whether a particular privilege basis is defensible. In such situations, it may be difficult to get additional time to make use of any documents later determined to be not privileged when logs have been delayed or large swaths of documents have been de-designated from an initial withholding position. Yet, conferring as to numerous iterations of a rolling log requires detailed organization to track and resolve disputes.

Second, it may be more difficult to assess the responding party's claims of privilege if logs are not produced with each production, so that everything can be analyzed in context. Rolling logs may facilitate earlier identification and resolution of concerns over the format, level of specificity, and substance of the privilege claims, and indeed, some courts have expressed an expectation for parties to use rolling privilege logs.[78]

From a producing party's perspective, there may be significant downsides to rolling privilege logs. Foremost, having to provide privilege logs at or near the same time as corresponding document productions potentially decreases the quality and accuracy of the privilege log because resources must be diverted away from the privilege log to complete a document

[78] "This Court does not condone waiting on the production of a privilege log until the end of a rolling ESI production. Producing parties should provide a log with each production tranche and/or on a rolling basis. This allows the requesting party to timely raise issues about withheld documents. It also allows for the review of smaller subsets of documents and smaller in camera reviews (if necessary), allowing for early clarification of privilege issues. Such a process is fairer to the requesting party, more efficient, and less costly. Additionally, Rule 26 contemplates the supplementation of privilege logs throughout discovery." Brown v. Barnes & Noble, Inc., 474 F. Supp. 3d 637, 647 (S.D.N.Y. 2019), *recons. denied*, No. 1:16-cv-07333 (RA) (KHP), 2020 WL 5037573 (S.D.N.Y. Aug. 26, 2020), and *aff'd*, No. 1:16-cv-07333 (MKV) (KHP), 2020 WL 5037573 (S.D.N.Y. Aug. 26, 2020).

production on time. Thus, rolling logs may result in privilege logs of inferior quality, which may often lead to disputes (including motion practice requiring court attention) where the receiving party objects to various log entries. Rolling logs may require the responding party to address potentially complex privilege issues, involving numerous email threads and strings, across an entire universe of documents early in the process, before the full scope of potentially privileged documents has been assessed. A privilege decision early in the document review may need to be changed based on information learned later in the review, which leads to decreased consistency in assertions of privilege and increased risk of the inadvertent production of privileged documents. For this reason, in cases involving large volumes of documents, it is typical for the responding party to apply a "privilege screen" (list of privilege-associated search terms) to the documents and to withhold all documents resulting from that search from its initial productions until they can be subjected to further privilege review. It may also be the norm that responding parties in this situation will be overly cautious in making early privilege assertions that would not have been made with the benefit of more time and context prior to providing a privilege log.

G. Motion Practice

As shown above, there is no agreed standard for how specific a log must be apart from the general requirement that the withholding party must provide enough information to "enable other parties to assess the claim" of privilege. This uncertainty can raise concerns for both parties—for the requesting party, who may have to expend time and resources pressing for more details when presented with a log they believe to be insufficient; for the responding party, who may have to expend additional time and resources responding to demands for more specific logs. Because there is no clear standard regarding how much specificity is required, this can create tension between the parties and lead to disputes about the sufficiency of a privilege log. If the parties are unable or unwilling to resolve these disputes in a cooperative manner, it can lead to costly motion practice that imposes a burden on both parties, as well as the court.

III. METHODOLOGIES TO MITIGATE BURDENS

The burdens often presented by the privilege logging process can be mitigated in a number of ways. These include (1) exclusion from the logging process of certain categories of documents that require less or no substantiation for a recognition of privilege protection, (2) utilization of alternative, less-involved privilege logging formats, and (3) early case communication via the Rule 26(f) conference and negotiation of an ESI protocol or other agreement to address the details regarding content, format, and timing of privilege logs.

A. Privilege Log Exclusions for Categories Requiring Less/No Substantiation

Generally, for certain categories of documents, an entry on a traditional privilege log does not materially add to the threshold of substantiation needed for a requesting party to assess a claim of privilege. Excluding these categories of documents from privilege logs in the first instance can greatly reduce the burdens associated with privilege logs for the parties.

As explained below, this *Commentary* recommends excluding three categories of documents from logging in the typical case: (1) communications with outside counsel after the date of litigation, (2) documents that post-date the complaint and constitute work product prepared in connection with the litigation at issue, and (3) redacted documents (provided that the basis for the redactions is evident on the face of the document itself).

Communications between a party and its outside counsel[79] after the date the litigation commenced about issues related to

[79] The responding party may also request to include in-house counsel in the scope of this exemption if it can demonstrate that the attorney(s) was

the litigation can reasonably be construed as communications between a client and attorney in connection with the request for or provision of legal advice related to the pending litigation.[80] In most circumstances, reasonable minds would agree such communications are protected by the attorney-client privilege, and likely also the work-product doctrine, and may be withheld from production. These documents generally are not subject to dispute as to the validity of a privilege claim.

For the same reason, work product generated by the party or its litigation counsel, prepared in connection with the litigation, after the date of the complaint, is generally understood to be protected from disclosure. In most cases, it benefits both parties to exclude these two document categories from privilege logging. For the responding party, excluding these document categories minimizes the time and expense required to prepare privilege log entries, and for the requesting party, it minimizes the number of log entries the party must assess. Moreover, agreeing to exclude these categories will decrease the number of log entries that may be subject to dispute between the parties. There may be cases, however,

exclusively providing litigation-related advice, rather than serving in a business or mixed role.

[80] Courts have routinely found that, for example, post-litigation communications with counsel do not need to be logged. *See, e.g.*, Grider v. Keystone Health Plan Cent., Inc., 580 F.3d 119, 139 n.22 (3d Cir. 2009) (declining to require preparation of a privilege log for all post-complaint privileged communications because doing so "would have a chilling effect on the attorney-client relationship"); Aetna Inc. v. Mednax, Inc., No. 18-CV-02217-WB, 2019 WL 6250850, at *7 (E.D. Pa. Nov. 22, 2019) (holding that a privilege log did not need to be prepared for communications between a party's attorneys, experts, and consultants retained in anticipation of litigation because the burden of laborious privilege review "would far exceed any likely benefit" of finding relevant, nonprivileged documents); Quincy Mutual Fire Ins. Co. v. Atlantic Specialty Ins. Co., 2019 WL 3409980, at *7 (D. Mass. July 29, 2019).

where the requesting party has particular questions or concerns about post-complaint communications, in which case the parties should discuss and negotiate the contours of this exclusion. Additionally, the parties should discuss whether and how to apply these exclusions where the underlying subject of the litigation may be ongoing and is relevant.

Documents produced with redacted text are another example where the privilege log entry may not materially add to the level of required substantiation. Where specific lines of text in an email chain are redacted, but the email sender, recipient(s), date, and subject line remain viewable and the nonprivileged metadata produced, the produced image and metadata of the document reflects much of the information already required to substantiate the claim of privilege—the "details concerning time, persons, and general subject matter" that the 1993 Advisory Committee Notes to Rule 26 state as appropriate information to provide. The email sent date provides the "time," the sender and recipient fields provide the "persons," and the subject line and surrounding unredacted text provide the "general subject matter."[81] If the "detail" information is already provided by way of the produced image, then as a threshold matter, the withholding party has "stated" the claim of privilege.[82] Any information that would be put into

[81] The same may also be true for redacted portions of a non-email attachment documents such as a Word document or PowerPoint presentation where the transmittal email is produced. This is the case because the produced transmittal email will present the time and persons details, and the nonredacted portions of the attachment document will provide the context of the subject matter. Often, the author or filename of a document will be in the produced metadata.

[82] Mid-State Auto. v. Harco Nat'l Ins. Co., No. 2:19-cv-00407, 2020 WL 1488741, at *4 (S.D. W.Va. Mar. 25, 2020) (holding that the privilege logs—which omitted any notes on redactions—were sufficient because the

a traditional privilege log entry is likely already reflected in the produced document, so the time it takes to create a log line entry adds to the responding party's burden but does not substantially add to the requesting party's ability to properly assess the claim.

However, if the type of protection (e.g., privilege versus work product) being asserted is not evident from the face of the document, the requesting party may need to seek clarification. Also, there may be situations in which the requesting party needs additional information regarding the subject matter of the documents to assess the privilege claims. To address such questions, the responding party may need to list the privilege asserted in the text of the redaction box and/or provide a Bates/assertion log only (e.g., a spreadsheet with the Bates numbers for redacted documents and the type of protection claimed—work product (WP), attorney-client privilege (ACP), or other protection). Alternatively, the parties could agree to have this information provided in the document's metadata, through the provision of a user-created metadata field containing the privilege basis.

In addition, a requesting party may not be able to determine the existence of a privilege where attorney names are not reflected as involved communicants or where new forms of communication or certain file types present unique challenges. In the interest of minimizing burdens, the responding party can agree to provide supplemental information about specific documents identified by the requesting party, rather than creating an additional log line for each redacted document. To aid in the identification of redacted documents and assess the metadata associated with them, it is recommended that

requesting party could still ascertain all the necessary information from the document itself).

redacted documents contain a populated value in a "redacted" field in the load file produced to the requesting party.

In summary, as additional description is not necessary to state a claim of privilege for such documents, this *Commentary* recommends exclusion from logging requirements for three categories of documents in the typical case:

- Post-Complaint Outside Counsel—Communications between outside counsel and the client after the complaint was filed.[83]
- Post-Complaint Work Product—Communications and work-product documents related to the underlying litigation (e.g., draft pleadings or discovery responses, litigation strategy memos) that post-date the complaint.
- Redacted Documents—Parties can negotiate the exclusion of redacted documents from a privilege log when the bibliographic information provided on a privilege log is available on the face of the redacted document and there is adequate context to understand the subject matter of the document in order to assess the privilege claim.

Agreeing to exclude these documents from logging in the first instance not only limits privilege log disputes to the entries that are more likely to be the subject of a true dispute, but also reduces the time and cost necessary to create the privilege log. This helps *both* parties reduce burdens. Furthermore, agreeing

[83] *See, e.g.*, Colibri Heart Valve LLC v. Medtronic CoreValve LLC, No. 820CV00847DOCJDEX, 2021 WL 6882375, at *3 (C.D. Cal. Dec. 6, 2021) ("Courts in this circuit routinely deny a motion to compel a privilege log of attorney-client communications or work product dated after commencement of litigation."). There may be other categories of documents that the parties agree are, on their face, likely to be privileged and exempt from a logging obligation, such as attorney billing entries.

to exclude certain categories of documents from privilege logging does not waive the requesting party's ability to request additional substantiation later should the situation warrant. Whether it is appropriate to agree to any or all of these exclusions should be evaluated based on the nature of the case and the documents reasonably sought in discovery. But agreeing to the concept of such exclusions and negotiating the parameters of them at the outset of the case will engender a degree of goodwill in cooperation between the parties.

B. Alternative Construction of Logs

In general, and as noted above, parties are free to create a log that provides the necessary information in the manner they agree is most appropriate for the case. There are several alternatives to the traditional log that may meet the requirements of Rule 26, such as categorical logs, metadata logs, metadata-plus-topic logs, and bespoke logs for nontraditional data sources. Each is discussed in greater detail below, but there is no "one size fits all" approach, and litigants should consider the document population and select the option that will most efficiently allow the responding party to substantiate the reason for withholding of otherwise responsive information. A responding party should also consider whether it is appropriate to use more than one type of privilege log formats for different sources or topics of withheld documents.

1. Categorical logs

A categorical log is a table of withheld documents, where documents are grouped based on similar characteristics and may share a single common description providing information to substantiate the claim of privilege. Typically, to generate a categorical log, the responding party will manually categorize the nature of the document (by a topic category) during privilege review. Once identified by category, the documents will be manually organized by overlapping sender/recipient groups. The log will reflect the date range applicable to that category, sender/recipient group for that category, and the number of documents withheld. (*See* Appendix A.2 for an example of a categorical log.) Because this is a manual task, it requires familiarity with all of the different ways in which the privileged documents present, so that the attorney can determine the schema of categories for the privilege log. Making these determinations is often a time-consuming process for the responding party.

Categorical logs have their origins in the Advisory Committee Notes to Rule 26. Specifically, prior to 1993, Federal Rules of Civil Procedure did not address privilege logging, though some district courts had requirements or local rules for logs. When subparagraph (5) was added to Rule 26(b) in 1993, the Advisory Committee Notes explained that a specific format was not required and could vary based on the needs of the case:

> The party must also provide sufficient information to enable other parties to evaluate the applicability of the claimed privilege or protection . . . . The rule does not attempt to define for each case what information must be provided when a party asserts a claim of privilege or work product protection. *Details concerning time, persons, general subject matter, etc., may be appropriate if only a few items are withheld, but may be unduly burdensome when voluminous documents are claimed to be privileged or protected, particularly if the items can be described by categories.*[84]

[84] The Note also acknowledges that a responding party objecting to an overbroad request does not have to log withheld privileged documents that fall outside the scope of how the party responds to the discovery request.

The emphasized portion of the Note above—suggesting description by categories—led to the creation of "categorical logs" as a means of potentially reducing the burden of having to draft descriptive narratives for each document.[85]

In the years since, some jurisdictions, such as the Southern District of New York, have implemented local rules stating that categorical logs are presumptively proper.[86] For example, New York state courts affirmatively require parties to discuss if using categories is more efficient.[87] The Supreme Court of New York adopted Rule 11-b of Section 202.70(g), which establishes a preference for categorical privilege logs.[88] Even in states where traditional logs are required, there may be an exception for

[85] For example, in Shufeldt v. Baker, Donelson, Bearman, Caldwell & Berkowitz, P.C., No. 3:17-CV-01078, 2020 WL 1532323 (M.D. Tenn. Mar. 31, 2020), the court said that "[w]here a document-by-document privilege log would be unduly burdensome, courts have permitted a categorical log" and then cited the following Advisory Committee Note: "Details concerning time, persons, general subject matter, etc., may be appropriate if only a few items are withheld, but may be unduly burdensome when voluminous documents are claimed to be privileged or protected, particularly if the items can be described by categories." *Shufeldt*, 2020 WL 1532323, at *5.

[86] *See, e.g.*, Local Rules of the U.S. Dist. Courts. for S.D.N.Y. & E.D.N.Y., CIV. R. 26.2 (Oct. 29, 2018), https://nysd.uscourts.gov/sites/default/files/local_rules/rules-2018-10-29.pdf. *See* Auto Club of New York, Inc. v Port Authority of New York and New Jersey, 297 F.R.D. 55, 59 (S.D.N.Y. 2013) (Per Local Rule 26.2, "a categorical privilege log is adequate if it provides information about the nature of the withheld documents sufficient to enable the requesting party to make an intelligent determination about the validity of the assertion of the privilege.").

[87] N.Y. COMP. CODES R. & REGS. tit. 22 § 202.20-a.

[88] Comm. on State Courts of Superior Jurisdiction, Guidance and a Model for Categorial Privilege Logs, https://www2.nycbar.org/pdf/report/uploads/20072891-GuidanceandaModelforCategoricalPrivilegeLogs.pdf (last visited May 16, 2024).

categorical logs for some portion of the privileged population.[89] There are several cases authorizing categorical logs as a less burdensome means of asserting privilege.[90] There are also cases confirming that parties are making affirmative use of this option.[91]

[89] Delaware Chancery practice guidelines, p. 24, https://courts.delaware.gov/forms/download.aspx?id=99468 (last visited May 16, 2024) ("Categories of documents that might warrant such treatment include internal communications between lawyer and client regarding drafts of an agreement, or internal communications solely among in-house counsel about a transaction at issue. These kinds of documents are often privileged and, in many cases, logging them on a document-by-document basis is unlikely to be beneficial.").

[90] United States v. Magnesium Corp. of Am., No. 01-00040, 2006 WL 1699608 (D. Utah June 14, 2006) (ordering a categorical log for documents generated after institution of action, with (1) time period, (2) list of authors, recipients, copy recipients, (3) representation by counsel that the documents were privileged; and did not require a subject matter or topic be disclosed for the documents identified on the categorical log); Auto. Club of NY., Inc. v. Port Auth. of NY & NJ, 297 F.R.D. 55 (S.D.N.Y. 2013) (holding categorical logs are adequate if they provide information about the nature of the withheld documents sufficient to enable the requesting party to make an intelligent determination about the validity of the assertion of the privilege); Orbit One Commc'ns, Inc. v. Numerex Corp., 255 F.R.D. 98, 109 (S.D.N.Y. 2008) ("[Attorney representing plaintiff who is challenging the subpoena] may provide a categorical privilege log rather than a traditional, itemized privilege log . . . .").

[91] *See, e.g.*, Mfrs. Collection Co. v. Precision Airmotive LLC, No. 3:12-cv-853-L, 2014 WL 2558888 (N.D. Tex. June 6, 2014) (Party providing categorical log had to identify authors and recipients of all documents, provide subcategories for each type of privilege claimed, and subdivide a litigation category into three subcategories designated by the court); CC-Aventura, Inc. v. Weitz Co., LLC, No. 06-21598-CIV, 2008 WL 828117 (S.D. Fla. Mar. 27, 2008) (requiring defendants to "identify the date on which each of the insurance companies assumed the defense of this litigation"); *In re* Imperial Corp. of Am., 174 F.R.D. 475 (S.D. Cal. 1997) (plaintiffs ordered to provide a log with an "aggregate listing of the numbers of withheld documents," "an identification of the time periods encompassed by the

Courts have differed on what showing, if any, is needed to create a categorical log in lieu of a traditional log. Many courts require a showing of burden.[92] One of the initial cases to evaluate use of a categorical log on a showing of burden was *SEC v. Thrasher*.[93] In that case, counsel had already represented that the privileged documents reflected communications between defense attorneys and that all of the documents had been kept in confidence. The court only required as additional privilege substantiation: "(1) an identification of the time period encompassed by the withheld documents; (2) a listing of the individuals who were authors or addressees or were copied on the documents; [and] (3) a representation by counsel as to whether all of the documents either (a) were prepared to assist in anticipated or pending litigation or (b) contain information reflecting communications between (i) counsel or counsel's representatives and (ii) the client or the client's representatives, for the purpose of facilitating the rendition of legal services to the client."[94] The *Thrasher* test has been utilized by numerous

withheld documents," and an affidavit representing that the withheld documents were trial preparation materials or contained information reflecting confidential communications between counsel and plaintiff).

[92] Tyco HealthCare Grp. LP v. Mut. Pharm. Co., No. 07-1299 (D.N.J. May 2, 2012) (holding that party was required to produce a document-by-document, post-complaint privilege log because the party did not establish that logging potentially less than 3,000 documents would be unduly burdensome); Sprint Commc'ns Co. L.P. v. Big River Tel. Co., LLC, No. 08–2046–JWL, 2009 WL 2878446 (D. Kan. Sept. 2, 2009) (court ordered a party who logged approximately 1,000 documents in one category to either provide a supplemental log with more specific subcategories or move for a protective order relieving it of the obligation to log, accompanied by evidence showing burden); Bethea v. Merchants Comm. Bank, Civil Action No. 11-51, 2012 WL 5359536 (D.V.I. Oct. 31, 2012).

[93] S.E.C. v. Thrasher, No. 92 CIV. 6987 (JFK), 1996 WL 125661, at *2 (S.D.N.Y. Mar. 20, 1996).

[94] *Id.*

other courts.[95] Some courts do not require a showing of burden and instead focus on what information the requesting party needs, or the potential risk of revealing privileged information in a document-by-document log.[96] Yet other courts have found categorical logs provide insufficient information for courts and requesting parties to assess the claim.[97]

Although categorical logs have been utilized by parties to reduce their privilege logging burdens, this format can present its own issues, including resistance from opposing parties and courts if the content of the log is deemed insufficient to satisfy the requirements of Rule 26(b)(5)(A).

Categorical logs have often been critiqued as not being as effective at reducing costs and burdens as perhaps originally anticipated. For example, grouping "like" documents into a single category often requires more manual effort to analyze

[95] *See* Asghari-Kamrani v. United Servs. Auto. Ass'n, No. 2:15CV478, 2016 WL 8243171, at *3 (E.D. Va. Oct. 21, 2016) (utilizing *Thrasher* test and stating: "Although no district court within the Fourth Circuit has utilized the *Thrasher* test, it has been adopted in primarily unpublished opinions by district courts within the Second, Fifth, Sixth, Ninth, Tenth, Eleventh, and DC Circuits." (citing cases)).

[96] United States v. Gericare Med. Supply Inc., No. Civ. A. 99-0366-CB-L, 2000 WL 33156442, at *4 (S.D. Ala. Dec. 11, 2000)("[D]efendants have not explained how a categorical privilege log impaired their ability to test the plaintiff's claim of work product protection, which rises or falls as a unit."); *In re* Motor Fuel Temperature Sales Pracs. Litig., No. 07–MD–1840–KHV, 2009 WL 959491 (D. Kan. Apr. 3, 2009) (defendants required to review post-litigation attorney communications because they did not make an adequate showing of the burden of review, but they could categorically group the documents in a privilege log).

[97] Neelon v. Krueger, 67 F. Supp. 3d 467, 470 (D. Mass. 2015), *aff'd in part, modified in part, vacated in part* by 2015 WL 1037992, at *4 (D. Mass. Mar. 10, 2015) (Plaintiff's assertion of privilege over categories of documents "is no more than a variant of a blanket assertion of the privilege, which, as noted, does not comply with the requirements of the law.").

and combine records than would be incurred compared to alternative methods. In addition, if categories are not described with sufficient particularity or encompass large numbers of documents over a lengthy time period within a single category, it can lead to discovery disputes. These disputes are costly and time consuming and may result in the court requiring either amendment of, or conversion to, a traditional privilege log for some or all of those categories, thereby eliminating any perceived efficiencies the responding party sought to achieve with this type of log.[98] Moreover, the timing of when in the review process to define a "category" can be problematic—a list of categories determined through early client discussions and

[98] Courts within the Southern and Eastern Districts of New York continue to clarify the requirements for categorical logs, rejecting overly vague, broad, and conclusory categories and, sometimes, requiring a document-by-document log instead. *See, e.g.*, Aviles v. S&P Global, Inc., 17-CV-2987 (JPO)(KHP), 2022 WL 336951, at *3-*4 (S.D.N.Y. Feb. 4, 2022) (requiring responding party to redo categorical log to provide categories with maximum six-month time frame (instead of years) and to more completely identify nonattorneys involved in withheld communications); U.S. Bank Nat'l Ass'n v. Triaxx Asset Mgmt., 18-CV-4044 (BCM), 2021 WL 1968325, at *3–5 (S.D.N.Y. Mar. 31, 2021) (finding categorical log inadequate where it provided 17 "vague and repetitive," conclusory category descriptions; ordering "document-by-document" log for three categories and modified categorical logs for other categories, including narrower date ranges and identities of parties to the communications); *In re* Aenergy SA, 451 F. Supp. 3d 319, 326–28 (S.D.N.Y. 2020) (ordering document-by-document log because court had "lost confidence" that responding party would provide adequate categorical log); Norton v. Town of Islip, CV 04-3079 (PKC) (SIL), 2017 WL 943927, at *9 (E.D.N.Y. Mar. 9, 2017) (rejecting categorical log for lack of sufficient information in category descriptions to permit requesting party to assess claims of privilege and ordering production of document-by-document log); Chevron Corp. v. Salazar, No. 11 CIV. 3718 LAK JCF, 2011 WL 4388326, at *2 (S.D.N.Y. Sept. 20, 2011) (finding, after in camera review of withheld documents, that party's categorical privilege log "obscures rather than illuminates the nature of the materials withheld" and that an itemized log was required).

sampling may evolve and change contours as more information is gained through review. This, in turn, may necessitate significant evolutions on categorization protocols and efforts to change category decisions previously applied to documents.

Notwithstanding, particular consideration should be given to using this format when a jurisdiction encourages it. Practitioners in New York, for example, should consider whether and how to make this solution work for their cases, or at least for large subsets of their document population. Also, for cases involving a large number of withheld privileged documents that can fairly be grouped together by subject matter and overlapping communicants, a categorical log may be appropriate. For example, for a privileged document population that heavily involves discussions with outside legal counsel pertaining to the lead up to the action (if not already excluded through negotiation), a categorical log may be appropriate.

2. Metadata logs

A metadata log is a table of withheld documents that provides only the metadata fields that can be extracted from the withheld documents, potentially with a designation for privilege bases (ACP, WP, etc.), but without a substantive privilege descriptive narrative. (*See* Appendix A.3 for an example of a metadata log.) Generating such a log is generally a straightforward process that involves exporting existing metadata fields associated from a document review platform for the documents that a party asserts are privileged. The parties may agree, in the first instance, to provide a document-level metadata log that provides the existing metadata for fields that correspond to information that would be on a traditional privilege log. The parties can agree to a sampling process to provide additional information for a percentage of the withheld documents or focus on entries for which the requesting party has indicated that the metadata does not provide enough information to understand the assertion of privilege. Parties can explore alternative approaches, including a combination of such approaches, for different types of documents.

Metadata logs are prepared by extracting information from the metadata of the native document maintained in the review platform. The fields can be easily exported, on a document-by-document basis, from the review platform into a spreadsheet-type table for further review, and if necessary, editing. Common examples of such fields are Priv Log ID, From, To, CC, BCC, Date, File Type or Extension (e.g., Email or .msg, Spreadsheet or .xls), Basis for Claim (Attorney-Client Privilege, Work Product, other). Additional fields that may be requested are as follows:

- Family ID[99]—identifying the relationship between a parent document and an attachment.
- Email subject/File name—note that where this field is provided there is the possibility that the field may contain privileged information and may need to be redacted.
- Custodian or Custodians
- Date/Time Created/Last Modified—note that these fields may not accurately reflect the date/time a file was created or modified.

[99] This field may help address the issue of where documents in the same electronic "family" (e.g., emails and attachments) are logged in separate, disjointed entries. Identifying the relationship between the parent and child documents (email and attachment, or presentation with embedded charts, etc.) in some manner in the log would allow for better assessment of the documents in relation to one another. *See* Appendix B for a detailed description of fields for various log formats.

- (File) author—note that where this field is provided it may not accurately reflect the actual author of the file given the tendency to reuse previous documents as the starting point for new documents.
- Last Edited By—this would provide additional information as to who has seen and edited the document.
- File Extension—can provide additional information about the type of document (email, spreadsheet, presentation), which may be important if File Type metadata is not a supported field.
- Email Thread ID[100]
- HashValue[101]

For metadata logs, counsel will often need to provide a "key" of legal personnel—names and affiliations/positions—as well as for non-parties that the responding party asserts do not break the privilege. A name normalization tool should not be used if the responding party agrees to a requesting party's suggestion that email addresses be provided to help identify the affiliations of each person on the log.

In many instances, the metadata maintained in the to/from/cc, document type, and email subject/filename fields

[100] This field will reflect an ID value that indicates which conversation an email belongs to and where in that conversation it occurred. *See* Email threading, RELATIVITY ONE, https://help.relativity.com/RelativityOne/Content/Relativity/Analytics/Email_threading.htm (last visited May 16, 2024).

[101] Hash Value, or Hash Coding, is a "mathematical algorithm that calculates a unique value for a given set of data, similar to a digital fingerprint, representing the binary content of the data to assist in subsequently ensuring that data has not been modified." It may include MD5 or SHA. The Sedona Conference, *The Sedona Conference Glossary: eDiscovery and Digital Information Management, Fifth Edition*, 21 SEDONA CONF J. 263, 317 (2020).

will provide information synonymous with much of what is contained in a descriptive narrative, which is omitted from metadata logs. Because a descriptive narrative can be understood to be a combination of multiple points of information—the involved communicants, the privilege claim, and the subject matter—that same formula may be easily met with the provision of metadata fields that serve just as well to "enable other parties to assess the claim" of privilege. Each of these data points can be independently provided on a log leveraging metadata, which may be sufficient to establish the privilege basis for many withheld documents, narrowing the disputes or requests for additional information to a smaller number of documents on the log.

One potential challenge to metadata privilege logs arises where email threads withheld in their entirety implicate multiple protections in different portions of the document, but the only metadata that can be automatically extracted by a typical document review platform is for the top (latest) email in the string.[102] The top email metadata may not provide sufficient information to support the privilege claims for emails elsewhere in the string. If the requesting party raises a concern, the parties can confer so that the responding party can, for example, provide additional information about particular documents, which may include individualized descriptions to account for the separate privileges and subject matters within a document.[103]

Similarly, if using email thread suppression and logging only the top-line email, the direct involvement of an attorney in

[102] For example, an attorney-client communication is forwarded between nonattorneys that are then communicating to prepare material to support a litigation.

[103] As referenced elsewhere, additional communicants involved in the lower string should also be disclosed in some manner.

a suppressed email may not be reflected if metadata is used to generate and populate the privilege log.[104] This leaves the requesting party wondering whether any attorney was involved at all.[105] In these situations, parties may also need to provide identification of other legal personnel involved in the communication that are reflected solely in the earlier communications within the email chain; this field cannot be extracted from a document's innate metadata and would have to be manually populated.

Metadata will not be perfect for every document. For example, the filename or subject line may be uninformative or not applicable to the subject matter at issue. Metadata may be missing or inaccurate. Scanned hard-copy documents may have no useful metadata. However, where these potential deficiencies prevent a reasonable assessment of the claim, the parties can confer on those entries for which the receiving party believes it needs additional information to assess the claim of privilege. This iterative process can occur a few ways. For example, the responding party can agree to provide supplemental descriptions for a limited number of entries, or over specific categories of entries (such as those without reference to an attorney, where a third-party communicant is included, or where the subject matter appears to be business rather than legal in nature).

[104] Consider a privileged email between an attorney and her nonattorney client, which is then forwarded by the client to a nonattorney company employee. The metadata on the log would reflect only the communication between the nonattorney client and employee. The original communication with the attorney may be suppressed from production, but not accounted for on the log.

[105] Practitioners also should be aware that courts have not been consistent on whether each message in the thread must be logged or if one entry will suffice. *See supra* Section II.E and corresponding footnotes.

Precedent for the use of metadata privilege logs is mixed. In *U.S. Bank National Association v. Triaxx Asset Management LLC*,[106] the court allowed a party to remedy a deficient categorical log by providing either an itemized log or a metadata log for a particular category. In *McEuen v. Riverview Bancorp, Inc.*,[107] the court held that providing a list of specific metadata fields on a log for documents kept on a withheld hard drive would satisfy the privilege log requirements. However, in *LaVeglia v. TD Bank*,[108] the Eastern District of Pennsylvania rejected a metadata log as insufficient because it did not provide any basis for the privilege assertion. Similarly, in *McNamee v. Clemens*,[109] the Eastern District of New York determined that a metadata privilege log was insufficient because the "subject line contains, in many instances, exceedingly unhelpful descriptions."[110]

Parties should consider using a metadata log format when the data population identified to be withheld is voluminous, because it allows for serving a log much sooner than could occur with other privilege log formats.

[106] U.S. Bank Nat'l Ass'n v. Triaxx Asset Mgmt. LLC, 19-CV-00783 (DLI) (CLP), 2021 WL 1207122 (S.D.N.Y. Mar. 31, 2021).

[107] McEuen v. Riverview Bancorp, Inc., NO. C12-5997 RJB, 2013 WL 12095581 (W.D. Wash. Oct. 1, 2013).

[108] LaVeglia v. TD Bank, No. 2:19-cv-01917, 2020 WL 127745 (E.D. Pa. Jan. 10, 2020).

[109] McNamee v. Clemens, No. 09 CV 1647 SJ, 2013 WL 6572899, at *3 (E.D.N.Y. Sept. 18, 2013).

[110] *Id.* ("Examples of such vague subjects include single word descriptions, such as: 'tomorrow,' 'Media,' 'My info,' 'statement,' 'Costs,' 'Letter,' 'notes,' 'Inquiry,' and 'Discussion.' These types of descriptions clearly do not provide sufficient information as to the content of the documents to enable plaintiff or the Court to evaluate whether each of the withheld documents is privileged . . . .").

3. Metadata-plus-topic logs

Similar to a metadata log, a metadata-plus-topic log is a table of withheld documents that provides the metadata fields that can be extracted from a review platform with minimal effort. By omitting a full privilege description sentence, this log form requires less effort than creating a traditional privilege log. However, in addition to the fields available in a pure metadata log, a metadata-plus-topic log will include an additional field—a category, or topic, description. Examples of a category/topic field could include things such as: contract drafting and evaluation; settlement analysis; consumer outreach; or internal investigation. (*See* Appendix A.4 for an example of a metadata-plus-topic log.) This one additional field is what distinguishes a metadata-plus-topic log from a pure metadata log.

As explained above, for most documents, the metadata of the document being withheld is likely to provide the details pertaining to time, persons involved, and general subject matter by providing fields such as to, from, cc, bcc, sent or modified date, email subject, and filename. The parties may wish to negotiate for the provision of additional fields, such as file extension, custodian, etc. The responding party should also provide an explicit reference to the basis for withholding—whether it is for attorney-client privilege, work-product protection, or some other privilege or immunity. Indeed, for many documents, this may be all the information necessary to allow the requesting party to assess the assertion of the claimed privilege.

However, where the metadata provided is not specific enough to provide the context of the subject matter, then providing an additional privilege topic field, exported from the party's document review platform, provides further insight into the subject matter of the privileged content. The topic field will reflect an independent assessment by a reviewer of the category that most closely describes the withheld document. The responding party will prepare a set of coding options/tags for the most likely topics, which can be amended/supplemented as review progresses. Whichever tag the reviewer selects for that document will be exported as the privilege topic field.

By providing information regarding time, persons involved, and general subject matter from the available metadata and category/topic fields, the metadata-plus-topic log generally meets the threshold showing required by Rule 26. Additional engagement between the parties is likely necessary for some portion of the documents on such a log, to request or provide additional substantiation. But engaging in that effort for a subset of the withheld documents involves lesser effort in terms of time, cost, and items of dispute for both parties. Preparing a metadata-plus-topic log and then responding to subsequent requests for additional information as to specific entries satisfies the parties’ obligations to respond to discovery diligently in an efficient manner.

Metadata-plus-topic logs are particularly useful when the data population to be withheld is voluminous, because they allow the responding party to serve a log much sooner than could occur with a traditional log. Another benefit of a metadata-plus-topic log over a metadata-only log is that the associated topic often helps the requesting party narrow the entries it may challenge or for which it may request additional information. Providing a topic for each logged document allows the requesting party to more easily identify areas of dispute by topic, which provides for a more streamlined and effective dispute resolution process.

Because of the additional benefits afforded by a metadata-plus-topic log, this *Commentary* recommends this type of log be considered the preferred format over a traditional log for most cases. However, the alternative log formats discussed in this

Commentary should be evaluated for their suitability to the case, based on the unique documents and factors at issue.

4. Different logs for different, nontraditional sources

New forms of communication present unique challenges, as they may not allow for easy export of the same information that would be expected on a log that is generated from metadata. For example, does a text message chain between attorney and client over several weeks, in which nonprivileged content is also discussed, constitute one communication or several? For collaboration tools such as Slack content or Teams channels, how does counsel log a question posed by one participant to the entire room, where responding communications span several days and intermixed messaging? These new forms of communication may have unique metadata fields that should be considered in determining how to log these sources.

It may be more efficient and lead to fewer disputes to prepare a log of nontraditional sources in a format separate from traditional ESI sources, as the fields necessary to substantiate the privilege are likely to be different. For example, for a withheld Slack channel communication, where the responding party has processed the Slack channel communications in 24-hour slices by agreement, the responding party can log the channel by providing fields such as: Date, Participants, Channel Name, Privilege Basis, Topic/Subject Matter. Note that the Participants field would reflect only the individuals that were in that channel/room in that allotted date/time slice. This is just one example of the emerging, nontraditional business communications that may give rise to unique privilege logging challenges.

C. *Early Conferences to Discuss Privilege Logging Issues*

As discussed above, privilege logging imposes burdens on both the requesting party and the responding party, and the parties' divergent views on what constitutes an adequate privilege log often lead to costly and time-consuming disputes. Early case communication is a critical step in streamlining the privilege log process and minimizing disputes between the parties. Parties can minimize or even eliminate many of the potential burdens associated with privilege logs by addressing them at the outset through an initial conference, negotiation of an ESI protocol or other agreement regarding privilege logs, and then consummation of agreed-upon procedures at the Rule 26(f) conference.

Some courts specifically require this type of discussion. For example, the U.S. District Court for the Northern District of California Guidelines for the Discovery of Electronically Stored Information requires parties to discuss at the 26(f) conference: "Opportunities to reduce costs and increase efficiency and speed, such as . . . using agreements for truncated or limited privilege logs . . . ."[111] Similarly, the Middle District of Tennessee's Administrative Rules provide an expectation that the parties will "discuss foregoing using traditional document-by-document logs in favor of alternate logging methods, such as identifying information by category or including only information from particular metadata fields (e.g., author, recipient, date)."[112]

[111] N.D. Cal. Guidelines for the Discovery of Electronically Stored Information, Guideline 2.02, *available at* https://www.cand.uscourts.gov/filelibrary/1117/ESI_Guidelines-12-1-2015.pdf (last visited May 16, 2024).

[112] M.D. Tenn. Admin. Rule 174-1, ¶ 8(b) (Sept. 12, 2018), *available at* https://www.tnmd.uscourts.gov/sites/tnmd/files/AO%20174-1%20entered%209-12-18.pdf.

Topics for these early communications can include: (1) privilege log exclusions; (2) the use of technology like email threading and its impact on the information contained in the privilege log; (3) alternative log formats for some or all of the ESI at issue; (4) when logs will be produced; and (5) court interaction to reduce disputes. More specifically, parties should consider the following questions:

What needs to be logged? Identify categories of information that can potentially be excluded from the privilege log process, such as the categories identified above.[113] Discuss if the responding party intends to identify and group all of the emails in the same email thread and identify the inclusive email message in lieu of logging each email in the thread.[114] Where the parties agree that only last-in-time emails will be included on a privilege log, discuss whether privilege logs will include (either in a separate field or in the narrative description) the names of the attorneys or third parties that were directly involved in the unlogged emails, if any, that give rise to or call into question the assertion of privilege. If the parties agree to exclude redacted documents from the privilege log, discuss what bibliographic information must remain unredacted on the face of the redacted document or provided in the metadata.[115] Discuss whether any privileges or protections other than attorney-client or work product may apply in the case, and if so, whether those privileges or protections warrant special/unique privilege procedures.

How does it need to be logged? Parties should consider the form, format (i.e., Excel vs. PDF), contents, and how attorneys and non-parties will be identified on the privilege logs (or

[113] *See* Section III.A.

[114] *See* Section II.E.

[115] *See* Section III.A.

through a separate document) to be used in the case and build that into an order entered by the court. Parties should seek agreement on how attorneys and third parties will be identified in the privilege logs, such as by providing separate lists and/or providing email addresses for logged emails. Similarly, consider whether to provide a list of the individuals identified in the privilege logs, with information such as titles/roles and company affiliations, and any limitations to that request. Further, parties should evaluate what additional metadata fields should be provided as part of the privilege logs to better illustrate the nature of the documents, including potentially "FamilyID" (to identify which documents relate to one another); "EmailThreadID" (to identify emails that are part of the same email thread, if threading is used); and "Redacted" (to identify when a document contains a redaction). If email thread suppression is used, decide whether the logging party will provide a description only for the inclusive emails in a thread, propagate the description to all of the noninclusive emails in the thread, or provide a separate description for all of the withheld emails in the thread. Confirm how the privilege log will be provided to the requesting party (PDF or Excel). Discuss if name normalization will be employed, or if the log will instead provide the email addresses of each individual on the log (if exporting this information from the document's metadata).

<u>When does it need to be logged</u>? A thoughtful approach to the timing of privilege logs (particularly when accompanied by early, candid discussion of the issue) can alleviate burdens. Parties should discuss early whether they intend to provide privilege logs either after substantial completion of production, or a "rolling" log that reflects withheld documents at the time of each production. As discussed in Section II.F, if the production is extremely large, rolling logs of some type may lessen the burden of dispute resolution by allowing the parties to engage earlier with each other and, if necessary, with the

court to resolve concerns with the logs themselves (format, detail, mechanics), as well as the scope of the applicable privilege or waiver—potentially informing later productions/logs on similar issues. On the other hand, requiring rolling logs in large volume cases where later document review may be necessary to inform or correct proper privilege determinations typically is extremely inefficient. This could lead to lower quality privilege logs, additional costs to revise privilege logs, and an increased likelihood of inadvertent production of privileged material. Where possible, the parties should seek agreement on whether depositions should be delayed until privilege log issues are resolved (by the parties or the court), or alternatively, whether witnesses may be recalled for an additional deposition for questioning documents that are later found to be not privileged.

What happens when a dispute arises? Planning for potential disputes regarding privilege logs, and discovery in general, can make resolution of those disputes, with minimal involvement by the court, more likely if and when they arise later. One step to facilitate this is adding certain mechanisms in the discovery protocol or similar written agreement between the parties at the outset of the case, or as soon as the responding party has obtained a grasp on the general nature and volume of privileged documents in its document population.

Consider incorporating the following concepts in a discovery protocol:

- At the beginning of a case, seek to include a date in the protocol to have a discovery conference with the court later during the discovery period. As discovery progresses, the prospect of defending one's discovery process or positions in front of the court at the set date may help keep all parties in line.

- Exchange sample privilege logs (10, 25, 50, or 100 entries) at the outset of discovery to confirm format, fields, and how, generally, the information in the log will be presented.
- Set requirements for what privilege logs should contain, including, at a minimum, the use of alternatives to a traditional log,[116] or the exclusion of certain documents from logs.[117] As with other aspects of the discovery process (such as document requests and search terms), getting to the "right" level of specificity can be facilitated through early discussion. The parties and the court should seek to define what type and level of specificity should be used for the privilege logs and a process that allows requesting parties to ask for more specific information, while also protecting responding parties from undue burden.
- Determine a process for challenging a privilege designation. This process can include: (1) a timeline for identification of possible errors or oversights, with a set timeline for the designating party to either agree and produce the documents or affirm that the privilege was properly asserted (see more below); (2) a commitment to confer before contacting the court or filing a motion; (3) a requirement that a party objecting to privilege designations raise specific challenges to individual or categories of documents in writing, with a set time period for the designating party to respond in writing by either agreeing to remove the privilege, providing additional information to support the assertion of privilege, or affirming the party's position

[116] *See* Section III.B and Appendix A.

[117] *See* Section III.A.

that no additional information is required to properly support the existence of a privilege; and (4) a commitment to contact the court for a status conference or other guidance prior to filing motions.

- Identify specific deadlines for when privilege logs will be produced (e.g., a certain time period after each production, after production is complete) that takes into account the practical reality of preparing the logs (including the burdens) and the requesting party's need to review and potentially challenge the logs in time to obtain documents and use them in depositions, in dispositive motions, with an expert, or at trial, or to raise challenges with the court before the close of discovery.[118]
- Discuss clawback procedures. The expanding volume of ESI led Congress to amend Federal Rule of Civil Procedure 26(f) in 2006 to instruct the parties to address clawback agreements in the Rule 26(f) conference.[119] Parties should also discuss the applicability of a Federal Rule of Evidence 502(d) Order.

Early case assessment and planning by the parties at the outset of the case can help alleviate, or at least make less burdensome, disputes related to the privilege logging process that may arise later in the case.[120]

[118] *See* Section II.F.

[119] As Congress explained: "The volume of such [ESI], and the informality that attends use of e-mail and some other types of electronically stored information, may make privilege determinations more difficult, and privilege review correspondingly more expensive and time consuming." FED. R. CIV. P. 26 advisory committee's note to 2006 amendment.

[120] It should be noted, however, that parties may not be in a position to fully discuss and negotiate privilege logging issues during the Rule 26

conference. At this early stage of the case, parties generally do not have a complete picture of what will be required during discovery, including as it relates to privilege logs. For example, responding parties are not likely to know their full custodian list, the prevalence of privileged communications in the production set, or the complexity of privilege issues that may arise once the review begins. Thus, even where parties engage in early discussion at the Rule 26 conference and memorialize agreements related to privilege logging in a discovery protocol, privilege logging challenges may still arise as the case proceeds. In these cases, parties should further confer on privilege logging issues as soon as the responding party has enough information related to the scope and volume of privileged documents in its document population to meaningfully engage on the issues.

IV. RESOLVING PRIVILEGE LOG DISPUTES

A. Preliminary communications to narrow issues

Rather than seeking court intervention as a first step, parties should engage with each other when a privilege logging issue first arises. What appears to be a potentially contentious issue may be nothing more than a simple oversight or unintentional error by the responding party. It could be the result of a coding error, a formatting mistake, or mere oversight. When brought to the responding party's attention, the party may be willing to fix the issue if it was an error or explain the claim further. If the parties have agreed on a Rule 502(d) order, they may consider leveraging it to allow the requesting party's counsel to view challenged innocuous privileged documents to resolve the dispute and then claw back.

Additionally, it may be that the process and format that the parties agreed on at the beginning of discovery does not, in practice, meet one or both of the parties' needs. This may be because of a misunderstanding or miscommunication, or it may also be a function of counsel making decisions before knowing what the discovery would actually include. Parties should be open to altering the format or providing additional information where necessary.

To this end, rather than letting these issues sit until it is time to set a formal conference in advance of a motion to compel, it is worth communicating with the opposing party more informally to address what appear to be oversights, mistakes, or inadvertently poor entries. It will benefit both parties to try to narrow the issues before engaging in more contentious discovery dispute resolution.

B. Formal conference

Typically, the applicable rules will require that parties hold a formal conference prior to the filing of a motion.[121] Even if the filing of a motion is not imminent, a formal conference should be set when informal discussions have reached a stalemate or when issues with a privilege log appear to be intentional, systemic, or involve genuine issues regarding how the law should be applied to a particular document.

A formal conference can be used to identify any areas where the parties agree, where a compromise can be had, and where court intervention is needed. To this end, consider providing a concrete plan for the conference with a scope of the issues to be discussed. Identify the specific document identifiers, log entries, or categories and the claimed deficiencies so that a constructive discussion can be had about them. Remember that a specific and well-defined concern is more likely to be considered than an ambiguous complaint. For example, where the requesting party has insufficient information to assess the privilege asserted via a categorical log, the requesting party should specify what additional information it needs. If particular entries are at issue, be as specific as possible in explaining why they are deficient. Then, use the conference to resolve misunderstandings and narrow the issues that need to be brought before the court.

As agreements to provide additional information are made, set periodic deadlines to provide the parties' positions or supplemental information. Such deadlines will keep responding parties accountable and provide an additional basis to seek court intervention to resolve the privilege dispute.

[121] *See, e.g.*, FED. R. CIV. P. 37(a)(1); CAL. CIV. PROC. CODE § 2016.040; LA. DIST. CT. R. 10.1; N.C. GEN. STAT. ANN. § 1A-1, R. 37(a)(2).

C. In camera review

The failure of parties to provide sufficient information on a privilege log can lead to disputes between the parties.[122] One mechanism to address this issue is seeking in camera review by the court of some or all of the withheld documents.[123] Depending on the volume of documents subject to challenge, this can be a time-consuming process for the courts. Whether to conduct an in camera review lies within the court's discretion.[124]

[122] *See, e.g.*, Chevron Corp. v. Weinberg Group, 286 F.R.D. 95, 99 (D.D.C. 2012) ("But, the descriptor in the modern database has become generic . . . the human being creates one description and the software repeats that description for all the entries for which the human being believes that description is appropriate . . . . This raises the term 'boilerplate' to an art form, resulting in the modern privilege log being as expensive to produce as it is useless."). *See also* Earthworks v. U.S. Dep't of the Interior, 279 F.R.D. 180, 193 (D.D.C. 2012); Lurensky v. Wellinghoff, 271 F.R.D. 345, 355 (D.D.C. 2010) (finding "privilege logs to be on the whole useless"); *In re* Rail Freight Fuel Surcharge Antitrust Litig., No. 07-489(PLF/JMF/AK), 2009 WL 3443563, at *10 (D.D.C. Oct. 23, 2009); Marshall v. D.C. Water & Sewage Auth., 214 F.R.D. 23, 25 n.4 (D.D.C. 2003); Mitchell v. Nat. R.R. Passenger Corp., 208 F.R.D. 455 (D.D.C. 2002); Avery Dennison Corp. v. Four Pillars, 190 F.R.D. 1, 2 (D.D.C. 1999) ("I have found that counsel rarely provides more than minimal information in the logs they submit which usually tell me the date of the document, its author and recipient, and the briefest possible description of its contents ('Letter from client to attorney'). Finding such a log useless, I have instead cut to the quick and ordered the production of the documents at issue.").

[123] *See, e.g.,* Bethea v. Merchants Com. Bank, No. 11-51, 2012 WL 5359536, note 5 (D.V.I. Oct. 31, 2012) ("[p]roviding information [a description] pertinent to the applicability of the privilege or protection should reduce the need for *in camera* examination of the documents.").

[124] *See, e.g.,* Washtenaw Cty. Emps.' Ret. Sys. v. Walgreen Co., No. 15 C 3187, 2020 WL 3977944, at *3 (N.D. Ill. July 14, 2020) ("But ultimately the question of whether to engage in an *in camera* review lies within the Court's discretion, and the Court ought not to engage in an *in camera* review of even a manageable number of documents if the review is not warranted. Where a

The decision turns on many factors, including whether it would be a needless use of the court's resources.[125] To reduce the burden and to preserve the court's resources, a court may provide guidance to parties to apply to contested documents and recurrent privilege issues[126] or sample a subset of the documents subject to challenge to determine whether further in camera review is appropriate. In addition, judges may consider the use of special discovery masters to help parties secure prompt resolution of discovery disputes, including potential in camera review of contested documents. The use of special discovery masters, or other neutral specialists, to review documents for privilege may come at a high cost to litigants, who will have to pay for their services, either jointly or by one party, depending on whether the challenge or the assertion of privilege was in good faith. However, requiring a log with

court's discretion is involved, two judges can reach two correct yet contrary conclusions based on identical fact patterns.") (citations omitted).

[125] *See, e.g.*, *Washtenaw*, 2020 WL 3977944, at *3 (citing Am. Nat. Bank & Trust Co. of Chicago v. Equitable Life Assurance Soc. of the United States, 406 F.3d 867, 879-880 (7th Cir. 2005)) ("The judicial discretion to review the described documents *in camera* has turned on multiple factors, including the burden involved in reviewing the sheer number of documents, but the thrust of these cases is that *in camera* review is more critical before compelled disclosure, so courts might make sure that the disclosed materials truly are not privileged."); *see also* NLRB v. Jackson Hosp. Corp., 257 F.R.D. 302, 307 (D.D.C. 2009) ("[D]eeming the log a waiver is the most draconian but the least consumptive of judicial resources while *in camera* inspection of all of the withheld documents is the most forgiving but the most consumptive of judicial resources.").

[126] *See, e.g.*, Chabot v. Walgreens Boots All., Inc., No. 1:18-CV-2118, 2020 WL 3410638, at *3 (M.D. Pa. June 11, 2020) ("To lessen the burdens associated with *in camera* review, the Court may dictate its holding on contested issues, which the parties will then apply when determining whether its documents are privileged.").

sufficient detail to describe the privilege may alleviate the need for in camera review.

V. CONCLUSION

The privilege logging process can be fraught with challenges and burdens for requesting parties, responding parties, and the courts. This *Commentary* suggests ways to navigate these issues, including (1) mitigating the burdens on responding parties associated with preparing a privilege log and protecting its privilege claims, (2) promoting the rights of requesting parties to be able to assess those claims, and (3) reducing the challenges on the courts to resolve privilege log disputes. A key ingredient in this process is cooperation among the parties. As a result, parties should endeavor to address as many privilege log issues as possible as early as practicable in the discovery process, including through the Rule 26(f) conference and discovery protocols.

As detailed above, this *Commentary* suggests that traditional privilege logging does not materially add to the necessary threshold showing of privilege substantiation for certain groups of documents, such as communications with outside counsel after the date of litigation, post-complaint work product, and redacted documents, and the parties should discuss excluding those groups of documents from privilege logging altogether. In addition, the use of alternative log formats may help parties strike a balance between providing information necessary to support a privilege claim with having to generate a costly traditional privilege log.[127] This *Commentary* takes the position that a metadata-plus-topic log will generally be the best format to streamline the privilege log process in a way that is beneficial to both parties and the courts and allows the requesting party to focus requests for additional information where warranted. This approach may reduce the number of documents in dispute and lead to lesser effort, in terms of time, cost, and items of

[127] *See* Appendices A, B, and C.

dispute, for both parties than the traditional manner of logging every withheld document.

APPENDIX A: INTRODUCTION TO WIDGETS EXEMPLARS AND EXAMPLE PRIVILEGE LOGS

Background

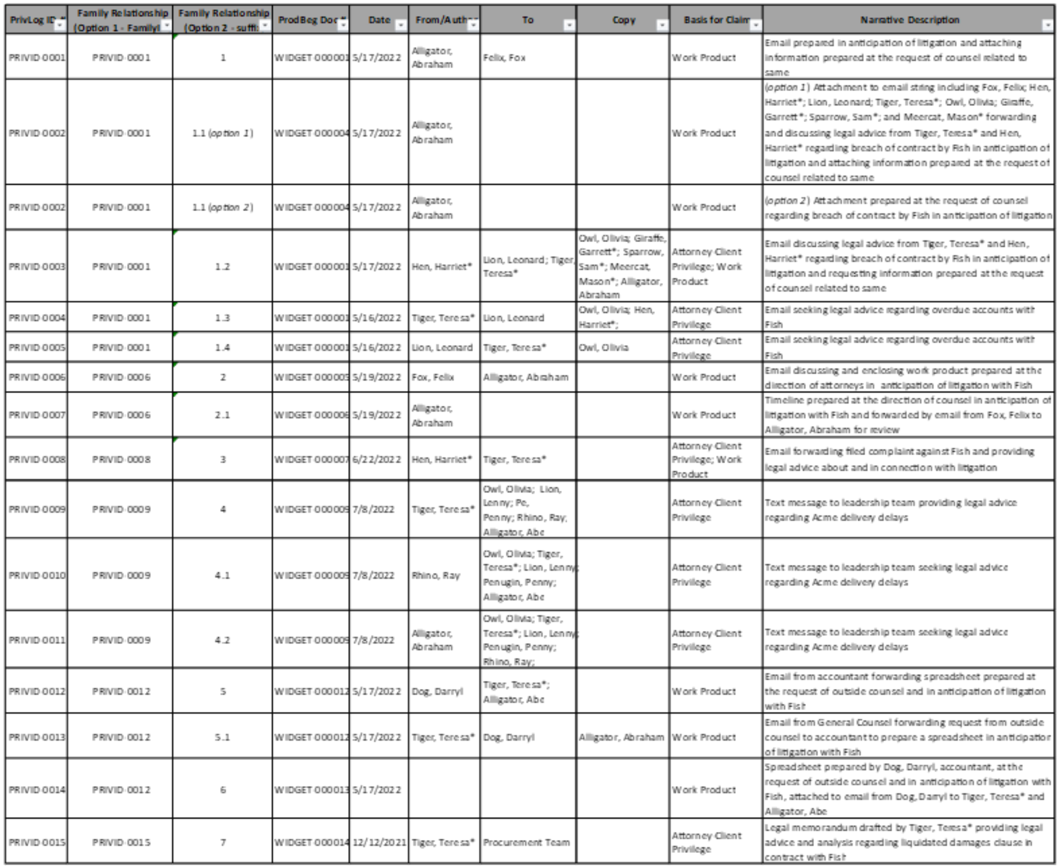
Certain information fields may be typical or expected on a privilege log and others are optional, depending on the needs of the case. Included in Appendices A and C are examples of various privilege log formats along with sample documents that appear on the logs. The exemplar documents and privilege logs are hypothetical and not intended to be perfect from a substantive, factual, or legal standpoint. However, these exemplars are useful tools for helping to understand terminology and illustrate different types of privilege logs, as well as provide a visual representation of the strengths and weaknesses of each type of privilege log. Ultimately, the party producing the privilege log must determine what is required and/or appropriate based on the particular circumstances of its case, including applicable rules, case law, judicial standing orders, volume and type of documents, and agreements between the parties.

To help illustrate the distinct features of the various privilege log formats, we are providing several reference points here. First, each field on the exemplars is defined in Appendix B and, where appropriate, commentary is provided. Second, the exemplars themselves are annotated to identify fields and items that are common in that type of privilege log versus potential ones, which may or may not be included (asterisked) depending on various factors.

For ease of readability, the exemplars can be downloaded in their native .xlsx format by clicking on this link.

A-1 TRADITIONAL PRIVILEGE LOG EXEMPLAR

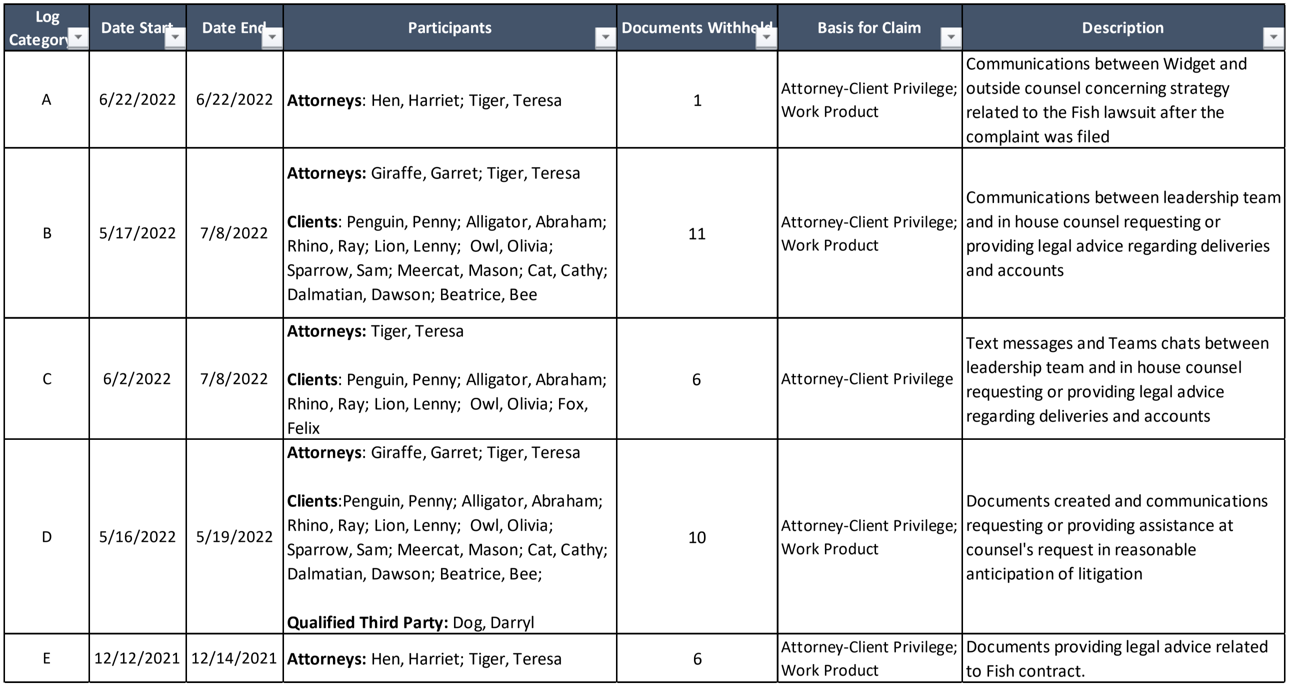
Click here to view the Traditional Privilege Log in its native .xlsx format.



PrivLog ID	Family Relationship (Option 1 - Family	Family Relationship (Option 2 - suffi	ProdBeg Doc	Date	From/Auth	To	Copy	Basis for Claim	Narrative Description
PRIVID-0001	PRIVID-0001	1	WIDGET 000001	5/17/2022	Alligator, Abraham	Felix, Fox		Work Product	Email prepared in anticipation of litigation and attaching information prepared at the request of counsel related to same
PRIVID-0002	PRIVID-0001	1.1 *(option 1)*	WIDGET 000004	5/17/2022	Alligator, Abraham			Work Product	*(option 1)* Attachment to email string including Fox, Felix; Hen, Harriet*; Lion, Leonard; Tiger, Teresa*; Owl, Olivia; Giraffe, Garrett*; Sparrow, Sam*; and Meercat, Mason* forwarding and discussing legal advice from Tiger, Teresa* and Hen, Harriet* regarding breach of contract by Fish in anticipation of litigation and attaching information prepared at the request of counsel related to same
PRIVID-0002	PRIVID-0001	1.1 *(option 2)*	WIDGET 000004	5/17/2022	Alligator, Abraham			Work Product	*(option 2)* Attachment prepared at the request of counsel regarding breach of contract by Fish in anticipation of litigation
PRIVID-0003	PRIVID-0001	1.2	WIDGET 000001	5/17/2022	Hen, Harriet*	Lion, Leonard; Tiger, Teresa*	Owl, Olivia; Giraffe, Garrett*; Sparrow, Sam*; Meercat, Mason*; Alligator, Abraham	Attorney-Client Privilege; Work Product	Email discussing legal advice from Tiger, Teresa* and Hen, Harriet* regarding breach of contract by Fish in anticipation of litigation and requesting information prepared at the request of counsel related to same
PRIVID-0004	PRIVID-0001	1.3	WIDGET 000001	5/16/2022	Tiger, Teresa*	Lion, Leonard	Owl, Olivia; Hen, Harriet*;	Attorney-Client Privilege	Email seeking legal advice regarding overdue accounts with Fish
PRIVID-0005	PRIVID-0001	1.4	WIDGET 000001	5/16/2022	Lion, Leonard	Tiger, Teresa*	Owl, Olivia	Attorney-Client Privilege	Email seeking legal advice regarding overdue accounts with Fish
PRIVID-0006	PRIVID-0006	2	WIDGET 000003	5/19/2022	Fox, Felix	Alligator, Abraham		Work Product	Email discussing and enclosing work product prepared at the direction of attorneys in anticipation of litigation with Fish
PRIVID-0007	PRIVID-0006	2.1	WIDGET 000006	5/19/2022	Alligator, Abraham			Work Product	Timeline prepared at the direction of counsel in anticipation of litigation with Fish and forwarded by email from Fox, Felix to Alligator, Abraham for review
PRIVID-0008	PRIVID-0008	3	WIDGET 000007	6/22/2022	Hen, Harriet*	Tiger, Teresa*		Attorney-Client Privilege; Work Product	Email forwarding filed complaint against Fish and providing legal advice about and in connection with litigation
PRIVID-0009	PRIVID-0009	4	WIDGET 000009	7/8/2022	Tiger, Teresa*	Owl, Olivia; Lion, Lenny; Pe, Penny; Rhino, Ray; Alligator, Abe		Attorney-Client Privilege	Text message to leadership team providing legal advice regarding Acme delivery delays
PRIVID-0010	PRIVID-0009	4.1	WIDGET 000009	7/8/2022	Rhino, Ray	Owl, Olivia; Tiger, Teresa*; Lion, Lenny; Penugin, Penny; Alligator, Abe		Attorney-Client Privilege	Text message to leadership team seeking legal advice regarding Acme delivery delays
PRIVID-0011	PRIVID-0009	4.2	WIDGET 000009	7/8/2022	Alligator, Abraham	Owl, Olivia; Tiger, Teresa*; Lion, Lenny; Penugin, Penny; Rhino, Ray;		Attorney-Client Privilege	Text message to leadership team seeking legal advice regarding Acme delivery delays
PRIVID-0012	PRIVID-0012	5	WIDGET 000012	5/17/2022	Dog, Darryl	Tiger, Teresa*; Alligator, Abe		Work Product	Email from accountant forwarding spreadsheet prepared at the request of outside counsel and in anticipation of litigation with Fish
PRIVID-0013	PRIVID-0012	5.1	WIDGET 000012	5/17/2022	Tiger, Teresa*	Dog, Darryl	Alligator, Abraham	Work Product	Email from General Counsel forwarding request from outside counsel to accountant to prepare a spreadsheet in anticipation of litigation with Fish
PRIVID-0014	PRIVID-0012	6	WIDGET 000013	5/17/2022				Work Product	Spreadsheet prepared by Dog, Darryl, accountant, at the request of outside counsel and in anticipation of litigation with Fish, attached to email from Dog, Darryl to Tiger, Teresa* and Alligator, Abe
PRIVID-0015	PRIVID-0015	7	WIDGET 000014	12/12/2021	Tiger, Teresa*	Procurement Team		Attorney-Client Privilege	Legal memorandum drafted by Tiger, Teresa* providing legal advice and analysis regarding liquidated damages clause in contract with Fish

A-2 CATEGORICAL PRIVILEGE LOG EXEMPLAR

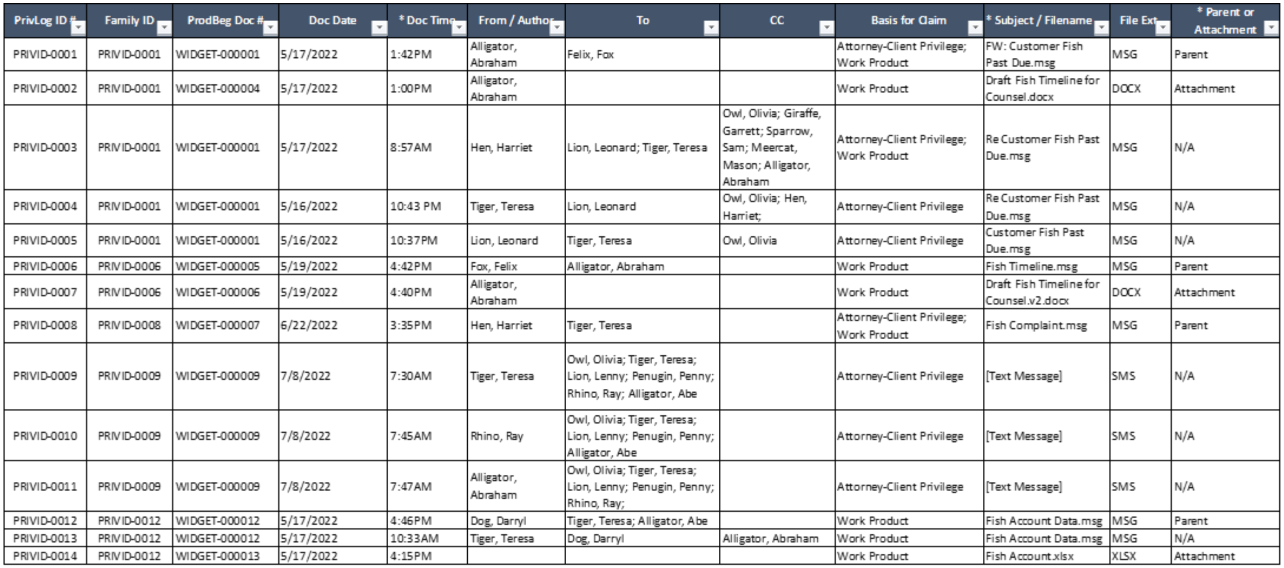
Click here to view the Categorical Privilege Log in its native .xlsx format.



Log Category	Date Start	Date End	Participants	Documents Withheld	Basis for Claim	Description
A	6/22/2022	6/22/2022	**Attorneys**: Hen, Harriet; Tiger, Teresa	1	Attorney-Client Privilege; Work Product	Communications between Widget and outside counsel concerning strategy related to the Fish lawsuit after the complaint was filed
B	5/17/2022	7/8/2022	**Attorneys:** Giraffe, Garret; Tiger, Teresa **Clients**: Penguin, Penny; Alligator, Abraham; Rhino, Ray; Lion, Lenny; Owl, Olivia; Sparrow, Sam; Meercat, Mason; Cat, Cathy; Dalmatian, Dawson; Beatrice, Bee	11	Attorney-Client Privilege; Work Product	Communications between leadership team and in house counsel requesting or providing legal advice regarding deliveries and accounts
C	6/2/2022	7/8/2022	**Attorneys:** Tiger, Teresa **Clients**: Penguin, Penny; Alligator, Abraham; Rhino, Ray; Lion, Lenny; Owl, Olivia; Fox, Felix	6	Attorney-Client Privilege	Text messages and Teams chats between leadership team and in house counsel requesting or providing legal advice regarding deliveries and accounts
D	5/16/2022	5/19/2022	**Attorneys**: Giraffe, Garret; Tiger, Teresa **Clients**:Penguin, Penny; Alligator, Abraham; Rhino, Ray; Lion, Lenny; Owl, Olivia; Sparrow, Sam; Meercat, Mason; Cat, Cathy; Dalmatian, Dawson; Beatrice, Bee; **Qualified Third Party:** Dog, Darryl	10	Attorney-Client Privilege; Work Product	Documents created and communications requesting or providing assistance at counsel's request in reasonable anticipation of litigation
E	12/12/2021	12/14/2021	**Attorneys:** Hen, Harriet; Tiger, Teresa	6	Attorney-Client Privilege; Work Product	Documents providing legal advice related to Fish contract.

A-3 METADATA PRIVILEGE LOG EXEMPLAR

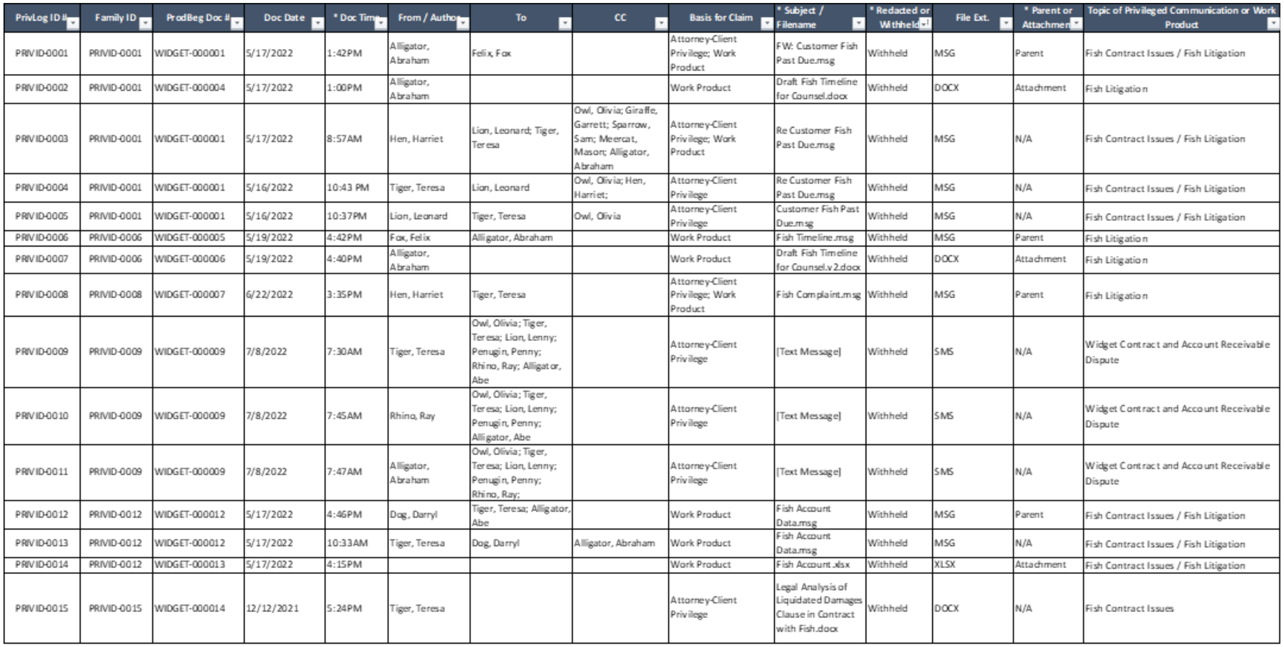
Click here to view the Metadata Privilege Log in its native .xlsx format.



PrivLog ID #	Family ID	ProdBeg Doc #	Doc Date	* Doc Time	From / Author	To	CC	Basis for Claim	* Subject / Filename	File Ext	* Parent or Attachment
PRIVID-0001	PRIVID-0001	WIDGET-000001	5/17/2022	1:42PM	Alligator, Abraham	Felix, Fox		Attorney-Client Privilege; Work Product	FW: Customer Fish Past Due.msg	MSG	Parent
PRIVID-0002	PRIVID-0001	WIDGET-000004	5/17/2022	1:00PM	Alligator, Abraham			Work Product	Draft Fish Timeline for Counsel.docx	DOCX	Attachment
PRIVID-0003	PRIVID-0001	WIDGET-000001	5/17/2022	8:57AM	Hen, Harriet	Lion, Leonard; Tiger, Teresa	Owl, Olivia; Giraffe, Garrett; Sparrow, Sam; Meercat, Mason; Alligator, Abraham	Attorney-Client Privilege; Work Product	Re Customer Fish Past Due.msg	MSG	N/A
PRIVID-0004	PRIVID-0001	WIDGET-000001	5/16/2022	10:43 PM	Tiger, Teresa	Lion, Leonard	Owl, Olivia; Hen, Harriet;	Attorney-Client Privilege	Re Customer Fish Past Due.msg	MSG	N/A
PRIVID-0005	PRIVID-0001	WIDGET-000001	5/16/2022	10:37PM	Lion, Leonard	Tiger, Teresa	Owl, Olivia	Attorney-Client Privilege	Customer Fish Past Due.msg	MSG	N/A
PRIVID-0006	PRIVID-0006	WIDGET-000005	5/19/2022	4:42PM	Fox, Felix	Alligator, Abraham		Work Product	Fish Timeline.msg	MSG	Parent
PRIVID-0007	PRIVID-0006	WIDGET-000006	5/19/2022	4:40PM	Alligator, Abraham			Work Product	Draft Fish Timeline for Counsel.v2.docx	DOCX	Attachment
PRIVID-0008	PRIVID-0008	WIDGET-000007	6/22/2022	3:35PM	Hen, Harriet	Tiger, Teresa		Attorney-Client Privilege; Work Product	Fish Complaint.msg	MSG	Parent
PRIVID-0009	PRIVID-0009	WIDGET-000009	7/8/2022	7:30AM	Tiger, Teresa	Owl, Olivia; Tiger, Teresa; Lion, Lenny; Penugin, Penny; Rhino, Ray; Alligator, Abe		Attorney-Client Privilege	[Text Message]	SMS	N/A
PRIVID-0010	PRIVID-0009	WIDGET-000009	7/8/2022	7:45AM	Rhino, Ray	Owl, Olivia; Tiger, Teresa; Lion, Lenny; Penugin, Penny; Alligator, Abe		Attorney-Client Privilege	[Text Message]	SMS	N/A
PRIVID-0011	PRIVID-0009	WIDGET-000009	7/8/2022	7:47AM	Alligator, Abraham	Owl, Olivia; Tiger, Teresa; Lion, Lenny; Penugin, Penny; Rhino, Ray;		Attorney-Client Privilege	[Text Message]	SMS	N/A
PRIVID-0012	PRIVID-0012	WIDGET-000012	5/17/2022	4:46PM	Dog, Darryl	Tiger, Teresa; Alligator, Abe		Work Product	Fish Account Data.msg	MSG	Parent
PRIVID-0013	PRIVID-0012	WIDGET-000012	5/17/2022	10:33AM	Tiger, Teresa	Dog, Darryl	Alligator, Abraham	Work Product	Fish Account Data.msg	MSG	N/A
PRIVID-0014	PRIVID-0012	WIDGET-000013	5/17/2022	4:15PM				Work Product	Fish Account.xlsx	XLSX	Attachment

A-4 METADATA-PLUS-TOPIC EXEMPLAR PRIVILEGE LOG

Click here to view the Metadata-Plus-Topic Privilege Log in its native .xlsx format.



PrivLog ID #	Family ID	ProdBeg Doc #	Doc Date	* Doc Tim	From / Autho	To	CC	Basis for Claim	* Subject / Filename	* Redacted or Withheld	File Ext.	* Parent or Attachmen	Topic of Privileged Communication or Work Product
PRIVID-0001	PRIVID-0001	WIDGET-000001	5/17/2022	1:42PM	Alligator, Abraham	Felix, Fox		Attorney-Client Privilege; Work Product	FW: Customer Fish Past Due.msg	Withheld	MSG	Parent	Fish Contract Issues / Fish Litigation
PRIVID-0002	PRIVID-0001	WIDGET-000004	5/17/2022	1:00PM	Alligator, Abraham			Work Product	Draft Fish Timeline for Counsel.docx	Withheld	DOCX	Attachment	Fish Litigation
PRIVID-0003	PRIVID-0001	WIDGET-000001	5/17/2022	8:57AM	Hen, Harriet	Lion, Leonard; Tiger, Teresa	Owl, Olivia; Giraffe, Garrett; Sparrow, Sam; Meercat, Mason; Alligator, Abraham	Attorney-Client Privilege; Work Product	Re Customer Fish Past Due.msg	Withheld	MSG	N/A	Fish Contract Issues / Fish Litigation
PRIVID-0004	PRIVID-0001	WIDGET-000001	5/16/2022	10:43 PM	Tiger, Teresa	Lion, Leonard	Owl, Olivia; Hen, Harriet;	Attorney-Client Privilege	Re Customer Fish Past Due.msg	Withheld	MSG	N/A	Fish Contract Issues / Fish Litigation
PRIVID-0005	PRIVID-0001	WIDGET-000001	5/16/2022	10:37PM	Lion, Leonard	Tiger, Teresa	Owl, Olivia	Attorney-Client Privilege	Customer Fish Past Due.msg	Withheld	MSG	N/A	Fish Contract Issues / Fish Litigation
PRIVID-0006	PRIVID-0006	WIDGET-000005	5/19/2022	4:42PM	Fox, Felix	Alligator, Abraham		Work Product	Fish Timeline.msg	Withheld	MSG	Parent	Fish Litigation
PRIVID-0007	PRIVID-0006	WIDGET-000006	5/19/2022	4:40PM	Alligator, Abraham			Work Product	Draft Fish Timeline for Counsel.v2.docx	Withheld	DOCX	Attachment	Fish Litigation
PRIVID-0008	PRIVID-0008	WIDGET-000007	6/22/2022	3:35PM	Hen, Harriet	Tiger, Teresa		Attorney-Client Privilege; Work Product	Fish Complaint.msg	Withheld	MSG	Parent	Fish Litigation
PRIVID-0009	PRIVID-0009	WIDGET-000009	7/8/2022	7:30AM	Tiger, Teresa	Owl, Olivia; Tiger, Teresa; Lion, Lenny; Penugin, Penny; Rhino, Ray; Alligator, Abe		Attorney-Client Privilege	[Text Message]	Withheld	SMS	N/A	Widget Contract and Account Receivable Dispute
PRIVID-0010	PRIVID-0009	WIDGET-000009	7/8/2022	7:45AM	Rhino, Ray	Owl, Olivia; Tiger, Teresa; Lion, Lenny; Penugin, Penny; Alligator, Abe		Attorney-Client Privilege	[Text Message]	Withheld	SMS	N/A	Widget Contract and Account Receivable Dispute
PRIVID-0011	PRIVID-0009	WIDGET-000009	7/8/2022	7:47AM	Alligator, Abraham	Owl, Olivia; Tiger, Teresa; Lion, Lenny; Penugin, Penny; Rhino, Ray;		Attorney-Client Privilege	[Text Message]	Withheld	SMS	N/A	Widget Contract and Account Receivable Dispute
PRIVID-0012	PRIVID-0012	WIDGET-000012	5/17/2022	4:46PM	Dog, Darryl	Tiger, Teresa; Alligator, Abe		Work Product	Fish Account Data.msg	Withheld	MSG	Parent	Fish Contract Issues / Fish Litigation
PRIVID-0013	PRIVID-0012	WIDGET-000012	5/17/2022	10:33AM	Tiger, Teresa	Dog, Darryl	Alligator, Abraham	Work Product	Fish Account Data.msg	Withheld	MSG	N/A	Fish Contract Issues / Fish Litigation
PRIVID-0014	PRIVID-0012	WIDGET-000013	5/17/2022	4:15PM				Work Product	Fish Account.xlsx	Withheld	XLSX	Attachment	Fish Contract Issues / Fish Litigation
PRIVID-0015	PRIVID-0015	WIDGET-000014	12/12/2021	5:24PM	Tiger, Teresa			Attorney-Client Privilege	Legal Analysis of Liquidated Damages Clause in Contract with Fish.docx	Withheld	DOCX	N/A	Fish Contract Issues

APPENDIX B: DESCRIPTIONS OF PRIVILEGE LOG FIELDS

Field Descriptions Frequently Found in Traditional Privilege Logs

Field Name	**Definition**
Privilege ID #	A unique number assigned to each entry on the log to help the parties and the court identify a specific entry. **Comment:** It is not recommended to use an internal document ID number from, for example, a review database, because it may reveal other information about the data set, like overall volume. To avoid confusion, if additional or supplemental logs are produced, they should *continue* the numbering and *not restart* with the same first number from the first log.
ProdBeg Doc #	The beginning Bates number for a document, typically only for a produced document. **Comment:** Some practitioners do not assign a Bates number to a document withheld in its entirety on the basis of privilege, work product, etc. Others will assign a Bates number to a single page "slip sheet" to help with tracking the document. If used, some parties may also include a ProdEnd Doc # (the ending Bates number for a document).

Field Name	**Definition**
Date	The date when a communication was sent. In the case of a document, often the date it was last modified. **Comment:** For privilege logs where the parties have agreed to populate the fields from metadata, practitioners may choose to use one from multiple date fields, including date last modified, date sent, master family date. Because multiple date fields are available, parties should discuss which date they intend to use. For documents without metadata, practitioners may choose to use the date reflected on the face of the document (assuming the parties have agreed to produce it).
From/ Author	This field is designed to capture who originated the communication or document. "From" is meant for communications like emails, whereas "Author" is for documents. **Comment:** It is common to combine these into a single field to save space on a log. For this field, and To, CC, BCC, parties should discuss whether name normalization will be used.
To	This field reflects who the communication or document (e.g., memorandum) was sent to.

Field Name	**Definition**
*Copy or CC	This field reflects anyone copied on the communication or document (e.g., memorandum). **Comment:** Some practitioners will group everyone who received a communication into a single field/column—for example, in the case of an email, all of the To / CC / BCC will be grouped into a single "Recipients" field.
*Blind Copy or BCC	This field reflects anyone blind copied on an email (or communication where such a function is available). **Comment:** It is common to exclude this field when none of the documents on the log include any BCC information.
Basis for Claim	This field identifies each legal basis for withholding the information at issue (e.g., attorney-client privilege, work product, common-interest doctrine, marital privilege, etc.). **Comment:** Each and every applicable basis should be asserted to avoid a contention by the opposing party that it has been waived.

Field Name	**Definition**
Family Relationship	A privilege log should identify whether a document is a parent or a child (attachment), so that the receiving party can understand the context and connection between multiple documents on the privilege log. Parties use various ways to do this. **Comment:** The "Traditional Log" exemplar shows three potential options, though practitioners may use alternative methods: (1) Using a "Family Identifier" field (see description in Metadata table below) – can be automated. (2) Using a suffix in the PrivLog ID # (e.g., parent email is 3 and the child/attachment is 3.1) (note that a second attachment would be 3.2) – this is a manual population. (3) Using a detailed "attachment description" to identify that the document is an attachment and to note which individuals received or sent the attachment (e.g., the first attachment description on the log).

Field Name	Definition
Narrative Description	If Subject and/or Filename is included, and sufficiently particularized, then some practitioners may provide less detail in the Narrative Description. **Comment:** Note the two versions of a Narrative Description for an attachment on the "Traditional Log" at PrivLog ID # 4a and 4b. Practitioners may include all of the names from the parent email (or email string) of those who sent or received the attachment, to better explain why the attachment remains protected. Others may not include names for various reasons, including: (1) the parent email was also withheld and is located immediately above the attachment entry, and those names will be visible there; (2) the parent email has been produced, which allows the requesting party to view the names in the produced parent email; and/or (3) the litigant's position is that including names in attachment descriptions is not required. The level of detail for this description may depend on the document itself and the needs of the case.

Field Name	**Definition**
*Redacted or Withheld	This field identifies whether a document has been withheld in its entirety or only redacted. **Comment:** Not all practitioners do this; some, as an alternative, state in the Description itself whether a document has been redacted. Others may produce two separate logs, one for withheld documents and another for redacted ones. This *Commentary* supports not logging redacted documents at all in the first instance (*see* Section III.A), which moots this field altogether. Accordingly, the sample logs do not include this column.

Additional Field Descriptions Frequently Found in Metadata or Metadata-Plus Privilege Logs

Field Name	**Definition**
File Extension/ Doc Type	Identifies the file type and format of a document, or the application in which the document was created. **Comment:** For example, ".doc, .xlsx, PowerPoint, etc."
Family Identifier (Family ID)	Identifies the family relationship of the privileged document so the receiving party can identify family members either on the privilege log or within the producing party's production. **Comment:** The Family Identifier uses either: (1) the beginning Bates number of the parent email for withheld/redacted documents assigned a Bates number; or (2) the Privilege Identifier of the parent email within fully withheld families that are not assigned a Bates number.
*Time	The time a document was created, sent, modified, etc. **Comment:** Some practitioners may choose to include this as a separate standalone field; others may combine it with the date field.
*Custodian/ Custodians	The individual or source from whom the document was collected. **Comment:** This field may be pulled from the metadata of the document, if available.

Field Name	**Definition**
*Last Author	The name or ID of the person who last created the document. **Comment:** This field may be pulled from the metadata of the document, if available.
*Last Edited By	The name or ID of the person who last revised the document. **Comment:** This field may be pulled from the metadata of the document, if available.
*Email Thread ID	Constitutes an ID value that indicates which conversation an email belongs to and where in that conversation it occurred.
*Hash Value	Reflects a unique value for a given set of data, similar to a digital fingerprint, representing the binary content of the data to assist in subsequently ensuring that data has not been modified.
*Additional Communicants	The names of other individuals who appeared as a sender or recipient in earlier portions of an email chain that are redacted or withheld, but who are not present from the metadata of the most inclusive part of the email chain. **Comment:** This field is generally manually populated by the reviewer. Thus, the inclusion of this field is subject to negotiation. Names of senders/recipients for portions of the email that are being produced would not need to be included in this field.

Field Name	**Definition**
*Other Legal Persons	Reflects other attorneys that may be present in the withheld document, or otherwise create the privilege, that are not reflected in the metadata of the document. **Comment:** Because this needs to be manually populated, it cannot be pulled from metadata alone. It may be provided in a metadata-plus log.

Field Name	**Definition**
*Subject / Filename	This field reflects the email "Subject" line and the metadata "Filename" for a document, which may be presented as a single field or two separate fields. *The Sedona Glossary* further defines "filename" as a name used to identify a specific file in order to differentiate it from other files, typically comprised of a series of characters, a dot, and a file extension (e.g., sample.doc). *The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition*, 21 SEDONA CONF. J. 263, 311. **Comment:** Practitioners may include this field because they believe it helps provide information about the document. Practitioners may exclude this field because, for example, it may contain privileged or work-product material and thus requires additional review. Depending on the type of log, this field may or may not be helpful. For example, if a traditional log includes a robust description, then this field may not be useful; but if doing a metadata or metadata-plus-topic log, it may be needed. The sample traditional privilege log does not include a "Subject/Filename" field because the descriptions are detailed.

Additional Field Descriptions Frequently Found in Categorical Privilege Logs

Field Name	Definition
Log Category #	A grouping number for each set of documents assigned a particular category.
Date Start/Date End	The beginning and ending date range for the documents associated with a particular category.
Description	A narrative sentence providing the topic of the legal advice sought/provided.
Participants	The names and roles of the individuals participating as communicants in the documents withheld in that category. **Comment:** Includes all senders, recipients, and copyees.
Documents Withheld	A count of the documents withheld in that category.

APPENDIX C: FACT PATTERN FOR WIDGETS EXEMPLARS AND EXEMPLAR DOCUMENTS

Fact Pattern

The sample documents that follow relate to three hypothetical legal issues/disputes involving Widgets, Inc. (a distributor of widgets), Acme, Inc. (a manufacturer/supplier of widgets), and Fish, Inc. (a consumer of widgets). The first issue is a payment dispute. On January 1, 2022, Fish contracted to purchase 100,000 widgets from Widgets, monthly, at a purchase price of $1.00 per widget. The terms of the contract included a provision that states: "A late fee of 1% of the unpaid invoice will be due on any payment not made within ten (10) business days of shipment in accordance with this Agreement, and Widgets reserves the right to cure the default in a Court of Law without necessity of notice." Widgets made their monthly shipment to Fish on February 1, 2022, and Widgets Sales Agent, Felix Fox, promptly sent Fish a notice of shipment and an invoice for $100,000. Felix received confirmation of delivery on February 3, 2022. Payment was not received, and Felix notified Fish of its outstanding balance on February 20, 2022. In May 2022, Widgets CEO, Lenny Lion, began discussing the overdue Fish account and possible legal recourse with Widgets CFO, Olivia Owl, and Widgets General Counsel, Teresa Tiger. Outside counsel got involved. As they began preparation for a collections action, counsel requested preparation of a spreadsheet of outstanding amounts, a timeline of events, and a memorandum regarding the availability of liquidated damages. Outside counsel filed suit on June 22, 2022.

The second legal issue reflected in the sample documents arises out of Widgets' supplier Acme's inability to transport shipments of widgets to Widgets' customers due to supply chain issues in spring and early summer 2022. Acme has been unable find truckers willing to drive from Acme's facilities in

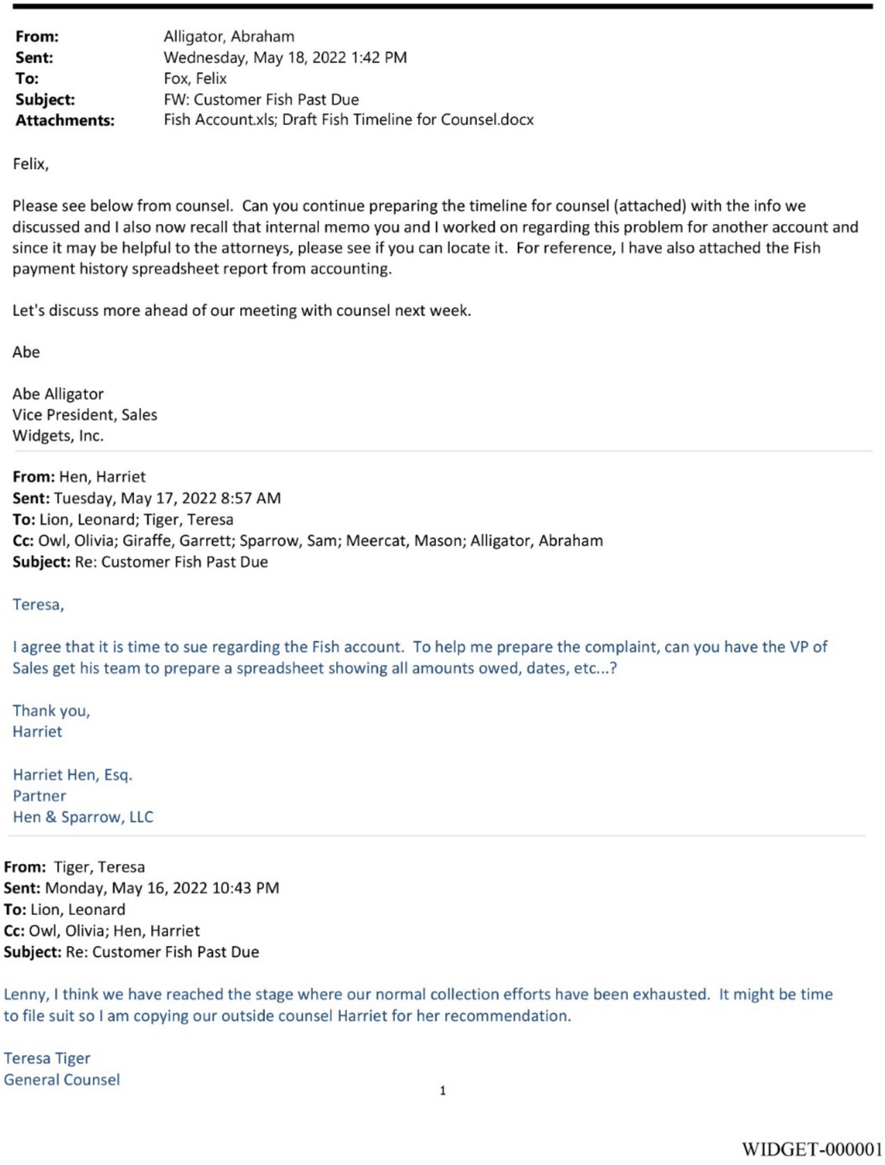
Chicago to the southern parts of the country as gas prices have soared and made it infeasible to transport widgets more than 500 miles. Some customers are threatening to find another supplier of widgets, and Widgets is contemplating legal action against Acme.

See next page for the Cast of Characters and their Roles.

Cast of Characters and Roles

NAME	ROLE
Abe Alligator	VP of Sales
Teresa Tiger	In- House Counsel 1
Olivia Owl	CFO
Lenny Lion	CEO
Harriet Hen	Outside Litigation Counsel 1
Mason Meercat	Paralegal
Sam Sparrow	Outside Litigation Counsel 2
Felix Fox	Sales Assistant
Ray Rhino	VP of Logistics
Penny Penguin	VP of Marketing
Garrett Giraffe	In- House Counsel 2; Board Secretary
[redacted]	
Beatrice Bee	Board Treasurer
Cathy Cat	Board Chair
Dawson Dalmatian	Board Vice Chair
Garrett Giraffe	Board Secretary
[redacted]	
Darryl Dog	Outside Accountant
Frank Fish	Owner of Fish Company, Customer of Widgets, Inc.

See the following pages for the exemplar documents, which form the basis for the entries on the exemplar logs in Appendix A.



From: Alligator, Abraham
Sent: Wednesday, May 18, 2022 1:42 PM
To: Fox, Felix
Subject: FW: Customer Fish Past Due
Attachments: Fish Account.xls; Draft Fish Timeline for Counsel.docx

Felix,

Please see below from counsel. Can you continue preparing the timeline for counsel (attached) with the info we discussed and I also now recall that internal memo you and I worked on regarding this problem for another account and since it may be helpful to the attorneys, please see if you can locate it. For reference, I have also attached the Fish payment history spreadsheet report from accounting.

Let's discuss more ahead of our meeting with counsel next week.

Abe

Abe Alligator
Vice President, Sales
Widgets, Inc.

From: Hen, Harriet
Sent: Tuesday, May 17, 2022 8:57 AM
To: Lion, Leonard; Tiger, Teresa
Cc: Owl, Olivia; Giraffe, Garrett; Sparrow, Sam; Meercat, Mason; Alligator, Abraham
Subject: Re: Customer Fish Past Due

Teresa,

I agree that it is time to sue regarding the Fish account. To help me prepare the complaint, can you have the VP of Sales get his team to prepare a spreadsheet showing all amounts owed, dates, etc...?

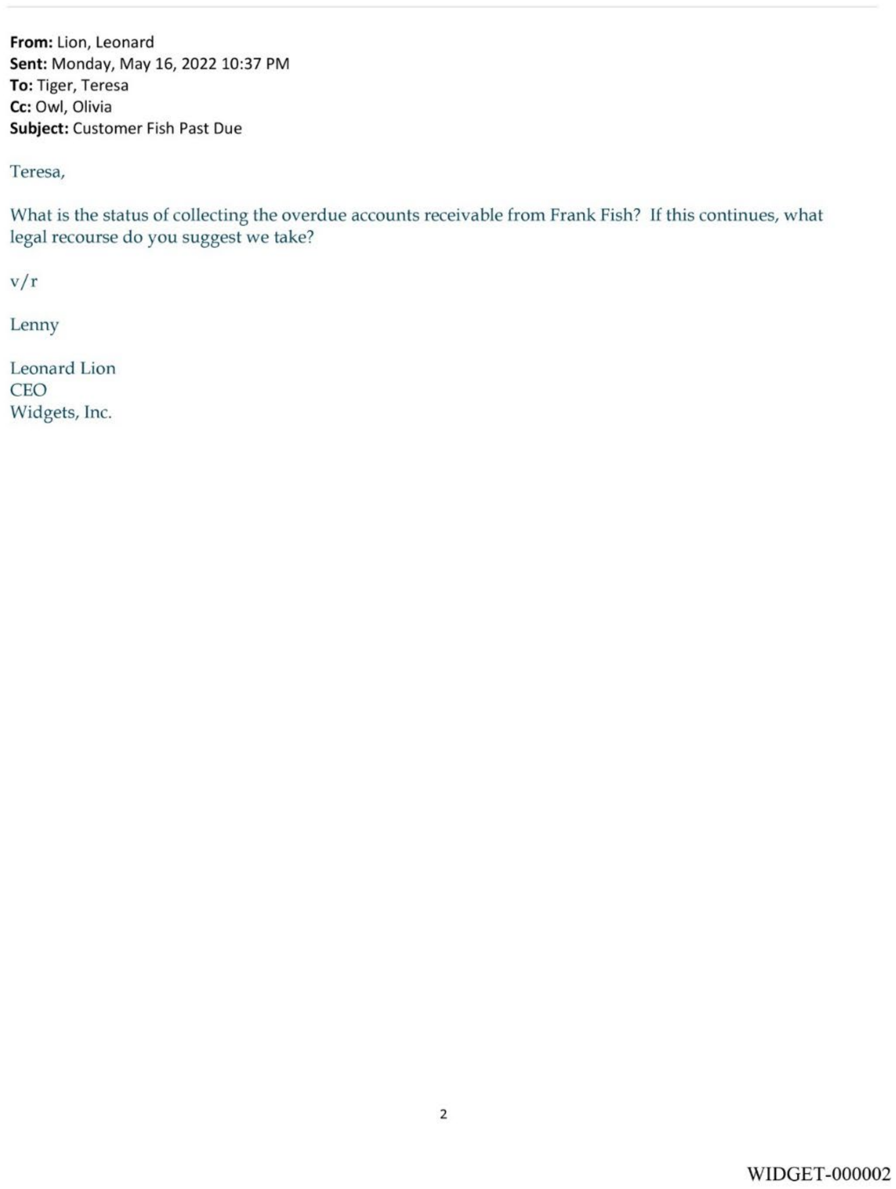
Thank you,
Harriet

Harriet Hen, Esq.
Partner
Hen & Sparrow, LLC

From: Tiger, Teresa
Sent: Monday, May 16, 2022 10:43 PM
To: Lion, Leonard
Cc: Owl, Olivia; Hen, Harriet
Subject: Re: Customer Fish Past Due

Lenny, I think we have reached the stage where our normal collection efforts have been exhausted. It might be time to file suit so I am copying our outside counsel Harriet for her recommendation.

Teresa Tiger
General Counsel



From: Lion, Leonard
Sent: Monday, May 16, 2022 10:37 PM
To: Tiger, Teresa
Cc: Owl, Olivia
Subject: Customer Fish Past Due

Teresa,

What is the status of collecting the overdue accounts receivable from Frank Fish? If this continues, what legal recourse do you suggest we take?

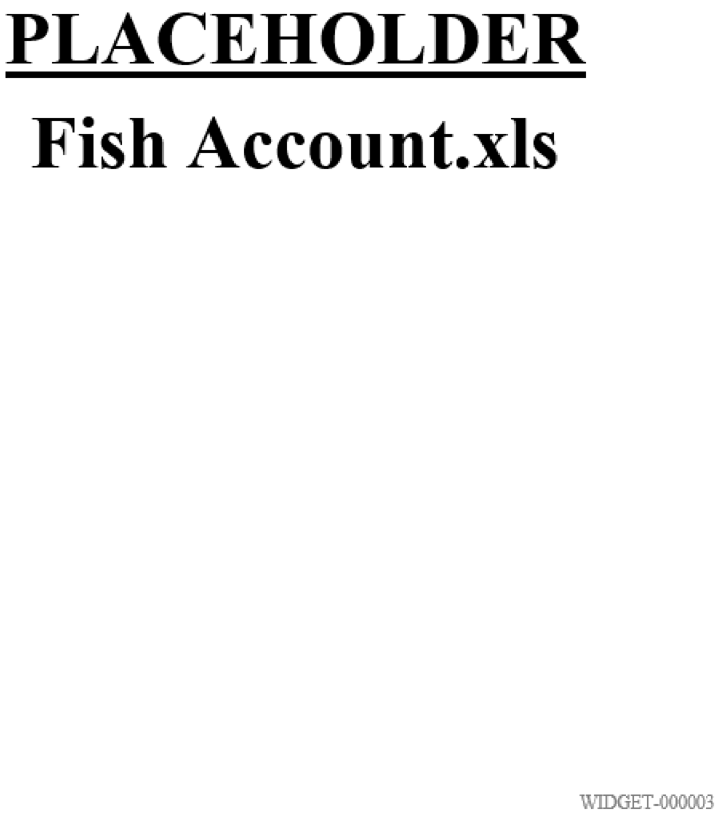
v/r

Lenny

Leonard Lion
CEO
Widgets, Inc.

2

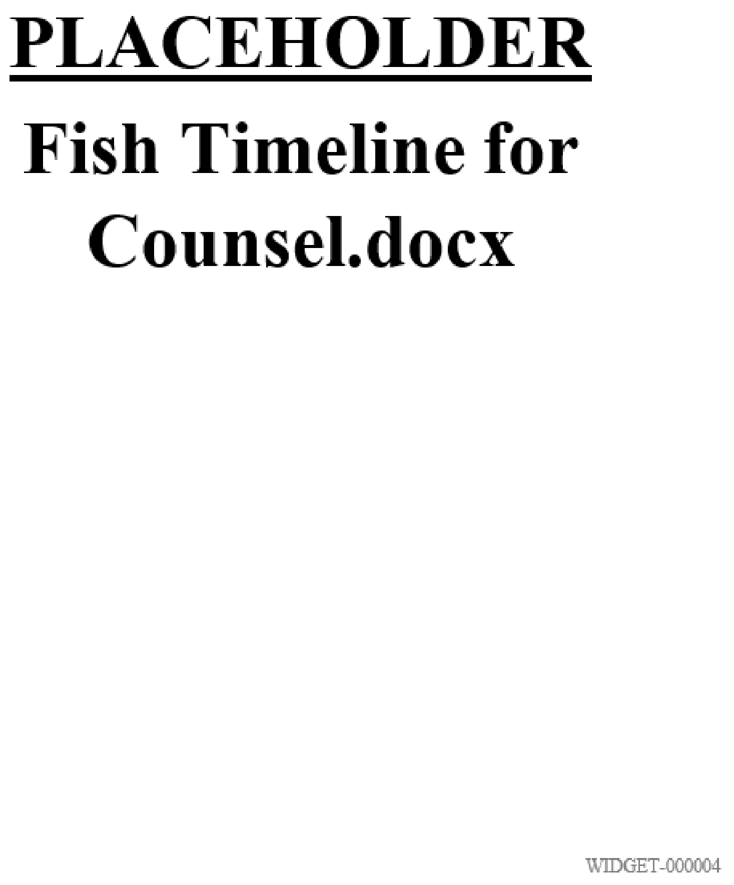
WIDGET-000002



PLACEHOLDER

Fish Account.xls

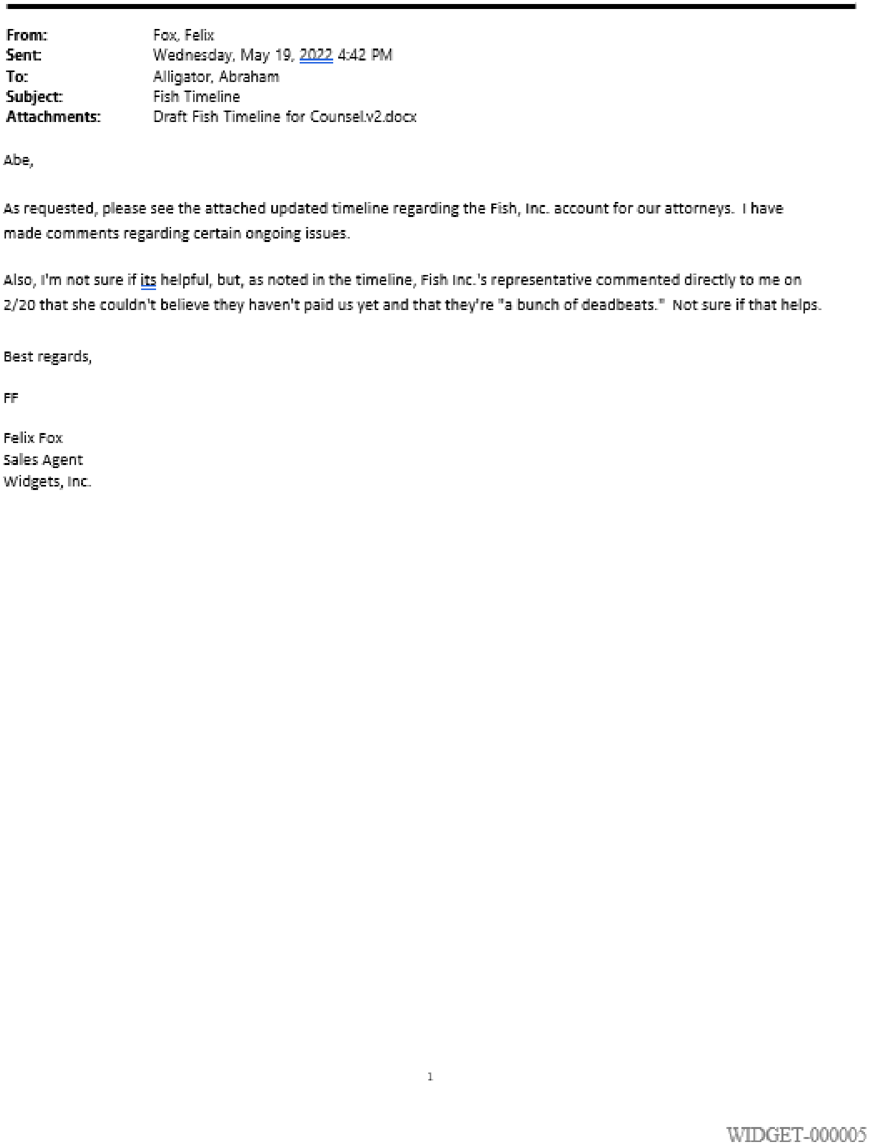
WIDGET-000003



PLACEHOLDER

Fish Timeline for Counsel.docx

WIDGET-000004



From: Fox, Felix
Sent: Wednesday, May 19, 2022 4:42 PM
To: Alligator, Abraham
Subject: Fish Timeline
Attachments: Draft Fish Timeline for Counsel.v2.docx

Abe,

As requested, please see the attached updated timeline regarding the Fish, Inc. account for our attorneys. I have made comments regarding certain ongoing issues.

Also, I'm not sure if its helpful, but, as noted in the timeline, Fish Inc.'s representative commented directly to me on 2/20 that she couldn't believe they haven't paid us yet and that they're "a bunch of deadbeats." Not sure if that helps.

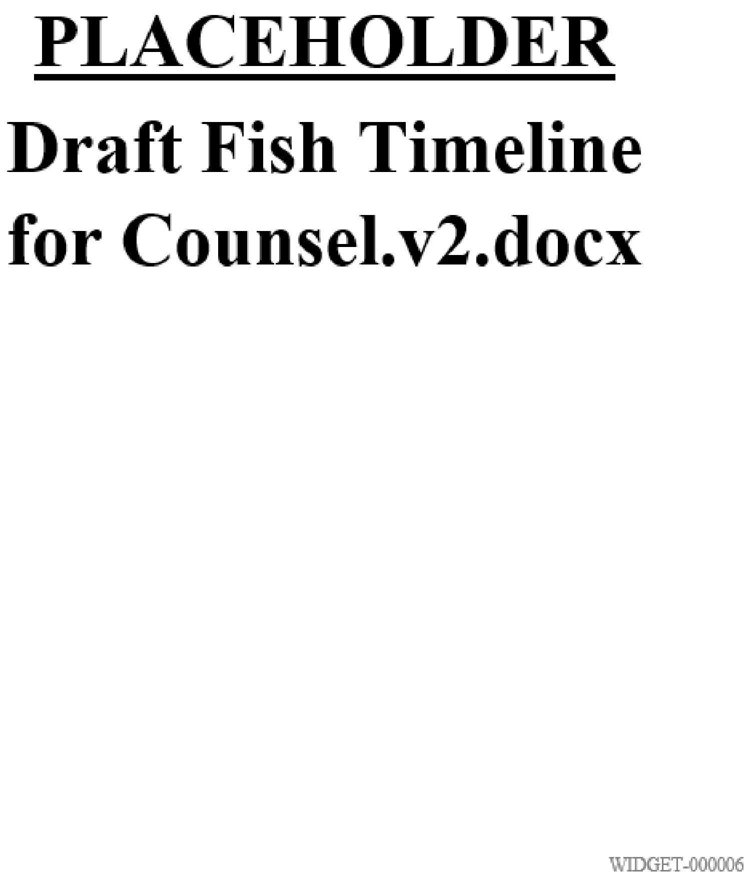
Best regards,

FF

Felix Fox
Sales Agent
Widgets, Inc.

1

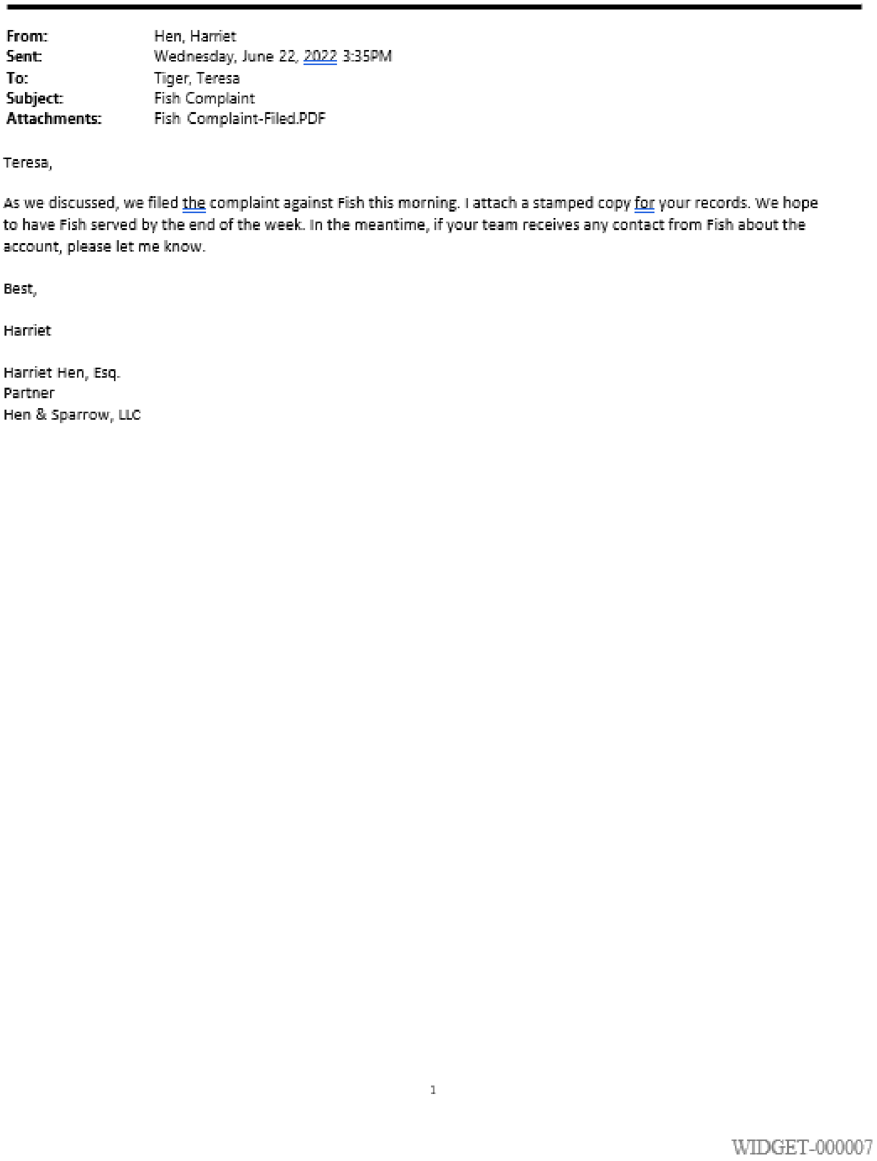
WIDGET-000005



PLACEHOLDER

Draft Fish Timeline for Counsel.v2.docx

WIDGET-000006



From:	Hen, Harriet
Sent:	Wednesday, June 22, 2022 3:35PM
To:	Tiger, Teresa
Subject:	Fish Complaint
Attachments:	Fish Complaint-Filed.PDF

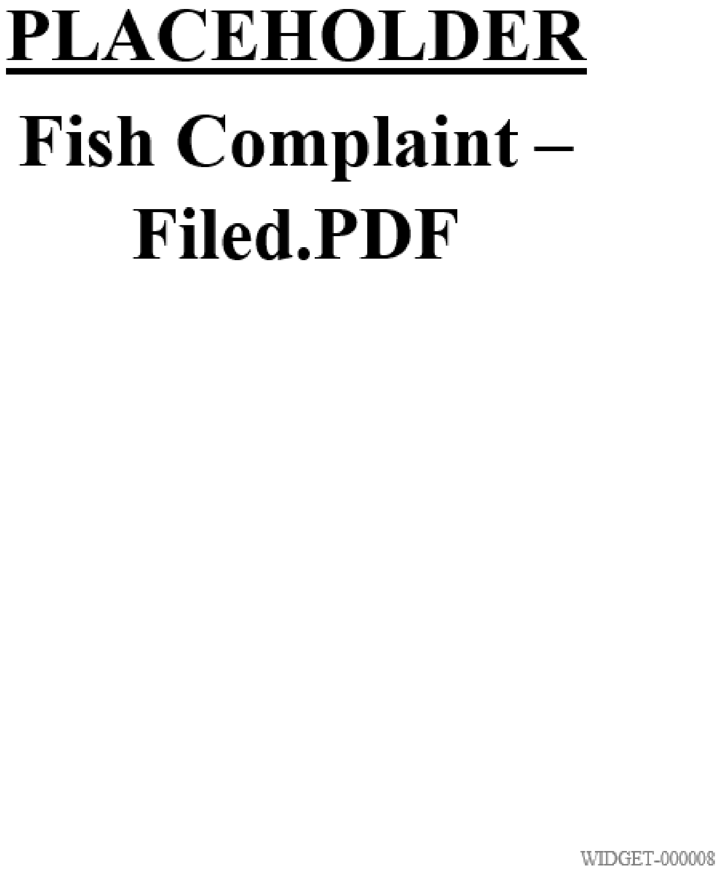
Teresa,

As we discussed, we filed the complaint against Fish this morning. I attach a stamped copy for your records. We hope to have Fish served by the end of the week. In the meantime, if your team receives any contact from Fish about the account, please let me know.

Best,

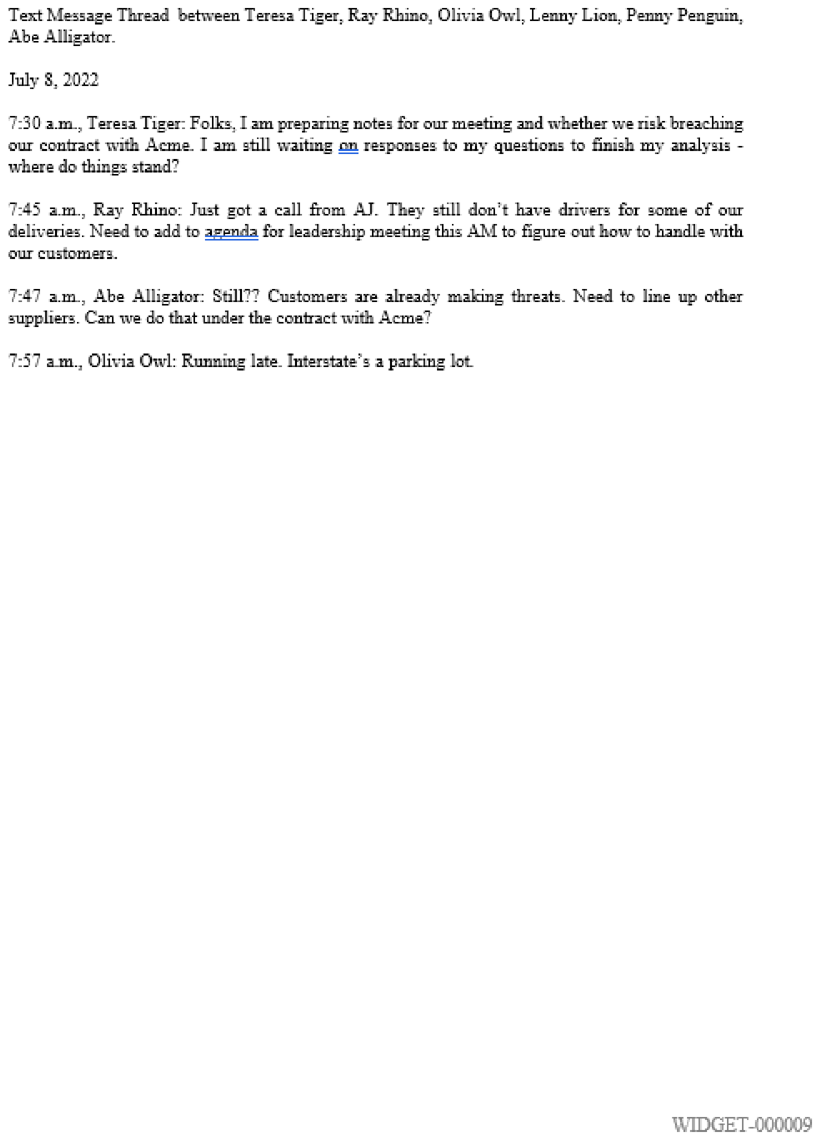
Harriet

Harriet Hen, Esq.
Partner
Hen & Sparrow, LLC



PLACEHOLDER

Fish Complaint – Filed.PDF



Text Message Thread between Teresa Tiger, Ray Rhino, Olivia Owl, Lenny Lion, Penny Penguin, Abe Alligator.

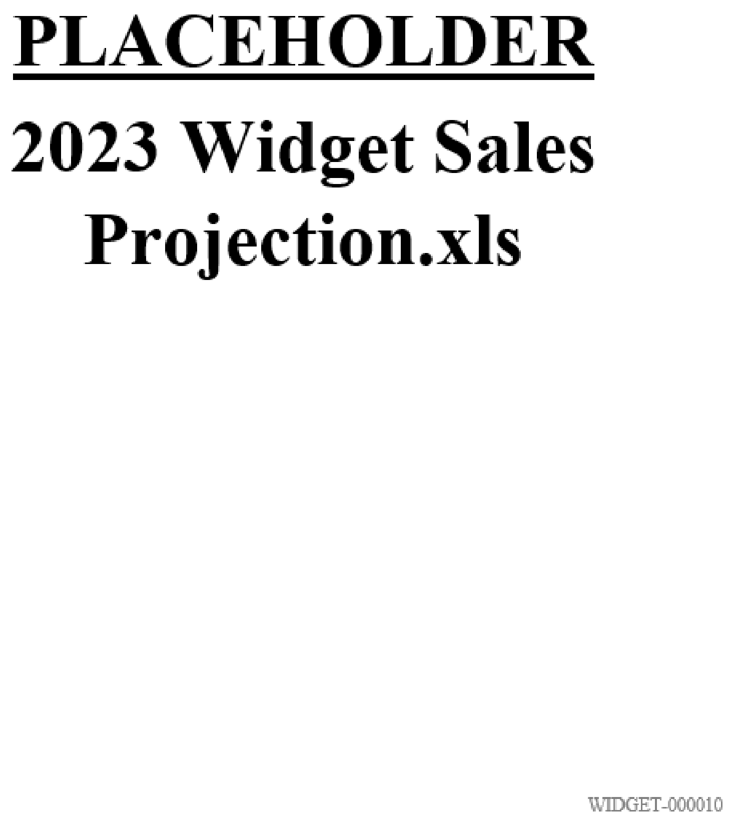
July 8, 2022

7:30 a.m., Teresa Tiger: Folks, I am preparing notes for our meeting and whether we risk breaching our contract with Acme. I am still waiting on responses to my questions to finish my analysis - where do things stand?

7:45 a.m., Ray Rhino: Just got a call from AJ. They still don't have drivers for some of our deliveries. Need to add to agenda for leadership meeting this AM to figure out how to handle with our customers.

7:47 a.m., Abe Alligator: Still?? Customers are already making threats. Need to line up other suppliers. Can we do that under the contract with Acme?

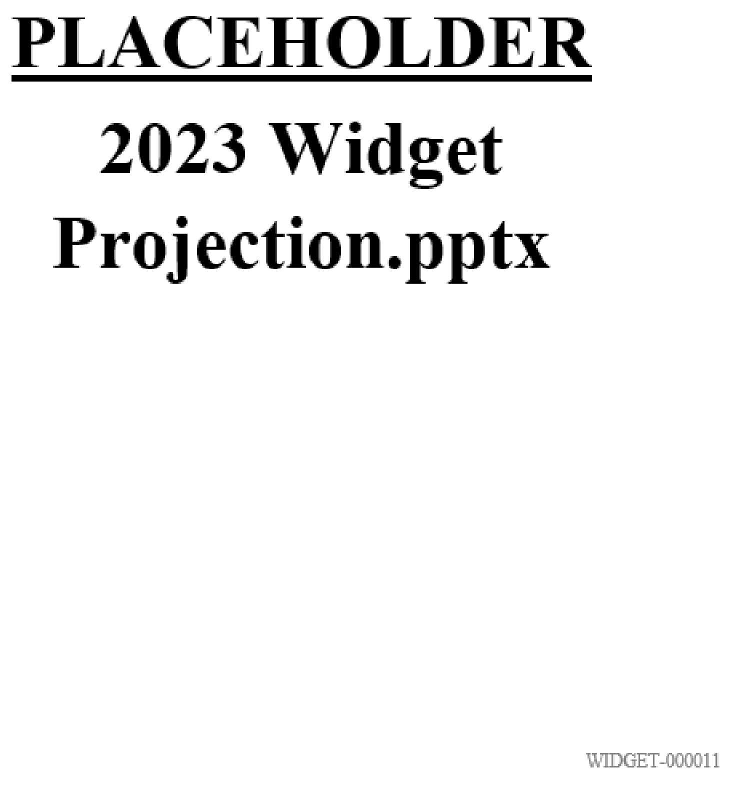
7:57 a.m., Olivia Owl: Running late. Interstate's a parking lot.



PLACEHOLDER

2023 Widget Sales Projection.xls

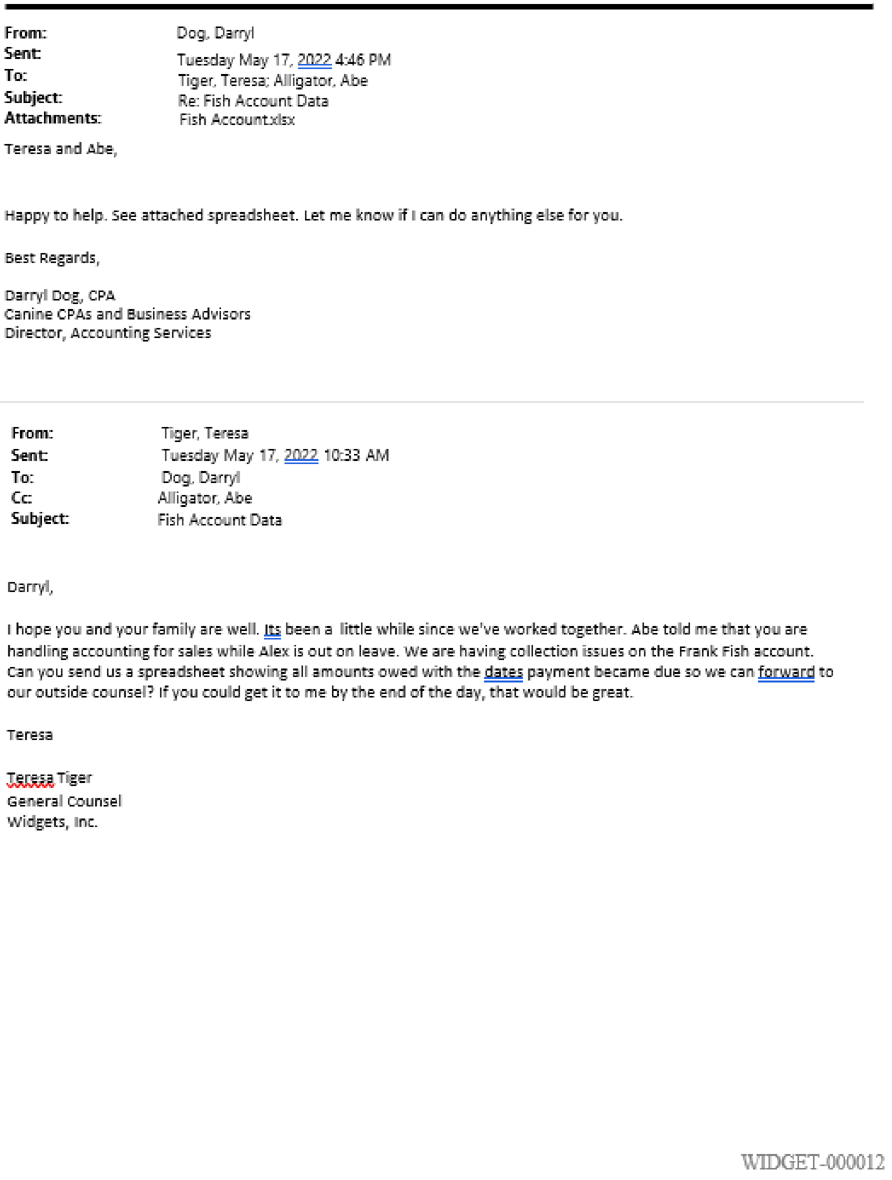
WIDGET-000010



PLACEHOLDER

2023 Widget Projection.pptx

WIDGET-000011



From: Dog, Darryl
Sent: Tuesday May 17, 2022 4:46 PM
To: Tiger, Teresa; Alligator, Abe
Subject: Re: Fish Account Data
Attachments: Fish Account.xlsx

Teresa and Abe,

Happy to help. See attached spreadsheet. Let me know if I can do anything else for you.

Best Regards,

Darryl Dog, CPA
Canine CPAs and Business Advisors
Director, Accounting Services

From: Tiger, Teresa
Sent: Tuesday May 17, 2022 10:33 AM
To: Dog, Darryl
Cc: Alligator, Abe
Subject: Fish Account Data

Darryl,

I hope you and your family are well. Its been a little while since we've worked together. Abe told me that you are handling accounting for sales while Alex is out on leave. We are having collection issues on the Frank Fish account. Can you send us a spreadsheet showing all amounts owed with the dates payment became due so we can forward to our outside counsel? If you could get it to me by the end of the day, that would be great.

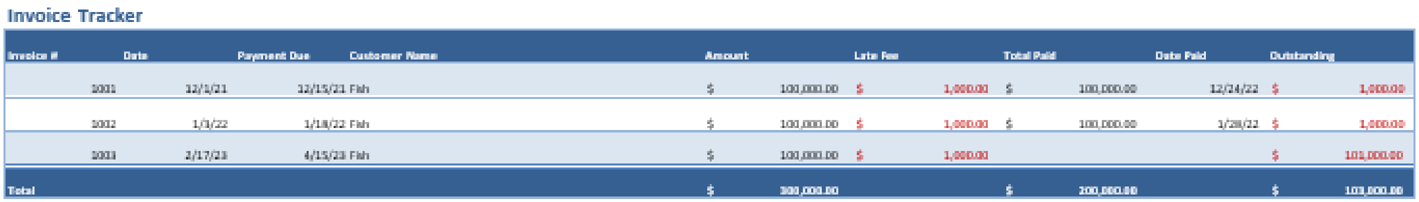
Teresa

Teresa Tiger
General Counsel
Widgets, Inc.

WIDGET-000012

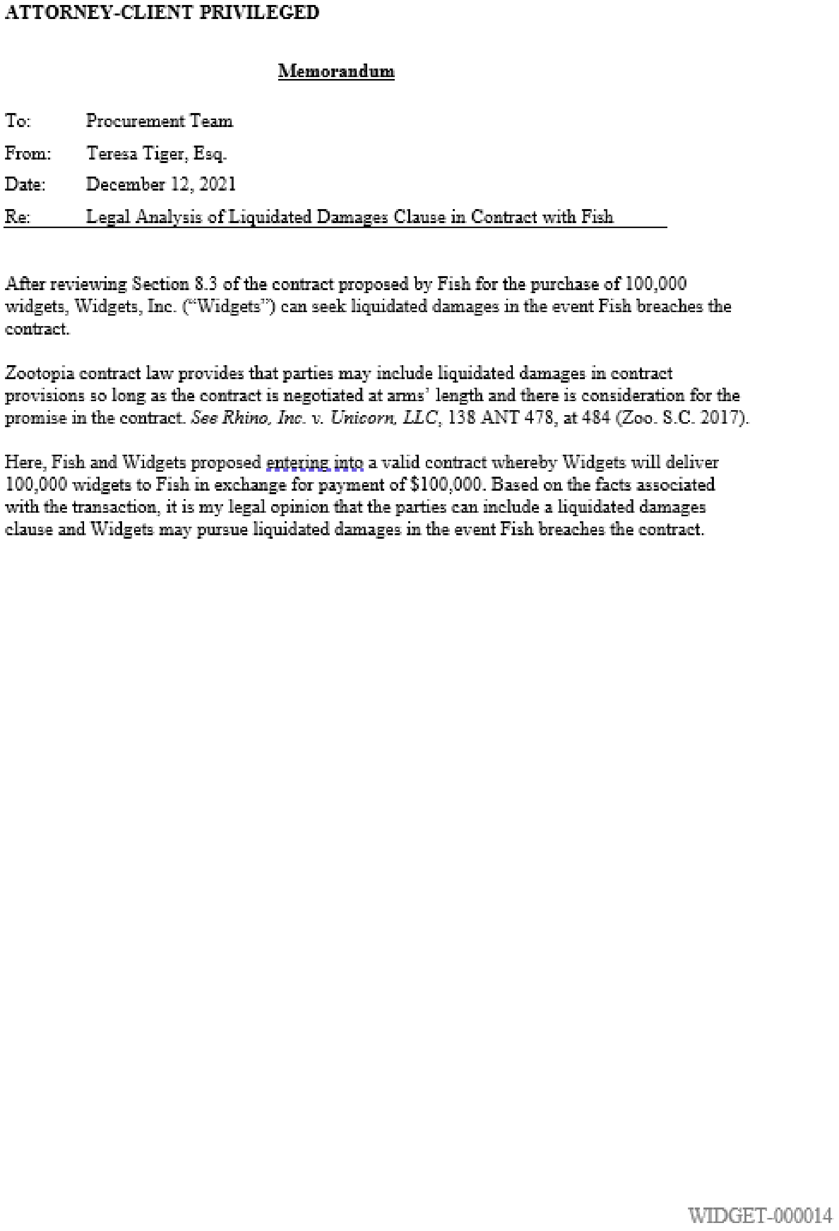
THIS DOCUMENT WAS PRODUCED NATIVELY

WIDGET-000013



Invoice Tracker

Invoice #	Date	Payment Due	Customer Name	Amount	Late Fee	Total Paid	Date Paid	Outstanding
1001	12/1/21	12/15/21	Fish	$ 100,000.00	$ 1,000.00	$ 100,000.00	12/24/22	$ 1,000.00
1002	1/3/22	1/18/22	Fish	$ 100,000.00	$ 1,000.00	$ 100,000.00	1/28/22	$ 1,000.00
1003	2/17/23	4/15/23	Fish	$ 100,000.00	$ 1,000.00			$ 101,000.00
Total				$ 300,000.00		$ 200,000.00		$ 103,000.00



ATTORNEY-CLIENT PRIVILEGED

Memorandum

To: Procurement Team
From: Teresa Tiger, Esq.
Date: December 12, 2021
Re: Legal Analysis of Liquidated Damages Clause in Contract with Fish

After reviewing Section 8.3 of the contract proposed by Fish for the purchase of 100,000 widgets, Widgets, Inc. ("Widgets") can seek liquidated damages in the event Fish breaches the contract.

Zootopia contract law provides that parties may include liquidated damages in contract provisions so long as the contract is negotiated at arms' length and there is consideration for the promise in the contract. *See Rhino, Inc. v. Unicorn, LLC*, 138 ANT 478, at 484 (Zoo. S.C. 2017).

Here, Fish and Widgets proposed entering into a valid contract whereby Widgets will deliver 100,000 widgets to Fish in exchange for payment of $100,000. Based on the facts associated with the transaction, it is my legal opinion that the parties can include a liquidated damages clause and Widgets may pursue liquidated damages in the event Fish breaches the contract.

WIDGET-000014

Evaluating the FTC's Authority to Enforce the GLBA's Provisions Regarding the Security and Privacy of Consumer Financial Information: Lessons from Recent Case Law

Douglas H. Meal and Sharilyn N. Clark[1]

I. Introduction

The Graham-Leach-Bliley Act ("GLBA") has two particular provisions that govern the conduct, in the privacy and cybersecurity context, of "financial institutions" that are subject to the GLBA. Many will be familiar with Section 501(b) of the GLBA[2] ("the GLBA Security Requirement"), which directs various agencies identified in the GLBA to establish "appropriate standards" for the financial institutions subject to their jurisdiction relating to "safeguards" (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. Less well known is Section 521(a) of the GLBA[3] ("the GLBA Pretexting Prohibition"), which protects the privacy of "customer

[1] Mr. Meal is an Adjunct Professor at Cleveland State University College of Law and teaches a course there in Cybersecurity Litigation. Ms. Clark is a 2024 graduate of Cleveland State University College of Law and focused her studies there on privacy and cybersecurity law. The views expressed herein are those of the authors only and are not attributable to the law school with which they are affiliated.

[2] 15 U.S.C. § 6801(b).

[3] 15 U.S.C. § 6821(a).

information of a financial institution" by prohibiting any person from employing a variety of fraudulent practices for the purpose of pretextually obtaining or causing the disclosure of such information.

The GLBA gives the Federal Trade Commission (FTC) certain enforcement authority with regard to both the GLBA Security Requirement (and any rule promulgated by the FTC thereunder) and the GLBA Pretexting Prohibition. As discussed in Part II below, the statutory language that the GLBA uses in conferring that enforcement authority on the FTC is not entirely clear on its face as to the boundaries of and limitations of that authority. Moreover, that statutory language is markedly different as between the GLBA Security Requirement on the one hand and the GLBA Pretexting Prohibition on the other hand. Further, even though GLBA was enacted in 1999, FTC efforts to enforce the GLBA Security Requirement and the GLBA Pretexting Prohibition rarely are litigated, so judicial decisions interpreting the FTC's enforcement authority under those statutes are nearly nonexistent.

Part III below discusses two such judicial decisions, both of which were recently rendered in a case pending before the U.S. District Court for the Southern District of New York. As discussed in Part III.A below, those decisions open the door to a very broad reading of the substantive scope of the GLBA Pretexting Prohibition and the remedies available to the FTC for a violation of that prohibition. We believe that reading is either clearly erroneous or at a minimum highly questionable in a number of respects, as we discuss in Part III.B below. Moreover, as discussed in Part III.C below, the reasoning of those rulings casts doubt on whether the FTC currently has *any* viable remedy available to it—even the ability to obtain a mere cease-and-desist order—for a violation of the GLBA Security Requirement or the so-called "Safeguards Rule" promulgated by the FTC thereunder.

II. THE STATUTORY BASIS FOR FTC ENFORCEMENT OF THE GLBA SECURITY REQUIREMENT AND THE GLBA PRETEXTING PROHIBITION.

A. *FTC Enforcement of the GLBA Security Requirement*

Section 501(a) of the GLBA declares that it is "the policy of the Congress" that "financial institutions" (as defined in the GLBA) have the obligation to "protect the security and confidentiality" of their customers' nonpublic personal information.[4] In furtherance of that policy, the GLBA Security Requirement calls for the various agencies and authorities that have regulatory jurisdiction over financial institutions to establish "appropriate standards" pertaining to administrative, technical, and physical safeguards "(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[5] GLBA Sections 504(a) and 505(a) in turn grant the FTC, among other agencies, rulemaking and enforcement authority, respectively, to carry out the directive of the GLBA Security Rule with respect to those financial institutions that are subject to the FTC's regulatory authority.[6] Specifically, Section 504(a) grants the FTC

[4] 15 U.S.C. § 6801(a).

[5] 15 U.S.C. § 6801(b).

[6] Per GLBA Section 505(a)(7), the FTC's regulatory authority extends to any financial institution "that is not subject to the jurisdiction of any [other] agency or authority" listed in Section 505(a)(1)-(6). 15 U.S.C. § 6805(a)(7). According to the FTC, those financial institutions "include, but are not limited to, mortgage lenders, 'pay day' lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally

authority to create "regulations as may be necessary" to carry out that directive, and Section 505(a)(7) of the GLBA provides that the GLBA Security Requirement and the rules enacted by the FTC thereunder may be enforced against those financial institutions by the FTC "[u]nder the Federal Trade Commission Act" ("FTC Act").[7]

The FTC complied with the rulemaking authority granted to it in the GLBA by creating what has come to be called the "Safeguards Rule."[8] The Safeguards Rule requires those institutions within the FTC's jurisdiction to "develop, implement, and maintain a [written] comprehensive information security program" that is "reasonably designed" to meet the three objectives specified in the GLBA Security Requirement and that, in addition, includes certain elements specified in Section 314.4 of the Safeguards Rule.[9]

Importantly, as will be discussed in Part III.C below, the Safeguards Rule was not enacted by the FTC pursuant to its rulemaking authority under Section 18 of the FTC Act, which allows the FTC to enact so-called "trade regulation rules"[10], i.e., "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or

insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders." 16 C.F.R. § 314.1(b).

[7] 15 U.S.C. § 6804(a) & 6805(a)(7).

[8] The Safeguards Rule is codified at 16 CFR Part 314.

[9] 16 C.F.R § 314.3.

[10] *See* The Federal Trade Commission, A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority, Part III (revised May 2021), *available at* https://www.ftc.gov/about-ftc/mission/enforcement-authority (defining "trade regulation rules" as being "''rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce'' within the meaning of Section 5(a)(1) of the [FTC] Act" (quoting FTC Act Section 5(a)(1))).

affecting commerce (within the meaning of [FTC Act Section 5(a)]."[11] Instead, the FTC relied solely on its rulemaking authority under the GLBA in enacting the Safeguards Rule.[12] Additionally, nothing in the Safeguards Rule purports to provide that a violation of the Safeguards Rule constitutes a violation of Section 5(a) of the FTC Act or purports to require the elements of a Section 5(a) violation to be established to prove a violation of the Safeguards Rule.

B. FTC Enforcement of the GLBA Pretexting Prohibition

The GLBA Pretexting Prohibition prohibits any person from attempting to obtain or obtaining, or causing or attempting to cause to be disclosed to any person, "customer information of a financial institution" relating to another person by (1) making a "false, fictitious, or fraudulent statement or representation" to an employee of a financial institution, (2) making such a statement or representation to a customer of a financial institution, or (3) providing any document to any employee of a financial institution, knowing the document was forged, counterfeit, lost, or stolen, was fraudulently obtained, or contains a false statement.[13] Section 522(a) of the GLBA gives the FTC jurisdiction to enforce the GLBA Pretexting Prohibition against pretty much the same group of "financial institutions" over which the FTC has enforcement authority with respect to the GLBA Security Requirement.[14] But instead of granting the FTC authority to

[11] 15 U.S.C. § 57(a)(1)(B).

[12] *See* "Authority," 26 C.F.R. Part 314 (only specifying GLBA Sections 501(b) and 505(b)(2) as the authority for the Safeguards Rule's enactment).

[13] 15 U.S.C. § 6822(a).

[14] *Compare* 15 U.S.C § 6822(b) (identifying which financial institutions are carved out from the FTC's GLBA Pretexting Prohibition enforcement jurisdiction) *with* 15 U.S.C. § 6805(a)(1)-(6) (identifying which financial

enforce the GLBA Pretexting Prohibition against those financial institutions "under the [FTC] Act" (as the GLBA had done with respect to the GLBA Security Requirement), GLBA Section 522(a) grants the FTC power to enforce the GLBA Pretexting Prohibition "with the same power and authority as the Commission has under the Fair Debt Collection Practices Act" ("FDCPA").[15] The difference in language is significant, as the FTC has broad enforcement authority under the FDCPA. Specifically, Section 814(a) of the FDCPA provides that, for purposes of the FTC's authority to enforce compliance with the FDCPA, a violation of the FDCPA shall be deemed "an unfair or deceptive act or practice" in violation of Section 5(a) of the FTC Act; "[a]ll of the functions and powers" of the FTC are available to enforce such compliance; and the FTC is entitled to treat any FDCPA violation "in the same manner as if the violation had been a violation of a [FTC] trade regulation rule."[16]

III. THE RECENT RULINGS IN *FTC V. RCG ADVANCES*

A. The District Court's Interpretation and Application of the GLBA Pretexting Prohibition in RCG Advances

In the first 20 years following the GLBA's enactment in 1999, the FTC rarely exercised its enforcement power with respect to the GLBA Pretexting Prohibition.[17] Indeed, we have found no case prior to 2020 in which the FTC's enforcement authority

institutions are carved out from the FTC's GLBA Security Requirement enforcement jurisdiction).

[15] 15 U.S.C. § 6822(a).

[16] 15 U.S.C. § 1692*l*(a).

[17] The most recent FTC settlement that we found where a claim was made under the GLBA Pretexting Prohibition was the Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief in *FTC v. Sun Spectrum Communications Organization, Inc.*, No. 03-81105-CIV-COHN/SNOW (S.D. Fla. filed Oct. 3, 2005).

under the GLBA Pretexting Prohibition was actually litigated. Things changed in 2021, however, when the FTC filed an amended complaint in *FTC v. RCG Advances* ("*RCG Advances*") in which the FTC asserted that the defendants had violated not only Section 5(a) of the FTC Act (as had been alleged in the FTC's original 2020 complaint), but also the GLBA Pretexting Prohibition.[18] The FTC's GLBA Pretexting Prohibition claim in *RCG Advances* has been addressed at length in two rulings recently rendered by the district court: first, in a September 2023 ruling on the FTC's summary judgment motion;[19] and second in a post-trial ruling rendered in February 2024.[20] As discussed below, by means of those two rulings the district court addressed numerous questions of first impression regarding the FTC's GLBA Pretexting Prohibition enforcement authority.

RCG Advances, LLC ("RCG") was in the business of entering into "merchant cash advance agreements" ("MCA Agreements") with merchants pursuant to which RCG loaned a lump sum of cash to a customer; in exchange, the customer assigned its future receivables to RCG until RCG collected an agreed-upon amount.[21] Specifically, the MCA Agreements contemplated that RCG would make an initial deposit of the loan amount directly into its customers' bank accounts and thereafter make daily debits of a specified amount directly from its customers' bank accounts until RCG recouped the entire amount that it was owed.[22] In order to accomplish this, the MCA

[18] *See* Amended Complaint, FTC v. RCG Advances, LLC, No. 20-cv-4432 (JSR), Count Five (S.D.N.Y., filed June 10, 2021).

[19] FTC v. RCG Advances, LLC (*SJ Ruling*), No. 20-cv-4432 (JSR), 2023 WL 6281138 (S.D.N.Y., Sept. 27, 2023).

[20] FTC v. Braun (*PT Ruling*), No. 20-cv-4432 (JSR), 2024 WL 449288 (S.D.N.Y., Feb. 6, 2024).

[21] *SJ Ruling* at *1.

[22] *Id.*

Agreements provided that customers would agree to permit direct debits from and credits to their bank accounts and give RCG information about their bank accounts necessary to implement such debits and credits.[23]

In *RCG Advances*, the FTC alleged that RCG and the other defendants (including an RCG "owner, officer, and manager" named Jonathan Braun) had defrauded RCG's customers by lying about terms of the advances, including the amount of money they would be loaned, the amount to be collected, and other material terms.[24] The FTC further alleged that the defendants intimidated the business owners by making violent threats when it was time to collect on the payments.[25] The FTC's amended complaint made five claims against the defendants. In Counts One through Four, the FTC claimed that the defendants had violated Section 5(a) of the FTC Act by (1) making false and misleading statements that qualify as deceptive acts or practices; (2) misusing Confessions of Judgment; (3) threatening customers to induce them to make payments; and (4) making unauthorized withdrawals from customers' bank accounts.[26] In Count Five, the FTC claimed that the defendants had violated the GLBA Pretexting Prohibition by making false statements to obtain customers' bank account information and then using that information to overdebit and undercredit funds from those customers' accounts.[27] The relief sought by the FTC under the GLBA Pretexting Prohibition claim included a permanent injunction, civil penalties, and monetary redress for RCG's

[23] *Id*.

[24] *Id*.

[25] *Id*.

[26] *Id*. at *2.

[27] *Id*.

customers in the amounts by which they were overdebited or undercredited.[28]

In ruling on the FTC's motion for summary judgment on its GLBA Pretexting Prohibition claim, the district court agreed that RCG had violated the GLBA Pretexting Prohibition. As noted above, the GLBA Pretexting Prohibition prohibits persons from obtaining or attempting to obtain or cause to be disclosed to any person, "customer information of a financial institution" relating to another person by making a "false, fictitious, or fraudulent statement or representation" to a customer of a financial institution.[29] The FTC alleged that by making false representations about the MCA Agreements to obtain customers' bank account information, the defendants violated the GLBA Pretexting Prohibition.[30] The district court found that RCG had a "practice" of breaching the MCA Agreements' covenants regarding the debiting and crediting of its customers' accounts.[31] Given this practice, the district court found that RCG had indeed made false representations about the MCA Agreements by inaccurately specifying (1) the amount of funding that would be provided and (2) the repayment amount that would be collected from its customers.[32] The district court further found that those misrepresentations were enough to induce customers into signing the MCA Agreements and granting RCG access to their bank account information.[33] Based on these findings, the district court ruled that RCG had made "false, fictitious, or fraudulent"

[28] *Id*.

[29] 15 U.S.C. § 6821(a)(2).

[30] *SJ Ruling*, 2023 WL 6281138 (S.D.N.Y., Sept. 27, 2023), at *9.

[31] *Id*. at *5; see also *id.* at *2 (defendants "regularly failed to adhere to the contractual terms of the MCA Agreements").

[32] *Id.* at *9–10.

[33] *Id*. at *10.

representations to its customers for purposes of obtaining "customer information of a financial institution" relating to those customers, in violation of the GLBA Pretexting Prohibition.[34]

The district court's summary judgment ruling further found that Braun was individually liable for RCG's violation of the GLBA Pretexting Prohibition. The district court first ruled that the standard for assessing individual liability under the GLBA, at least in the context of a GLBA claim brought by the FTC, was the same standard that applies to assessing individual liability under the FTC Act.[35] The district court next held that, under the FTC Act standard for assessing individual liability, Braun was individually liable for RCG's GLBA Pretexting Prohibition violation.[36]

The district court then turned to the remedies sought by the FTC by reason of Braun's GLBA Pretexting Prohibition violation. Regarding the FTC's requests for compensatory damages and civil penalties, the FTC argued, and the district court agreed, that by virtue of GLBA Section 522(b)'s grant of enforcement authority under the GLBA Pretexting Prohibition analogous and equivalent to the FTC's enforcement authority in the FDCPA, the FTC had the authority to enforce against Braun's GLBA Pretexting Prohibition violation in the same manner as if the violation has been a violation of an FTC trade regulation rule.[37] The district court further held that, because the language of the GLBA allows the FTC such enforcement authority, the FTC had the right to seek both consumer redress under Section 19(a)(1) of the FTC Act and civil penalties under Section 5(m)(1)(A) of the FTC Act as remedies for Braun's GLBA

[34] *Id*.

[35] *Id*.

[36] *Id*.

[37] *Id*. at *11.

Pretexting Prohibition violation, because both those provisions make relief available where there has been a violation of one of the FTC's trade regulation rules.[38] However, the district court declined to award summary judgment in the FTC's favor as to either of these requested remedies, finding that material issues of fact existed as to the amount of consumer redress that should be awarded under FTC Act Section 19(a)(1) and as to whether Braun acted knowingly, as required for a penalty to be imposable under FTC Act Section 5(m)(1)(A).[39]

The district court did, however, award summary judgment in the FTC's favor on its request for entry of a permanent injunction against Braun as a remedy for his GLBA Pretexting Prohibition violation. The district court ruled that Section 13(b) of the FTC Act authorizes a permanent injunction as a remedy for a violation "of any provision of law enforced by the [FTC],"[40] when "there exists some cognizable danger of recurrent violation"[41] "or some reasonable likelihood of future violations."[42] Applying that standard to Braun, the district court "ha[d] no trouble finding a permanent injunction prohibiting Mr. Braun from making merchant cash advances or participating in debt collection activities (as defined the FTC's proposed order) to be appropriate."[43] The district court also found appropriate a permanent injunction requiring Braun to refrain from illegal

[38] *Id*. at *11, 13.

[39] *Id*. at *11–13.

[40] *See* 15 U.S.C. § 53(b).

[41] *SJ Ruling*, 2023 WL 6281138 (S.D.N.Y., Sept. 27, 2023), at *14 (quoting United States v. W.T. Grant Co., 345 U.S. 62 9, 633 (1953)).

[42] *SJ Ruling*, 2023 WL 6281138 at *14 (quoting FTC v. Minuteman Press, 53 F. Supp. 2d 248, 260 (E.D.N.Y. 1998)).

[43] *SJ Ruling*, 2023 WL 6281138 at *14.

conduct and to request removal of negative credit reports issued against customers.[44]

In February 2024, subsequent to the district court's summary judgment ruling, the case went to trial. Following the trial, the district court issued the post-trial ruling, which addressed the three issues that the summary judgment ruling had left open regarding the relief to be awarded for Braun's violation of the GLBA Pretexting Prohibition: (1) what amount of money should be awarded under Section 19(a)(1) of the FTC Act for consumer redress, (2) whether Braun acted "knowingly" when violating GLBA Section 521(a), as required for a civil penalty to be imposable by reason of that violation under FTC Act Section 5(m)(1)(A), and (3) if Braun did act knowingly, what amount of civil penalties should be imposed under Section 5(m)(1)(A).[45] As to the first question, the district court concluded that the FTC's trial evidence "reasonably approximated the defendants' unjust gains" and accordingly held that Braun was liable for $3,421,067 under Section 19(a)(1) of the FTC Act to redress the harm to individual consumers caused by the amounts the defendants' "over-collected or underfunded" pursuant to the MCA Agreements.[46] As to the second question, the jury in the trial had concluded that Braun acted "with actual knowledge or knowledge fairly implied on the basis of objective circumstances" when violating the GLBA Pretexting Prohibition, and the district court concluded it was bound by that conclusion.[47] As to the third question, the district court held that (a) because Braun exercised "considerable control and authority" over RCG, gained "substantial money" from his work, and showed "utter disregard

[44] *Id*.

[45] *PT Ruling*, 2024 WL 449288 (S.D.N.Y., Feb. 6, 2024) at *1.

[46] *Id*. at *8–10.

[47] *Id*. at *1 & *10.

and contempt" for consumers, the civil penalty amount should be calculated at $18,000 per violation, against a maximum per-violation penalty of either $50,120 or $51,744[48]; (b) Braun had violated the GLBA Pretexting Prohibition 942 times, because RCG overcollected on 396 and underfunded on 546 of the MCA Agreements; and (c) the FTC was therefore entitled to a total civil penalty award of $16,956,000 ($18,000 multiplied by 942).[49]

B. *Analysis of the District Court's Interpretation and Application of the GLBA Pretexting Prohibition in RCG Advances*

RCG Advances appears to be the first litigated case brought by the FTC to enforce the GLBA Pretexting Prohibition. For this reason alone, the district court's rulings in *RCG Advances* are groundbreaking and warrant significant attention. Moreover, those rulings address numerous questions of first impression as to the interpretation and application of the GLBA Pretexting Prohibition. For example, *RCG Advances* addresses not just the showing the FTC must make to establish a *corporate* violation of the GLBA Pretexting Prohibition, but also what showing is required to hold a person *individually* liable for such a corporate violation. Further, *RCG Advances* addresses what showing must be made to entitle the FTC to remedy either a corporate or an individual violation of the GLBA Pretexting Prohibition by an award of (1) compensatory damages to any consumers injured by the violation; (2) civil monetary penalties; and/or (3) a permanent injunction.

RCG Advances therefore stands to become a veritable road map for both the FTC and any future defendant in any future FTC enforcement action under the GLBA Pretexting

[48] The parties disputed the applicable maximum amount, and the district court found it unnecessary to resolve that dispute. *Id.* at *11 n.9.

[49] *Id.* at *10–11.

Prohibition. In an effort to assist future litigants and courts in following (or not) the GLBA Pretexting Prohibition roadmap created by *RCG Advances*, we set forth below our analysis of each component of the district court's rulings with respect to the theories of corporate liability, individual liability, and relief advanced by the FTC under the GLBA Pretexting Prohibition.[50]

Corporate Liability. As noted in Part III.A *supra*, in *RCG Advances* the district court found a violation of the GLBA Pretexting Prohibition based on RCG's contractual promise to its customers that it "would collect a specified amount from customers and customers would receive a specified lumpsum amount upfront," a promise that RCG had a "practice" of breaching. In reaching this conclusion, the district court reasoned as follows:

1. RCG made the promise in question in order to obtain from RCG's customers their bank account information so as to enable RCG to make deposits into and withdrawals from those customers' bank accounts, information that constituted "customer information of a financial institution" within the meaning of the GLBA Pretexting Prohibition.
2. RCG had no intention of performing that promise at the time it was made, making the promise not merely a contractual obligation to a customer of a financial institution,

[50] As will be seen, we take issue with a number of aspects of the district court's rulings in *RCG Advances*. In so doing, we intend no disrespect whatsoever for the district court. In nearly every aspect of our disagreement with the district court's rulings, the district court was either (1) led into error by the FTC's erroneous assertions as to the scope of its enforcement authority or (2) never faced with an objection by the defendant as to the FTC's erroneously asserted position or (3) both. We therefore offer our conclusions regarding the district court's rulings in *RCG Advances* not as a criticism of the district court but rather to assist future litigants on both sides of the "v." in preventing future courts from committing similar errors.

but a "false, fictitious, or fraudulent statement or representation to a customer of a financial institution" within the meaning of the GLBA Pretexting Prohibition.

3. The RCG promise therefore violated the GLBA Pretexting Prohibition, (a) first because the statute by its express terms extends to *any* "false, fictitious, or fraudulent statement or representation" that (as was the case here) otherwise satisfies the language of GLBA Section 521(a), and (b) second because the statute at a bare minimum extends to a statement or representation that (as was the case here) independently constitutes a "deceptive" act or practice prohibited by FTC Act Section 5(a) and otherwise satisfies the language of GLBA Section 521(a).[51]

The district court's reasoning in points 1 and 3(a) above was sound given the language of the GLBA Pretexting Prohibition itself. Moreover, its reasoning in point 2 above likewise appears to have been sound given the defendant's apparent concession that RCG had no intention of performing the promise at the time it was made.[52] But the district court's reasoning in point 3(b)

[51] *See SJ Ruling*, 2023 WL 6281138 (S.D.N.Y., Sept. 27, 2023), at *9–10.

[52] *See id*. at *9 (noting defendant's argument that "never having the intent to perform contractual obligations is different in kind from the false statements the GLB Act was intended to reach"). At least in some jurisdictions, a promise to perform a contractual obligation may be fraudulent if "the promisor had no intention to perform at the time the promise was made." *See, e.g.*, Martens v. Minn. Mining & Mfg. Co., 616 N.W.2d 732, 747 (Minn. 2000). Holdings of this sort support the district court's apparent theory that proof of an intent not to perform a contractual promise can make the promise a "false, fictitious, or fraudulent statement or representation" within the meaning of the GLBA Pretexting Prohibition. The actual evidence that the district court presented as to RCG's alleged intent not to perform was not particularly compelling, however, as that evidence indicated that as to most customers RCG actually *did not* follow its alleged "practice" of breaching the promise in question and, instead, fully complied with that promise. *See SJ Ruling*, 2023 WL 6281138 at *11 (noting that the FTC had presented evidence that

above, whereby the district court offered an alternative, fallback ground for its finding of a violation of the GLBA Pretexting Prohibition, does not withstand scrutiny. Statements do not need to be "false, fictitious, or fraudulent" to violate Section 5(a)'s prohibition on deceptive acts and practices; rather, they need only be materially misleading. Thus, statements that are literally true can violate Section 5(a)'s deception prong where they are misleading by implication or omission, but such statements could never be "false, fictitious, or fraudulent" within the meaning of the GLBA Pretexting Prohibition. Also, to prevail on a claim under Section 5(a)'s deception prong the FTC need not prove that the defendant's materially misleading statements were made with an intent to defraud or deceive or were made in bad faith,[53] but such proof might well be required to establish a "false, fictitious, or fraudulent" statement or representation within the meaning of the GLBA Pretexting Prohibition. The district court therefore erred in defending its finding of GLBA Pretexting Prohibition liability on the fallback theory that the GLBA Pretexting Prohibition's requirement of a "false, fictitious, or fraudulent" statement or representation "certainly reaches statements that would be independently violative of Section 5 of the FTCA."[54]

only 26.4% of RCG's customers were overcharged at least once, and only 36.4% had fees "over-deducted" (and thus had their accounts undercredited) at least once, over a five-year period). But in opposing summary judgment, the defendant did not contest RCG's alleged intent not to perform, so the district court seems to have taken that particular point as having been conceded.

[53] *See* FTC v. Moses, 913 F.3d 297, 306 (2d Cir. 2019); FTC v. LeadClick Media, LLC, 838 F.3d 158, 168 (2d Cir. 2016) ("[I]t is enough that the representations or practices were likely to mislead consumers acting reasonably.") (internal quotation and citation omitted); FTC v. Five-Star Auto Club, 97 F. Supp. 2d 502, 526 (S.D.N.Y. 2000) ("It is not necessary to prove Defendants' misrepresentations were made with an intent to defraud or deceive, or were made in bad faith to establish a Section 5 violation.").

[54] *See SJ Ruling*, 2023 WL 6281138 at *10.

Individual Liability. As discussed in Part III.A above, the district court's ruling in *RCG Advances* that Braun was individually liable for RCG's violation of the GLBA Pretexting Prohibition rested on the district court's conclusion that the standard for assessing individual liability under the GLBA, at least in the context of a GLBA claim brought by the FTC, is the same standard that applies to assessing individual liability under the FTC Act.[55] The district court arrived at this conclusion based on *FTC v. Moses*,[56] which held that the standard for assessing individual liability under the FDCPA, at least in the context of a FDCPA claim brought by the FTC, is the same standard that applies to assessing individual liability under the FTC Act.[57] In so holding, the Second Circuit reasoned that because FDCPA violations are statutorily deemed to be violations of Section 5(a) of the FTC Act and to be subject to enforcement in the same manner as if they had been violations of an FTC trade regulation rule, "it follows, we conclude, that the FTCA individual liability standard applies" to claims of individual FDCPA liability asserted by the FTC.[58] In *RCG Advances*, the district court concluded that the "logic [of *Moses*] demands that the same result obtain here" and accordingly carried that "logic" over to the GLBA Pretexting Prohibition by applying the FTC Act's individual liability standard to the FTC's claim that Braun was individually liable for RCG's violation of GLBA Section 521(a).[59] We agree that if *Moses* were logical, its logic would apply equally in the context of an FTC claim under the GLBA Pretexting Prohibition, but we

[55] *Id*. at *10.

[56] 913 F.3d 297 (2d Cir. 2019).

[57] *Id*. at 307.

[58] *Id*.

[59] *SJ Ruling*, 2023 WL 6281138 at *10. The district court's ruling on this point was recently followed in *FTC v. Celsius Network Inc.*, 2023 WL 8603064, *5 (S.D.N.Y. Dec. 12, 2023).

disagree with the supposed "logic" of *Moses*. Just because a violation of the FDCPA or the GLBA Pretexting Prohibition can be *enforced against* by the FTC as if it were a violation of Section 5(a) of the FTC Act and/or an FTC trade regulation rule does not mean, logically or otherwise, that the FTC Act must be used to determine whether a violation of the FDCPA or the GLBA Pretexting Prohibition *can be found in the first place*. Indeed, to us *Moses* illogically turns the statutory language on its head, by deeming individual conduct to violate the FDCPA where it would have violated the FTC Act, rather than (as the statute commands) deeming individual conduct to violate the FTC Act only if it violated the FDCPA. In our view then, in *RCG Advances* Braun's individual liability for RCG's violation of GLBA Section 521(a) should have been assessed under the GLBA's standard for individual liability, which may well differ substantially from the FTC Act's standard for individual liability.[60]

Relief. As discussed in Part III.A *supra*, in *RCG Advances* the relief awarded by the district court as a remedy for the violation it found of the GLBA Pretexting Prohibition included (1) consumer redress under Section 19 of the FTC Act; (2) civil monetary penalties under Section 5(m)(1)(A) of the FTC Act; and (3) a permanent injunction under Section 13(b) of the FTC Act. We set forth below our analysis of the district court's three remedy rulings.

1. **Consumer Redress**

Under Section 19(a) of the FTC Act, an award of consumer redress is permissible only where the defendant

[60] We unfortunately have found no case purporting to set forth the standard for individual liability under either GLBA Section 521(a) or the GLBA generally. We do note, however, that other statutes have stricter standards for individual liability than the standard applied under the FTC Act. *See* FTC v. Ross, 743 F.3d 886, 892 (4th Cir. 2014) (contrasting standard for individual securities fraud liability with the FTC Act individual liability standard).

either (1) violates a "trade regulation rule" (i.e., a rule enacted under FTC Act Section 18(a)(1)(B) that defines with specificity acts or practices that are unfair or deceptive within the meaning of FTC Act Section 5(a)),[61] or (2) has been found in a final FTC cease-and-desist order entered pursuant to FTC Act Section 5(b) to have committed an unfair or deceptive trade practice in violation of FTC Act Section 5(a).[62] As discussed in Part III.A *supra*, the district court found that the FTC was entitled to recover consumer redress by reason of the defendant's violation of the GLBA Pretexting Prohibition[63] and further found that the amount of recoverable consumer redress was $3,421,067.[64] Both findings were correct, in our judgment. The district court based the first finding on its conclusion that GLBA authorizes the FTC to enforce the GLBA Pretexting Prohibition by treating violations of the GLBA Pretexting Prohibition as violations of a trade regulation rule,[65] and indeed that is the only reasonable reading of the relevant statutory language.[66] The

[61] *See* 15 U.S.C. § 57b(a)(1).

[62] *See* 15 U.S.C. § 57b(a)(2).

[63] *See SJ Ruling*, 2023 WL 6281138 at *11.

[64] *See PT Ruling*, 2024 WL 449288 (S.D.N.Y., Feb. 6, 2024) at *8–10.

[65] *See SJ Ruling*, 2023 WL 6281138 at *11.

[66] As the district court pointed out (*see SJ Ruling* at *11), GLBA Section 522(a) allows the FTC to enforce the GLBA Pretexting Prohibition "in the same manner and with the same power and authority" that the FTC has under the FDCPA, see 15 U.S.C. § 6822(a), and the FDCPA in turn allows the FTC to use "all of its functions and powers" under the FTC Act to enforce compliance with the FDCPA and, in so doing, to treat an FDCPA violation "in the same manner as if it had been a violation of a [FTC] trade regulation rule." 15 U.S.C. § 1692l(a). Given this statutory language, the conclusion is inescapable that, for purposes of the FTC's enforcement of the GLBA Pretexting Prohibition, violations of the GLBA Pretexting Prohibition may be treated as violations of a trade regulation rule.

district court thus correctly concluded that, under FTC Act Section 19(a)(1), the defendant's violation of the GLBA Pretexting Prohibition in and of itself was sufficient to entitle the FTC to recover consumer redress for the injury consumers suffered by reason of that violation. The district court based the second finding on a statistical study done by the FTC that estimated the aggregate amount by which RCG either overdebited or underfunded its customers.[67] Given that the defendant made no effort to challenge the reasonableness of the FTC's statistical methodology and presented no calculation of his own of the aggregate amount of the overdebiting and underfunding that occurred,[68] the district court was well within its discretion to accept the essentially uncontradicted evidence the FTC offered on this point.

2. Civil Monetary Penalties

Under Section 5(m)(1)(A) of the FTC Act, an award of a civil monetary penalty is permissible only where the defendant (1) violates a trade regulation rule (2) "with actual knowledge or knowledge fairly implied on the basis of objective circumstances" that the violative act or practice is unfair or deceptive and is prohibited by the rule.[69] As discussed in Part III.A *supra*, in *RCG Advances* the district court's summary judgment ruling found that the defendant had violated a trade regulation rule,[70] and the district court's post-trial decision found that the defendant "knowingly"

[67] *See PT Ruling*, 2024 WL 449288 at *9.

[68] *See id*. at *10.

[69] 15 U.S.C. § 45(m)(1)(A).

[70] *See SJ Ruling*, 2023 WL 6281138 at *13.

committed that violation[71] and should be assessed a Section 5(m)(1)(A) penalty in the amount of $16,965,000.[72]

The district court's finding of a violation of a trade regulation rule seems to us to be correct. The district court based that finding on its conclusion that the GLBA authorizes the FTC to enforce the GLBA Pretexting Prohibition by treating violations of the GLBA Pretexting Prohibition as violations of a trade regulation rule.[73] That conclusion was in our view correct, for the reasons discussed above in relation to the district court's ruling on consumer redress.

The district court's finding of a "knowing" violation of Section 521(a) on the defendant's part seems highly questionable to us. The district court based that finding on the jury's supposedly "binding" trial finding that the defendant "knowingly violated the GLB Act."[74] But the jury's finding is only binding on the district court to the extent the district court properly instructed the jury regarding the law on a "knowing" violation of the GLBA Pretexting Prohibition (which we believe it did not do[75]) and to the extent the jury

[71] *See PT Ruling*, 2024 WL 449288 at *10.

[72] *See id*. at *10–11.

[73] See *SJ Ruling*, 2023 WL 6281138 at *13.

[74] *See PT Ruling*, 2024 WL 449288 at *1 & *10.

[75] The district court instructed the jury that in order to find a "knowing" violation of GLBA Section 521(a) the jury needed to find that the defendant had actual knowledge that RCG made material misrepresentations to its customers and that the defendant "knew or should have known that [the misrepresentations] were violating the GLB Act," meaning that he had "actual knowledge that [RCG] was violating the GLB Act or that a reasonable person under the circumstances would have known that there was a federal law prohibiting deceptive practices in making agreements like" RCG's agreements with its customers. *See* The Court's Instructions to the Jury, Instruction No. 10, FTC v. RCG Advances, LLC, No. 1:20-cv-04432 (S.D.N.Y, filed Jan. 10, 2024). As the district court's summary judgment ruling pointed out (*see SJ*

was presented with evidence from which a reasonable fact-finder could find that the defendant committed a "knowing" violation of the GLBA Pretexting Prohibition (which

Ruling, 2023 WL 6281138 at *13), there is case law supporting the district court's use of a "should have known" standard for determining whether, per Section 5(m)(1)(A), the defendant had "knowledge fairly implied on the basis of objective circumstances that [his conduct in violation of GLBA Section 521(a) was] prohibited by" GLBA Section 521(a), although that statutory language certainly could be read to require something more than that the defendant "should have known" he was violating the statute in question. However, even assuming that part of the Court's instruction was correct, we believe the district court was on shaky ground in describing the "should have known" standard as being whether a "reasonable man" would have known that the conduct in question violated the GLBA Pretexting Prohibition. We believe a more reasonable "should have known" standard would be the standard used for determining individual liability under the FTC Act, under which an individual "should have known" that the company's conduct violated the FTC Act only where the individual "was recklessly indifferent to its [violative nature], or had an awareness of a high probability of [its being violative] and intentionally avoided learning of the truth." FTC v. Moses, 913 F.3d 297, 307. Moreover, the district court in our view was also on shaky ground in characterizing the GLBA Pretexting Prohibition as a "federal law prohibiting deceptive practices in making agreements like" the MCA Agreements. That language sounds like a description of FTC Act Section 5(a)'s deception prong, rather than a description of the GLBA Pretexting Prohibition. The GLBA Pretexting Prohibition would be more accurately characterized as a "federal law prohibiting false, fictitious, or fraudulent statements in order to obtain customer information of a financial institution." Given the substantial differences between the two statutes, having actual knowledge or reason to know of Section 5(a)'s deception prong, or that one's conduct was violating that prong, would certainly not equate to having actual knowledge or reason to know of the GLBA Pretexting Prohibition or that one's conduct was violating *that* requirement. Yet that is what the district court's jury instruction mistakenly suggests. And the district court's mistake was material, because the defendant's mere knowledge or reason to know that RCG was violating a "federal law prohibiting deceptive practices" (*i.e.*, FTC Act Section 5(a)) would not be knowledge sufficient to justify a Section 5(m)(1)(A) penalty.

> seems highly questionable to us, from what we can tell from the district court's summary judgment and post-trial rulings[76]).

[76] The district court's post-trial ruling does not set forth what evidence the jury was presented in regard to the defendant's alleged "knowing" violation of the GLBA Pretexting Prohibition, so we cannot be sure on this point. At summary judgment, however, the only evidence the FTC offered on the "knowing" violation point was two documents showing that the defendant was aware of the existence of *the GLBA in general*. *See SJ Ruling*, 2023 WL 6281138 at *13. The district court ruled that this evidence was insufficient to conclusively establish a "knowing" violation of Section 521(a) on the defendant's part, but it then went on to find this evidence sufficient to enable a reasonable factfinder to find such a violation at trial. *Id*. We respectfully disagree with the district court on the latter point. Evidence that the defendant knew of the existence of *the GLBA in general* does not raise an inference that he knew of the existence of *the GLBA Pretexting Prohibition in particular*, much less an inference that he knew RCG was violating the GLBA Pretexting Prohibition by its misrepresentations to its customers. Nor does such evidence suggest anything about what a reasonable person would know regarding the GLBA or the GLBA Pretexting Prohibition or what conduct violates the GLBA Pretexting Prohibition. After all, the GLBA Pretexting Prohibition is just one subsection of a massive statute that contains seven separate Titles, 20 separate Subtitles, 141 separate sections, and certainly more than 1000 (we haven't counted) other subsections. Moreover, FTC enforcement of the GLBA Pretexting Prohibition was virtually unheard of prior to *RCG Advances*, as prior to the Supreme Court's decision in AMG Capital Management, LLC. v. FTC, 593 U.S. 67 (2021), the FTC could have used Section 5(a)'s deception prong to challenge, and FTC Act Section 13(b) to seek consumer redress for, any conduct that might have violated the GLBA Pretexting Prohibition. As a result, as the district court pointed out, no litigated decisions existed as to the scope of the GLBA Pretexting Prohibition prior to its rulings in *RCG Advances*. *See SJ Ruling*, 2023 WL 6281138 at *9. Indeed, many privacy and cybersecurity lawyers (including the senior author of this Article) had never had any occasion even to encounter the GLBA Pretexting Prohibition prior to *RCG Advances*. And the FTC's original complaint in *RCG Advances* did not even allege a violation of the GLBA Pretexting Prohibition, suggesting that *even the FTC* did not have reason to know that the facts it was alleging amounted to a violation of the GLBA Pretexting Prohibition. With all that being the case, a

Finally, we believe the district court's finding as to the amount of the Section 5(m)(1)(A) fine was clearly incorrect. The district court based that finding on its conclusion that the defendant had committed 942 violations of the GLBA Pretexting Prohibition during the five-year limitations period, consisting of the estimated 546 RCG customers who were overdebited, and the estimated 396 RCG customers who were underfunded, during that five-year period under the 1,499 MCA Agreements that RCG then had in place with its customers.[77] Evidently, the district court assumed that the defendant had violated the GLBA Pretexting Prohibition only if, and only when, RCG overdebited or underfunded a customer pursuant to one of the MCA Agreements.[78] This assumption seems to us to have been clearly erroneous.[79] By

person's mere knowledge of the existence of GLBA in general would not, in our view, give anyone reason to know of the requirements of and the sort of conduct that violates the GLBA Pretexting Prohibition. Thus, assuming that at trial the jury was presented with the same "evidence" of the defendant's "knowing" violation of the GLBA Pretexting Prohibition that the FTC had relied on at summary judgment, and was presented with no other evidence that went to the issue (we are not aware of any), we believe the district court should have directed a verdict in the defendant's favor on this point on the ground that no reasonable jury could find a knowing GLBA Pretexting Prohibition violation based on that evidence.

[77] *See PT Ruling*, 2024 WL 449288 at *10–11.

[78] The FTC appears to have made this very same assumption, as its summary judgment motion calculated the proposed Section 5(m)(1)(A) penalty based on its expert's estimate of the number of customers who were overdebited or underfunded during the five-year limitations period. *See* FTC's Memorandum in Support of Its Motion for Summary Judgment Against Defendant Jonathan Braun, FTC v. RCG Advances, LLC, No. 1:20-cv-04432, at 35-36 (S.D.N.Y, filed Apr. 8, 2022).

[79] Even if this assumption had been correct, it seems to us the penalty amount was miscalculated, because under this assumption the number of GLBA Pretexting Prohibition violations should have been calculated not based on the *number of customers* who suffered overdebiting or underfunding

its own express terms, the GLBA Pretexting Prohibition is violated when "customer information of a financial institution" *is obtained* by a third party by means of a false, fictitious, or fraudulent statement or representation—not when such information, having been so obtained, is thereafter misused by the third party to the detriment of the customer in question. In *RCG Advances*, then, the number of GLBA Pretexting Prohibition violations should have been calculated based on the number of MCA Agreements that, during the five-year limitations period, RCG *entered into* and by which it thereby unlawfully obtained the customer's bank account information.[80] It should have been irrelevant to the calculation of the number of violations whether or how often the customer's bank account information was thereafter misused to the detriment of the customer.

3. Permanent Injunction

Under Section 13(b) of the FTC Act, entry of a permanent injunction against conduct violative of "any provision of law enforced by the [FTC]" is permissible in certain circumstances.[81] As discussed in Part III.A *supra*, in *RCG Advances* the district court's summary judgment ruling applied the *W.T. Grant* standard and found that the FTC was entitled to a Section 13(b) permanent injunction against the defendant,

the five-year limitations period, but the *number of times* overdebiting or underfunding occurred during that period. In other words, under this assumption there should have been two violations—not one violation—if a customer was overdebited twice during the limitations period.

[80] The district court's rulings in *RCG Advances* do not say how many of the 1,499 MCA Agreements that RCG had in place during the five-year limitations period were entered into during that period, so we are not able to say whether the district court's finding of 942 GLBA Pretexting Prohibition violations over- or undercalculated the actual number of GLBA Pretexting Prohibition violations that occurred.

[81] *See* 15 U.S.C. § 53(b).

on the ground that "there exists some cognizable danger of recurrent violation" by the defendant of the GLBA Pretexting Prohibition and FTC Act Section 5(a).[82] Even assuming the district court correctly applied the *W.T. Grant* standard, we believe the district court's entry of a Section 13(b) permanent injunction was erroneous, as it failed to take account of certain of the other statutory predicates to the entry of such an injunction and the FTC's failure to establish those other predicates in *RCG Advances*.

First, by its express terms FTC Act Section 13(b)(1) permits the FTC to commence a civil action "to enjoin" a particular act or practice only where the FTC "has reason to believe" that the defendant "is violating, or is about to violate, any provision of law enforced by the [FTC]."[83] In *RCG Advances*, neither the FTC's original complaint nor the amended complaint it filed approximately a year later made any allegation to the effect that the defendants were violating or were about to violate either the GLBA Pretexting Prohibition or FTC Act Section 5(a). Moreover, at summary judgment the FTC advanced no argument and proffered no evidence that the defendant was violating or was about to violate either of those statutes, and the district court certainly made no finding to this effect.[84] Absent any such allegation, argument, evidence, or finding, no authority existed for the Section 13(b) injunction the district court entered in *RCG Advances*.[85]

[82] *See SJ Ruling*, 2023 WL 6281138 (S.D.N.Y., Sept. 27, 2023), at *14 (quoting United States v. W.T. Grant Co., 345 U.S. 629, 633 (1953)).

[83] 15 U.S.C. § 53(b)(1).

[84] *See SJ Ruling*, 2023 WL 6281138 at *14.

[85] *See* FTC v. Shire ViroPharma, Inc., 917 F.3d 147, 161 (3d Cir. 2019) (to state a claim for a permanent injunction under Section 13(b) of the FTC Act,

Second, by its express terms Section 13(b)(2) permits the FTC to commence a civil action "to enjoin" a particular act or practice only where the FTC "has reason to believe" that "the enjoining thereof *pending the issuance of a complaint by the Commission* and *until such complaint is dismissed by the Commission or set aside by the court on review, or until the order of the Commission made thereon has become fina*l, would be *in the interest of the public*."[86] In *RCG Advances*, neither the FTC's original complaint nor the amended complaint it filed approximately a year later made any allegation to the effect that it "would be in the interest of the public" to enter injunctive relief "pending the issuance," and during the pendency, of an FTC administrative complaint. Nor did the FTC make any argument or offer any evidence to this effect at summary judgment, and the district court certainly made no such finding in granting the permanent injunction requested by the FTC. Indeed, satisfying Section 13(b)(2) would have been impossible in *RCG Advances*, as the FTC never filed an administrative complaint under FTC Act Section 5(b) with respect to the acts and practices that its complaint alleged violated the GLBA Pretexting Prohibition and FTC Act Section 5(a). Nor did it ever seek interim injunctive relief of ***any*** sort, much less of the sort described in Section 13(b)(2), namely an injunction pending the issuance and during the pendency of an FTC administrative complaint.[87] Absent any such allegation, argument, evidence, or finding,

"the FTC must plead that [the defendant] 'is' violating or 'is about to' violate [a] law" enforced by the FTC).

[86] 15 U.S.C. § 53(b)(2) (emphasis added).

[87] The FTC's failure to seek interim injunctive relief in *RCG Advances* strongly suggests that *RCG Advances was not* a case where, as required by Section 13(b)(1), the FTC had reason to believe the defendants "[were] violating, or [were] about to violate, any provision of law enforced by the [FTC]."

no authority existed for the Section 13(b) permanent injunction the district court entered in *RCG Advances*.[88]

Third, as the Supreme Court noted in *AMG Capital Management, LLC v. FTC*, the "appearance of the words ''permanent injunction'' (as a proviso [following after Section 13(b)'s authorization of interlocutory injunctive relief]) suggests that those words are directly related to a previously issued preliminary injunction."[89] While this statement by the Supreme Court was dictum, and while several courts have subsequently refused to follow that dictum[90], we

[88] It might be argued that our first and second points of disagreement with the district court's Section 13(b) ruling are invalid because the FTC need only satisfy Sections 13(b)(1) and 13(b)(2) where it is seeking interim—rather than permanent—injunctive relief under Section 13(b). *See, e.g.,* FTC v. American Future Systems, Inc., No. 20-CV-2266, 2021 WL 3185777 at *1, n.1 (PartA) (E.D. Pa. July 26, 2021) (holding that the FTC can seek a Section 13(b) permanent injunction without ever filing (or intending to file) an administrative complaint). Such an argument would however run afoul of the plain language of Section 13(b) itself, which requires the Section 13(b)(1) and 13(b)(2) predicates to be met in any action "to enjoin"—not to "preliminarily" or "temporarily" or "interlocutorily" enjoin—an act or practice thereunder. That argument would also run afoul of the overall structure of Section 13(b), which sets the Section 13(b)(1) and 13(b)(2) predicates off from the rest of Section 13(b) in a fashion that can only be read as intending that Section 13(b)'s remaining language, including its permanent injunction proviso, is *all* subject to satisfaction of the Section 13(b)(1) and 13(b)(2) predicates.

[89] 593 U.S. 67, 76 (2021).

[90] *See, e.g.,* FTC v. Am. Future Sys., Inc., No. 20-CV-2266, 2021 WL 3185777, at *1 (E.D. Pa. July 26, 2021) ("Neither *AMG Capital* nor any other case in this Circuit or others requires FTC to seek or obtain a temporary restraining order or preliminary injunction before pursuing permanent injunctive relief under Section 13(b)."); FTC v. Elec. Payment Sols. of Am. Inc., No. 17-CV-2535, 2021 WL 3661138, at *16 (D. Ariz. Aug. 11, 2021) ("the provision of §13(b) authorizing the FTC to seek a permanent injunction operate[s] separately from the provision authorizing the FTC to seek a preliminary injunction while pursuing administrative proceedings"); FTC v. Neora LLC, 552 F.

believe that the structure of Section 13(b)'s statutory language inescapably conditions the availability of a Section 13(b) permanent injunction on the FTC's having sought and obtained interlocutory injunctive relief with respect to whatever act or practice the FTC is seeking to permanently enjoin. After all, given that as discussed above Section 13(b)(2) expressly conditions *any* action "to enjoin" an act or practice under Section 13(b) on the FTC's having reason to believe that interim injunctive relief with respect to such act or practice is in the interest of the public, how is it plausible that Congress did not also intend to condition any such action on the FTC's actually *acting* on that required belief by seeking and obtaining the interim injunctive relief it believes to be in the public interest? If our (and apparently the Supreme Court's) reading of that statutory language is correct, then the district court's entry of a Section 13(b) permanent injunction in *RCG Advances* was erroneous, as the FTC never sought, much less obtained, a Section 13(b) interlocutory injunction in that case.

Fourth, by its express terms Section 13(b)'s permanent injunction proviso says that the FTC may seek a permanent

Supp. 3d 628, 635-36 (N.D. Tex. 2021)(rejecting the argument that, under Section 13(b), "permanent injunctions are wholly unavailable absent a prior administrative proceeding or previously issued preliminary injunction or temporary restraining order," reasoning that this argument was "inconsistent" with Section 13(b)'s "legislative history and relevant precedent"). But each of these three courts reached its conclusion based on a still-binding pre-*AMG* Court of Appeals precedent that the court believed to preclude it from following the Supreme Court's *AMG* dictum on this point. Also, while in FTC v. Hoyal & Assocs., Inc., 859 F. App'x 117, 120 (9th Cir. 2021), the Ninth Circuit issued a "non-precedential" opinion reaffirming its pre-*AMG* holdings regarding the availability of a Section 13(b) permanent injunction ("We have long held that the FTC can obtain injunctive relief without initiating administrative proceedings."), it did so without considering the *AMG* dictum that calls the continuing validity of those holdings into question.

injunction thereunder only "in proper cases" and that the court may issue such an injunction only "after proper proof."[91] In *RCG Advances* the district court gave no consideration as to whether the action was a "proper case" for the FTC to seek a Section 13(b) permanent injunction, and it may well be that neither party raised the issue to the district court. As discussed below, we believe *RCG Advances* was not a "proper case" for the FTC to seek a Section 13(b) permanent injunction and that the district court accordingly erred in entering such an injunction in that case.

The sparse case law under Section 13(b)'s permanent injunction proviso offers little guidance as to what constitutes a "proper case" for a Section 13(b) permanent injunction.[92] Neither does Section 13(b)'s legislative history or the plain meaning of the word "proper" provide any useful interpretive guidance.[93] For its part, the FTC initially advanced but later withdrew an interpretation of a "proper case" as being a "clear case" of a violation of the statute in question.[94] Today, however, the FTC evidently advocates for a "proper case" as being one where the violation either is ongoing or

[91] 15 U.S.C. § 53(b).

[92] *See* Howard Beales III & Timothy J. Muris, S*triking the Proper Balance: Redress Under Section 13(b) of the FTC Act*, 79 ANTITRUST L. J. 1, 31 (2013) (concluding that "the case law does not answer the question what is a 'proper case'" under Section 13(b)). Our review of the post-2013 case law likewise reveals no answer to this question, although one decision came close to adopting (and could be read as having adopted) the standard for "proper case" advocated in Beales & Muris. *See infra* note 99.

[93] *Id*. (noting that "[t]he term ''proper'' simply means ''suitab[le],'' and does not tell us whether a case is one that is suitable for an award of" a Section 13(b) permanent injunction and that "the legislative history of Section 13(b) . . . does not specifically address this point").

[94] *See id*. at n.146.

likely to recur.[95] That interpretation, however, would render the "proper cases" requirement completely superfluous, as it would simply duplicate the long-standing requirement for entry of a permanent injunction by a federal court that the Supreme Court enunciated (some two decades before Section 13(b) was added to the FTC Act) in *W.T. Grant*. Moreover, that interpretation would strip Section 13(b)'s separate "after proper proof" permanent injunction precondition of any possible independent meaning, because the "after proper proof" predicate to Section 13(b) permanent injunctive relief is where—if anywhere—Congress might reasonably be thought to have statutorily enshrined the *W.T. Grant* standard. We therefore find the FTC's interpretation of "proper cases" to be unpersuasive.

For similar reasons, we are not persuaded by interpretations that read "proper cases" to mean cases in which the FTC has satisfied one or more of the above-discussed statutorily specified preconditions for a Section 13(b) permanent injunction.[96] Under those interpretations the "proper cases" requirement accomplishes nothing, as the preconditions are all independently statutorily specified and thus there was no need for Congress to limit Section 13(b) permanent injunctions to "proper cases" to make those preconditions

[95] *See, e.g.*, Plaintiffs' Opposition to Defendants' Motion for Summary Judgment, FTC v. Quincy Bioscience Holding Co. Inc., No. 1:17-cv-00124, at 43 (S.D.N.Y., filed June 12, 2022).

[96] *See, e.g.*, Reply Memorandum of Law in Further Support of Defendants' Motion for Summary Judgment, FTC v. Quincy Bioscience Holding Co. Inc., No. 1:17-cv-00124, at 35 (S.D.N.Y., filed July 11, 2022) (arguing that "Section 13(b)'s provision for permanent injunctive relief in ''proper cases'' means cases in which the agency has either commenced a contemporaneous administrative proceeding and/or sought preliminary relief at the outset of the federal court litigation").

statutorily applicable to requests for permanent injunctive relief under Section 13(b) .

We believe the far most persuasive interpretation of "proper cases" is advanced by two former high-ranking FTC officials, Howard Beales III and Timothy J. Muris,[97] who argue that the interpretation of "proper cases" should focus on the circumstances where it made sense for Congress to permit the FTC to forego the standard FTC Act Section 5(b) administrative process, and instead resort to a Section 13(b) judicial proceeding, in seeking to have the violative conduct prospectively, and permanently, enjoined. They conclude such circumstances exist, and therefore a "proper case" for seeking a Section 13(b) permanent injunction exists, only where "the case presents a straightforward violation of Section 5 such that the FTC's expertise [and therefore an FTC Act Section 5(b) administrative proceeding in which such expertise could best be brought to bear] is not necessary."[98] A "proper case," per Beales & Muris, would therefore not be one where the FTC "seeks to advance or clarify the law."[99]

[97] Beales & Muris, *supra* note 92.

[98] *Id*. at 32.

[99] *Id*. The approach advocated in Beales & Muris was quoted with apparent approval in *FTC v. Surescripts, LLC*, 424 F. Supp. 3d 92, 99 (D.D.C. 2020). There the court found "considerable weight to Surescripts's argument that 'proper cases' is not synonymous with 'all cases,' for such an interpretation would make the phrase superfluous." *Id.* at 98. But the court found that while authorities such as Beales & Muris "conclude that permanent injunctions are ill suited for cases requiring the FTC's expertise and the development of law through the administrative process," those authorities "do not then go on to preclude a case brought under circuit precedent." *Id*. at 100. Thus, because "[t]he FTC grounds its legal argument here in Circuit precedent," the court found that the FTC's complaint adequately alleged a "proper case" for Section 13(b) relief. *Id*. at 98. In *RCG Advances*, of course, the FTC had no circuit

Had the Beales & Muris interpretation of "proper cases" been applied in *RCG Advances*, the district court surely would have rejected the FTC's request for a Section 13(b) permanent injunction. As the district court's summary judgment decision amply illustrates on repeated occasions, the FTC's theory of liability and relief in *RCG Advances* raised numerous novel, never-before-decided issues under FTC Act Section 5 and the GLBA Pretexting Prohibition and thus in no way, shape, or form "present[ed] a straightforward violation" of those statutes. Instead, it unambiguously was a case where the FTC sought to "advance or clarify the law."[100] For this further reason, then, we believe the district court's entry of a Section 13(b) permanent injunction in *RCG Advances* was in error.

precedent on which to ground its interpretations of the GLBA Pretexting Prohibition, so the FTC's GLBA Pretexting Prohibition claim in *RCG Advances* was not a "proper case" for Section 13(b) relief under the test employed in *Surescripts*.

[100] *See, e.g.*, Alysa Hutnik, Donnelly McDowell & John Villafranco, *"FTC Continues Push for Civil Penalties with Important Implications for Financial Institutions and MLMs*," JDSUPRA (June 16, 2021), www.jdsupra.com/legal-news/ftc-continues-push-for-civil-penalties-6913247/ (describing FTC's penalty theory under the GLBA Pretexting Prohibition in *RCG Advances* as a "novel theory" that is "likely to be tested in litigation").

C. *What Do the District Court's RCG Advances Rulings Regarding the FTC's Ability to Enforce the GLBA Pretexting Prohibition Imply Regarding the FTC's Ability to Enforce the GLBA Security Requirement?*

The district court's rulings in *RCG Advances* also have significant implications regarding the FTC's enforcement authority with respect to the GLBA Pretexting Prohibition's sister provision, namely, the GLBA Security Requirement, and the Safeguards Rule enacted thereunder by the FTC. As discussed above, the linchpin of the enforcement authority theory the FTC advanced and the district court accepted in *RCG Advances* with respect to the GLBA Pretexting Prohibition was the statutory language in the GLBA that (via the FDCPA) expressly provided for any violation of the GLBA Pretexting Prohibition to be treated as a violation of the prohibition on unfair and deceptive trade practices contained in Section 5(a) of the FTC Act and/or as a violation of a trade regulation rule promulgated by the FTC under the FTC Act.[101] The GLBA contains no comparable statutory language with respect to the GLBA Security Requirement and/or rules promulgated by the FTC thereunder, however . Rather, with respect to enforcement of those components of the GLBA, the GLBA merely provides, in Section 505(a)(7), that the GLBA Security Requirement and the rules promulgated by the FTC thereunder are to be enforced by the FTC "[u]nder the Federal Trade Commission Act."[102]

Looking at the phrase "[u]nder the [FTC] Act" in isolation, it might be imaginable that Congress intended by that phrase for violations of the GLBA Security Requirement and the rules promulgated by the FTC thereunder to be deemed violations of (1) the prohibition on unfair and deceptive trade practices

[101] See Parts III.A and III.B *supra*.

[102] 15 U.S.C. § 6805(a)(7).

contained in Section 5(a) of the FTC Act, or (2) a "trade regulation rule" promulgated by the FTC under the FTC Act,[103] or (3) both. But when that phrase is viewed alongside the GLBA's separate language *expressly* providing for any violation of the GLBA Pretexting Prohibition to be treated as a violation of *both* the prohibition on unfair and deceptive trade practices contained in Section 5(a) of the FTC Act *and* a violation of a trade regulation rule promulgated by the FTC under the FTC Act, it becomes manifestly untenable to read the phrase "[u]nder the Federal Trade Commission Act" as being intended to accomplish that very same outcome with respect to the GLBA Security Requirement and the rules promulgated by the FTC thereunder. If that were Congress's intent, then why didn't Congress use the very same language to specify the FTC's enforcement authority with respect the GLBA Security Requirement and the rules promulgated by the FTC thereunder that Congress used to specify the FTC's enforcement authority with respect to the GLBA Pretexting Prohibition? After all, the GLBA Security Requirement and the GLBA Pretexting Prohibition were enacted simultaneously in 1999 as the linchpins of GLBA Title V (entitled "Privacy"), with the GLBA Security Requirement being the foundation of Subtitle A of GLBA Title V ("Disclosure of Nonpublic Personal Information") and the GLBA Pretexting Prohibition being the foundation of Subtitle B of GLBA Title V ("Fraudulent Access to Financial Information"). That being the case, how can it be that Congress would have used the phrase "under the [FTC] Act" in order to give the FTC the very same enforcement authority with respect to the GLBA Security Requirement and the rules promulgated by the FTC thereunder that Congress expressly gave to the FTC, by means of dramatically different language, with respect to the GLBA Pretexting Prohibition?

[103] *See* FTC's definition of the term "trade regulation rule," *supra* note 10.

The answer to that question, we suggest, is that it simply cannot be that the language of GLBA Section 505(a)(7) creates the very same FTC enforcement authority with regard to the GLBA Security Requirement and the rules promulgated thereunder by the FTC that GLBA Section 522(a) (via the FDCPA) creates for the FTC with regard to the GLBA Pretexting Prohibition. Instead, the far more reasonable reading of GLBA Section 505(a)(7) is that it gives the FTC a far more limited enforcement authority, restricting the FTC's enforcement of the GLBA Security Requirement and the rules promulgated by the FTC thereunder to situations where the act or practice in question would otherwise be actionable "under the [FTC] Act."

So when (if ever) would a violation of the Safeguards Rule enacted by the FTC under the GLBA Security Requirement be in and of itself actionable by the FTC under the FTC Act? The answer appears to us to be "likely never," at least as matters currently stand. The FTC Act creates four mechanisms by which the FTC can take enforcement action thereunder: (1) filing an administrative complaint seeking a cease-and-desist order under FTC Act Section 5(b); (2) filing a civil action seeking a civil monetary penalty under FTC Act Section 5(m)(1)(A) or (B); (3) filing a civil action seeking injunctive relief under FTC Act Section 13(b); or (3) filing a civil action seeking consumer redress under FTC Act Section 19. As shown below, none of these mechanisms currently creates FTC enforcement authority with respect to a mere violation of the FTC's Safeguards Rule.

> **Section 5(b) Administrative Complaint**. FTC Act Section 5(b) authorizes the FTC to file an administrative complaint for the purpose of seeking a cease-and-desist order with respect to an act or practice that the FTC finds to be unfair or deceptive in violation of FTC Act Section 5(a).[104] A

[104] *See* 15 U.S.C. § 45(b).

violation of the FTC's Safeguards Rule, standing alone, would not ipso facto constitute a violation of FTC Act Section 5(a), however, for three reasons. First, as noted above, there is no statute deeming a violation of the FTC's Safeguards Rule to be a violation of FTC Act Section 5(a) or an FTC trade regulation rule.[105] Second, the FTC Safeguards Rule does not itself deem violations thereof to be violations of FTC Act Section 5(a), and even if it did that aspect of the FTC's Safeguards Rule would be beyond the FTC's rulemaking authority, because the FTC's Safeguards Rule was enacted by the FTC under GLBA Sections 501(b) and 505(b)(2), not under FTC Act Section 18(a)(1)(B), which is the FTC's sole authority to enact trade regulation rules, i.e., rules that "define with specificity acts or practices which are unfair or deceptive acts or practices" violative of Section 5(a).[106] Third, nothing in the FTC's Safeguards Rule itself conditions an act or practice only being found to violate the rule if the act or practice meets either (1) the three-prong test set forth in FTC Act Section 5(n), satisfaction of which is a necessary precondition to any act or practice being found

[105] Compare, by way of contrast, (1) Section 814(a) of the FDCPA, 15 U.S.C. § 1692l(a) (in granting FDCPA enforcement authority to the FTC, expressly providing that "a violation of [the FDCPA] shall be deemed an unfair or deceptive act or practice in violation of [the FTC] Act" and that the FTC shall have the power address FDCPA violations "in the same manner as if the violation had been a violation of a Federal Trade Commission trade regulation rule"); and (2) Section 1303(c) of the Childrens Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6502(c) (in granting COPPA enforcement authority to the FTC, expressly providing that "a violation of a regulation prescribed [by the FTC] under [COPPA Section 1303(a)] shall be treated as a violation of a [FTC trade regulation rule]").

[106] *See* 15 U.S.C. § 57a(a).

"unfair" within the meaning of Section 5(a),[107] or (2) the three elements of a valid claim under Section 5(a)'s deception prong, as those elements are laid out in the FTC's 1983 Policy Statement on Unfairness.[108] That being the case, the conclusion is inescapable that the FTC has no authority "under the [FTC] Act", and thus has no authority of any sort, to remedy an alleged violation of the Safeguards Rule by means of a cease-and-desist order entered under FTC Act Section 5(b), unless the FTC alleges and proves that the alleged Safeguards Rule violation also independently violated FTC Act Section 5(a)'s prohibition on unfair and deceptive trade practices.

Perhaps in tacit recognition of this deficiency in its Safeguards Rule enforcement arsenal, most of the FTC's enforcement actions under the Safeguards Rule have indeed alleged both a Safeguards Rule violation and an independent violation of FTC Act Section 5(a). But not always. As Commissioner Phillips pointed out in his statement regarding the FTC's 2020 administrative complaint against Ascension Data & Analytics, LLC, that complaint (as well as several prior FTC administrative complaints) alleged a violation of the Safeguards Rule without also alleging an independent

[107] *See* FTC Act Section 5(n), 15 U.S.C. § 45(n) (providing that the FTC shall have no authority to declare an act or practice violative of FTC Act Section 5(a) as being "unfair" "unless the act or practice [1] causes or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition").

[108] *See* FTC Policy Statement on Deception (Oct. 14, 1983), *available at* https://www.ftc.gov/legal-library/browse/ftc-policy-statement-deception (specifying that a valid claim under FTC Act Section 5(a)'s deception prong requires showing an act or practice that is (1) likely to mislead (2) a reasonable consumer (3) in a material way).

violation of FTC Act Section 5(a).[109] Evidently, then, a school of thought may exist at the FTC that the FTC somehow *does* have authority to remedy an alleged violation of the Safeguards Rule by means of a cease-and-desist order entered under FTC Act Section 5(b)—regardless of whether the alleged Safeguards Rule violation also independently violated FTC Act Section 5(a)'s prohibition on unfair and deceptive trade practices. As Commissioner Phillips rightly pointed out in his statement in *Ascension Data & Analytics*, having such authority would be quite convenient for the FTC, as it may often be difficult for the FTC to show that the act or practice in question violated not only the Safeguards Rule, but also FTC Act Section 5(a), given the heightened requirements for proving an violation of Section 5(a)'s unfairness and deception prongs.[110] But to date there is no *litigated* case where a court has found that the FTC in fact has such authority. And as other recent litigated cases regarding the FTC's enforcement authority under the FTC Act show only too well, courts that are asked to rule on that authority give short shrift to whether the authority being claimed by the FTC would be helpful to the FTC's mission or has long been exercised by the FTC (or both).[111] Instead, such courts focus on the relevant statutory language and apply that language

[109] *See* Statement of Commissioner Noah Joshua Phillips Regarding Ascension Data & Analytics (Dec. 14, 2020), at p.2 and n.4, *available at* www.ftc.gov/system/files/documents/public_statements/1584714/phillips_ascension_statement_final_for_posting.pdf.

[110] *See id*. at p.2.

[111] For example, in the *AMG*, *Shire*, and *LabMD* rulings discussed *infra* in note 112, the courts rejected longstanding FTC interpretations of its enforcement authority that, according to the FTC, significantly advanced the FTC's consumer protection mission.

as written.[112] In like fashion, one would expect a court that is asked to rule on the FTC's claimed authority to remedy an alleged violation of the Safeguards Rule by means of a cease-and-desist order entered under FTC Act Section 5(b) to reject that claim as being directly at odds with the relevant statutory language. One would further expect such a court, in so doing, to follow the lead of other courts by ignoring the FTC's arguments that the FTC had long purported to exercise such authority and that the FTC's having such authority would serve its consumer-protection mission.

Section 5(m)(1) Action for Penalties. FTC Act Section 5(m)(1) authorizes the FTC to file a civil action for the purpose of seeking to recover a civil monetary penalty with respect to an act or practice that either violates a trade regulation rule[113] or was previously found unfair or deceptive by

[112] *See, e.g.*, AMG Capital Mgmt., LLC. v. FTC, 593 U.S. 67 (2021) (rejecting FTC's interpretation of term "injunction" in FTC Act Section 13(b) as including equitable monetary relief, on the ground that plain meaning of the word "injunction" defeated the FTC's interpretation); FTC v. Shire ViroPharma, Inc., 917 F.3d 147, 161 (3d Cir. 2019) (rejecting as being impossible to square with the plain language of FTC Act Section 13(b)(1) the FTC's position that it can state a claim for a permanent injunction under Section 13(b) of the FTC Act without pleading that the defendant is violating or is about to violate a law enforced by the FTC); LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018) (rejecting, as being at odds with the plain meaning of FTC Act Section 5(n), FTC's interpretation that satisfaction of Section 5(n)'s three-prong test is not merely necessary, but sufficient, to make an act or practice "unfair" within the meaning of FTC Act Section 5(a)); LabMD, Inc. v. FTC, 678 F. App'x 816, 821 (11th Cir. 2016) (rejecting FTC's interpretation of the phrase "likely to cause" in FTC Act Section 5(n) to mean "significant risk," on the ground that dictionary meaning of the word "likely" made it impossible to "read the word 'likely' to include something that has a low likelihood" of occurring).

[113] *See* 15 U.S.C. § 45(m)(1)(A).

a final FTC cease-and-desist order under FTC Act Section 5(b).[114] As discussed above, the Safeguards Rule is not a trade regulation rule, and a Safeguards Rule violation could not in and of itself be the basis for an FTC cease-and-desist order under FTC Act Section 5(b). The FTC therefore has no authority "under the [FTC] Act" to seek a Section 5(m)(1) civil monetary penalty merely by reason of a violation of the Safeguards Rule.[115]

Section 13(b) Action for Injunctive Relief. FTC Act Section 13(b) authorizes the FTC to file a civil action for the purpose of seeking injunctive relief whenever the FTC "has reason to believe . . . . . . that any person, partnership, or corporation is violating, or is about to violate, any provision of law enforced by" the FTC.[116] As the Safeguards Rule is a "provision of law enforced by" the FTC, this language at first blush seems to authorize the FTC to seek injunctive relief where a person "is violating, or is about to violate," the Safeguards Rule. But read as a whole, FTC Act Section 13(b) negates the FTC's having any such authority. As discussed in Part III.B *supra*, under FTC Act Section 13(b)(2),[117] Section

[114] *See* 15 U.S.C. § 45(m)(1)(B).

[115] *See* United States Government Accountability Office Report to Congressional Requesters, GAO-19-196, Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies, at 32 (Feb. 2019) ("GLBA, one of the key laws governing the security of consumer information, does not provide FTC with civil penalty authority."). Nor does the FTC have any authority to remedy a Safeguards Rule violation by seeking a civil monetary penalty under FTC Act Section 5(l), first because only the Department of Justice has authority to seek such a penalty, and second because a Section 5(l) penalty must be predicated on a violation of an FTC order, and the FTC (as shown above) has no authority to enter a Section 5(b) cease-and-desist order based on a mere violation of the Safeguards Rule.

[116] *See* 15 U.S.C. § 53(b)(1).

[117] 15 U.S.C. § 53(b)(2).

13(b) injunctive relief is permitted only where it would be in the interest of the public to enter such relief "pending the issuance of a [Section 5(b)] complaint by the Commission and until such complaint is dismissed by the Commission or set aside by the court on review, or until the order of the Commission made thereon has become final." In other words, Section 13(b) injunctive relief is available only where the FTC would be entitled to seek a Section 5(b) cease-and-desist order with respect to the violation of law in question. That being the case, if (as we believe we have shown above) the FTC has no authority to seek a Section 5(b) cease-and-desist order merely because a person "is violating, or is about to violate" the Safeguards Rule, the FTC likewise has no authority to seek Section 13(b) injunctive relief with respect to such a violation, because such relief could never be entered (as Section 13(b)(2) expressly requires) pending the issuance and final disposition of a Section 5(b) administrative complaint as to that violation.

Section 19 Action for Consumer Redress. FTC Act Section 19(b) authorizes the FTC to file a civil action for the purpose of seeking consumer redress in the circumstances identified in FTC Act Section 19(a), namely, where a person engages in an act or practice that either violates a trade regulation rule or was previously found unfair or deceptive by a final FTC cease-and-desist order under FTC Act Section 5(b).[118] As discussed above, the Safeguards Rule is not a trade regulation rule, and a Safeguards Rule violation could not in and of itself be the basis for an FTC cease-and-desist order under FTC Act Section 5(b). The FTC therefore has no authority "under the FTC Act" to seek Section 19 consumer

[118] *See* 15 U.S.C. § 57b(a)(1).

redress merely by reason of a violation of the Safeguards Rule.

If, as we believe we have shown above, none of the mechanisms by which the FTC can take enforcement action "under the [FTC] Act" currently creates FTC enforcement authority with respect to a mere violation of the FTC's Safeguards Rule, doesn't that mean that Congress accomplished nothing by giving the FTC authority to enforce the GLBA Security Requirement and the rules enacted by the FTC thereunder "under the [FTC] Act"? And doesn't interpreting that congressional grant of enforcement authority to be a legal nullity call into question the validity of that interpretation? We think the answer to both these questions is "no." The FTC's lack of enforcement authority regarding violations of the Safeguards Rule stems not from some deficiency in the statutory language that Congress used in granting that authority (as we have interpreted that language), but rather from a deficiency in the way the FTC exercised the rulemaking authority that Congress gave it by means of the GLBA Security Requirement and GLBA Section 505(b)(2). Specifically, the FTC chose to exercise its GLBA Security Requirement rulemaking authority by enacting the Safeguards Rule *under the GLBA*, rather than enacting it as a trade regulation rule *under FTC Act Section 18(a)(1)(B)*. As our above discussion of the FTC Act's enforcement mechanisms shows, if the Safeguards Rule had been enacted not under the GLBA, but rather as a trade regulation rule, then violations thereof would ipso facto violate FTC Act Section 5(a), and such violations would, therefore, open the door to remedies under Sections 5(b), 5(m)(1), 13(b), and 19 of the FTC Act.

That being the case, the FTC's lack of enforcement authority in regard to violations of the Safeguards Rule can and should be addressed not by the FTC's adopting (and asking the courts to bless) an untenable interpretation of the phrase "under the [FTC] Act" as used in GLBA Section 505(a)(7), but instead by the

FTC's exercising its authority "under the [FTC] Act" to implement the GLBA Security Requirement by means of a trade regulation rule, rather than by means of a rule enacted merely under the GLBA.[119] As then-Commissioners Phillips and Wilson recently stated:

> The Supreme Court['s *AMG*] decision . . . made clear that the words of a statute matter. Those words trump the policy preferences of commissioners. That decision should have been a wake-up call, a reminder to the [FTC] that, no matter how egregious the conduct or righteous our cause, the [FTC] is not entitled to go beyond the bounds of what the law permits. If we continue to flout the limits of our authority, the [FTC] should fully expect additional rebukes from the courts.[120]

IV. CONCLUSION

The district court's recent rulings in *RCG Advances* open the door to a very broad reading of the substantive scope of the GLBA Pretexting Prohibition and the remedies available to the

[119] We recognize that the process involved in enacting the Safeguards Rule as a trade regulation rule would have been far more cumbersome than the process involved in enacting the Safeguards Rule under the GLBA and, indeed, might have resulted in the trade-regulation-rule version of the Safeguards Rule having significant substantive differences from the Safeguards Rule as enacted by the FTC. *See* FTC Act Section 18(b), 15 U.S.C. § 57a(b) (specifying the process the FTC is required to follow in enacting trade regulation rules). But requiring the FTC to follow that process regarding the Safeguards Rule, as cumbersome as it may be, simply requires the FTC to comply with the congressionally mandated process for the FTC to promulgate rules under the GLBA Security Requirement that will be enforceable by the FTC "under the FTC Act."

[120] Dissenting Statement of Commissioners Noah Joshua Phillips and Christine S. Wilson, In the Matter of Resident Home LLC, Commission File No. 2023179 (Oct. 7, 2021), *available at* https://www.ftc.gov/system/files/documents/public_statements/1597270/resident_home_dissenting_statement_wilson_and_phillips_final_0.pdf.

FTC for a violation of that prohibition. That reading is, we believe, either clearly erroneous or at a minimum highly questionable in a number of respects. Moreover, the reasoning of those rulings casts doubt on whether the FTC currently has *any* viable remedy available to it—even the ability to obtain a mere cease-and-desist order—for a violation of the GLBA Security Requirement or the so-called "Safeguards Rule" promulgated by the FTC thereunder.

TESTING THE LIMITS OF THE IP LEGAL REGIMES: THE UNIQUE CHALLENGES OF ARTIFICIAL INTELLIGENCE

Jim W. Ko & Hon. Paul R. Michel[†]

[†] Jim W. Ko is a Partner at Wood Phillips, headquartered in Chicago, and focuses his practice on providing counsel for all the ways that intellectual property and artificial intelligence issues can and will impact businesses. Jim previously served as Senior Program Attorney for The Sedona Conference for almost a decade, managing its patent litigation (WG9/10) and trade secret (WG12) working groups.

Hon. Paul R. Michel served on the U.S. Court of Appeals for the Federal Circuit for 22 years, starting in March 1988. From December 2004 until his retirement in May 2010, he was the court's Chief Judge and a member of the Judicial Conference of the United States and its seven-judge Executive Committee.

TABLE OF CONTENTS

I. INTRODUCTION* 398

II. TO EFFECTIVELY REGULATE IP AND AI, WE MUST UNDERSTAND WHERE WE ARE AND HOW WE GOT HERE. 403

A. Terminology 403

B. The U.S. Copyright Office (USCO) and U.S. Patent and Trademark Office (USPTO) Guidance publications on AI are not binding for sufficiency-of-human-contribution determinations or any other de facto substantive rules. 408

1. The basis of and limitations on administrative agency rulemaking authority 409

2. Our Constitutional system of checks and balances at work 414

3. We need to foster and implement a consensus process for developing the law at the intersection of AI and IP and procedures for complying with and challenging it. 416

C. The copyright and patent qualification determination "lifecycle" from USCO and USPTO examination through federal court litigation 417

1. The USCO's examination of copyright applications has been largely ministerial and recordkeeping. 419

2. The USPTO's examination of patent applications has been more substantive and quasi-judicial. 420

a. USPTO examiners focus on assessing patent claim invalidity over the prior art under 35 U.S.C. §§ 102(a) and 103. 421

b. USPTO rejection rates applying a gating 35 U.S.C. § 101 subject-matter eligibility analysis increased significantly for software patents post-Alice (2014). 422

c. USPTO examiners also assess any disqualifying actions by applicants, including any prefiling public disclosures under 35 U.S.C. § 102(a)–(b). 427

3. Both the USCO and the USPTO leave final adjudication on all issues to the federal courts. 428

D. From generative artificial intelligence (GenAI-)assisted to GenAI-created or GenAI-conceived works of authorship and inventions? 429

III. ISSUE NO. 1: CAN THE POLICY OBJECTIVES UNDERLYING THE COPYRIGHT AND PATENT LEGAL REGIMES BE ATTAINED WITH SUFFICIENCY-OF-HUMAN-CONTRIBUTION DETERMINATIONS FOR GENAI-ASSISTED WORKS OF AUTHORSHIP AND INVENTIONS? 433

A. The USCO's and the USPTO's current frameworks 436

1. Both preclude any work of authorship or invention that is wholly generated by AI. 436

2. When both humans and AI contribute 438
    a. According to current USCO guidance, copyright protections are available only for the "human-authored aspects" of GenAI-assisted works of authorship. 438
    b. In its February 2024 Guidance, the USPTO extended the Pannu joint inventorship framework to AI-assisted inventions to create a "significant human contribution" requirement for inventorship. 441
    c. What quality of prompt engineering is necessary to constitute a sufficient human contribution for copyrightability or patentability? 444

B. Issue No. 1(a): Will the courts adopt the USCO's and the USPTO's frameworks for sufficiency-of-human-contribution determinations for GenAI-assisted works of authorship and inventions? 451
    1. Can prompt engineering never confer rights to the resulting GenAI output under copyright law, as presumed by the USCO? 451
    2. Did the USPTO apply the law correctly in adopting and applying the *Pannu* joint inventorship analysis as its framework? 454

a. Does the Pannu joint inventorship analysis seamlessly apply to the GenAI-assisted invention context under patent law, as presumed by the USPTO? 454

b. Did the USPTO appropriately apply principles of patent law in developing its Five Guiding Principles to apply the Pannu factors to GenAI-assisted inventions? 458

C. Issue No. 1(b): Can the USCO's and the USPTO's frameworks for sufficiency-of-human-contribution determinations feasibly be applied . . . ? 459

1. . . . by USCO examiners? 459

2. . . . by USPTO examiners with respect to separating out human contributions from GenAI-assisted inventions 460

a. . . . even with complete GenAI-input/output records? 461

b. . . . or particularly with limited access to the relevant GenAI-input/output records? 463

D. Issue No. 1(c): Can the USCO's and USPTO's frameworks for sufficiency-of-human-contribution determinations feasibly be complied with by GenAI-assisted copyright and patent applicants? 464

1. The USCO and the USPTO have taken contrasting approaches to the applicant's duty of disclosure for GenAI-assisted works of authorship or inventions. 464

a. The USCO only requires disclosure of any inclusion of GenAI-generated content and a brief explanation of the human author's contributions. 465

b. The USPTO imposes a detailed duty of disclosure for GenAI-assisted inventions. 466

2. Can the burden of proof for patentability be properly shifted under patent law for any issue? 475

3. Can the duties of disclosure for GenAI-assisted works of authorship and inventions be feasibly complied with. 476

a. . . . by copyright applicants?.................... 476

b. . . . by patent applicants for all information material to sufficiency-of-human-contribution determinations?.... 477

E. We need a better system for making sufficiency-of-human-contribution determinations. 479

IV. ISSUE NO. 2: ARE GENAI-ASSISTED SOFTWARE CODING AND AI SOFTWARE INNOVATIONS AT RISK OF SLIPPING THROUGH THE CRACKS OF THE IP LEGAL REGIMES?..... 483

A. Software lies somewhere in between the existing IP legal regimes..................................... 483

B. Software program source code and object code: why they are valuable, and how the IP regimes protect them. 487

1. Object code is the form of software programs that is pirated................................. 487

2. Source code is the form of software programs that can be exploited..................... 488

C. GenAI-assisted software coding is becoming standard practice, but its protectability under current copyright law is entirely uncertain...... 490

1. Will clear standards be set for identifying the "human-authored aspects" of GenAI-assisted works of authorship and protecting them under copyright law?........ 490

2. Even if copyrightable, will the functional reverse-engineerability of GenAI-assisted software coding render software copyrighting obsolete? 493

3. Most AI software is provided under the software-as-a-service (SAAS) model, which further reduces the utility of copyright protections.. 494

4. The risk of GenAI incorporating copyleft protected software code, potentially rendering GenAI-assisted software uncopyrightable 494

D. The "rise" of trade secrets to protect software in the AI Age? 495

E. To support the growth and protection of the AI industry in the U.S., clear and consistent guidance on 35 U.S.C. § 101 patent subject-matter eligibility for software/AI inventions is needed. 498

1. The manufactured paradoxes of the software invention and now the AI invention............ 499

2. Steering the patent law into the Information and the AI Ages 502

a. The increased bias against the 35 U.S.C. § 101 patent subject- matter eligibility for software inventions from the Supreme Court in Alice (2014)................................ 503

b. The increased bias against the 35 U.S.C. § 101 patent subject-matter eligibility for software inventions from USPTO policy and procedure 505

c. Should the USPTO continue to play a quasi-judicial role for Section 101 determinations for software and now AI inventions? 511

3. The broader implications of Section 101 patent subject-matter eligibility issues on the development of the AI industry in the U.S. 512

4. We need an improved legal regime for making 35 U.S.C. § 101 patent subject-matter eligibility determinations for software inventions... 514

V. ISSUE NO. 3: HOW IS PATENT LAW IMPACTED BY THE USE OF GENAI TO EXPAND HUMAN CAPABILITIES AND ALSO GENERATE VOLUMINOUS "ART"?.............. 520

A. The impact of GenAI on the foundational patent law concept of the person having ordinary skill in the art (PHOSITA) 520

B. The use of GenAI as a permutation generator of "art" 524

VI. ISSUE NO. 4: SHOULD THE USE OF PUBLIC GENAI IN A COMPANY'S PRODUCT DEVELOPMENT LIFECYCLE PRESUMPTIVELY CONSTITUTE PUBLIC DISCLOSURE INVALIDATING PATENT OR DESTROYING TRADE SECRET RIGHTS? 528

A. The prohibition against public disclosures of inventions before filing a patent application or of trade secrets in general 528

VII. ISSUE NO. 5: SHOULD INDIVIDUALS HAVE RIGHTS AGAINST THE USE OF GENAI TO CREATE DEEPFAKES APPROPRIATING THEIR IDENTITIES? 532

A. There is no comprehensive set of federal laws against deepfakes. 532

B. Should LLM providers bear liability for providing the tools for the generation of deepfakes? 534

VIII. ISSUE NO. 6: SHOULD WORKS OF AUTHORSHIP BE PROTECTED FROM UNAUTHORIZED USE FOR TRAINING GENAI MODELS? 535

A. Issue No. 6(a): Does existing copyright law limit the unauthorized use of works of authorship for training GenAI models? 535

B. Issue No. 6(b): Should AI providers be shielded from copyright and other liability to support the development of the AI industry in the U.S.? 537

IX. CONCLUSION 540

I. INTRODUCTION*

The U.S. copyright law protects "original works of authorship," including literary works (which includes software source code), musical works, dramatic works, choreographic works, pictorial, graphic, and structural works, audiovisual works, sound recordings, and architectural works.[1] It protects any original work "fixed in any tangible medium of expression."[2] But copyright protections do not "extend to any idea."[3] They only cover the particular expression of work of authorship, not any inventive concepts or any other ideas underlying them. The latter is where we start venturing into the arena of patent law, which protects the ideas themselves if they are "new and useful" and are adequately disclosed and nonobvious.[4]

[*] This article is intended to provide a framework for analysis for the IP issues to which the advent of generative AI gives rise, which the authors believe to be *sui generis* and at times slip through the cracks of the current IP law framework. It is intended to start a broader discussion, with the goal of developing an IP and AI law and policy that appropriately balances the rights and interests of the diverse stakeholders on these issues consistent with the underlying policy goals of the copyright, patent, trade secret, trademark, and other IP laws. The plan is to form one or more representative drafting teams to draft consensus, nonpartisan Sedona Conference commentaries on these issues. Should you have any comments on this paper and/or would be interested in participating in such a process, please reach out to comments@sedonaconference.org.

[1] 17 U.S.C. § 102(a).

[2] *Id*.

[3] 17 U.S.C. § 102(b).

[4] Patent law protects "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof," subject to certain limitations. 35 U.S.C. § 101.

Generative artificial intelligence (GenAI) in theory most directly implicates copyright and patent law for two main reasons:

- GenAI purportedly mimics or replicates critical functions of the human mind, including creative processes and problem solving. When a user of a GenAI tool inputs a "prompt" framing a creative goal or a technical problem to solve, the GenAI generates an output in response that might otherwise confer authorship or inventorship rights under our copyright and patent laws had it been generated by a human.
- Copyright and patent law both grant exclusive rights to the original works of authorship or inventions, including the right to exclude others from reproducing or using them. But if GenAI is used, in whole or in part, to create an otherwise copyrightable work or to conceive an otherwise patentable invention, should the owner or manager of the GenAI have the right to exclude others from copying or using such output? And if so, when? Without such exclusive rights, the potential value of the GenAI-assisted work of authorship or invention is reduced significantly, if not eliminated.

In contrast, neither trademark law (which protects against competitors unfairly using a company's brand to sell their goods or services) nor trade secret law (which protects against the misappropriation of any information of value, including technological processes or innovations, for which the owner takes "reasonable measures" to keep secret) are specifically directed at protecting any creative or inventive process or output.

Can the policy objectives behind the current intellectual property (IP) legal regimes be met when GenAI is implemented?[5] Or will new laws and regulations be necessary to bring patent, copyright, trade secret, and other IP law into the AI Age? This paper will explore the intersection of AI and IP law, in particular:

[5] For a broader discussion of the intersection of AI and the law in general, *see* Hon. Xavier Rodriguez, *Artificial Intelligence (AI) and the Practice of Law*, 24 SEDONA CONF. J. 783 (2023), *available at* https://thesedonaconference.org/sites/default/files/announcements/Artificial-Intelligence-and-the-Practice-of-Law-Xavier-Rodriguez_1.pdf.

1. Should GenAI-assisted works of authorship or inventions (i.e., works of authorship or inventions created in whole or in part upon GenAI output that would be copyrightable or patentable were GenAI not involved)[6] [7] ever qualify for copyright or patent protections, and if so, when?

[6] "AI-assisted invention" is the term the USPTO has adopted to discuss this concept for patent applications. *See* U.S. Patent and Trademark Office, Inventorship Guidance for AI-Assisted Inventions, 89 Fed. Reg. 10043, 10045 (Feb. 13, 2024) [hereinafter *USPTO Feb. 2024 AI-Assisted Invention Guidance*], *available at* https://www.federalregister.gov/documents/2024/02/13/2024-02623/inventorship-guidance-for-ai-assisted-inventions. For the analogous concept in copyright applications, the USCO has instead adopted the verbiage "works containing material generated by artificial intelligence." *See* U.S. Copyright Office, Copyright Registration Guidance: Works Containing Materials Generated by Artificial Intelligence, 88 Fed. Reg. 16190, 16192 (Mar. 16, 2023) [hereinafter *USCO Mar. 2023 Guidance*], *available at* https://www.govinfo.gov/content/pkg/FR-2023-03-16/pdf/2023-05321.pdf.

Both terms apply to the identical concept—when AI is involved in some fashion in the creation of a work of authorship or the conception of an invention, what quality of human contribution is necessary to convey ownership rights under the copyright and patent law? The USCO's application of this concept is a bright-line rule precluding the direct output of GenAI from ever by itself being protectable by copyright. In contrast, the USPTO's application is more permissive allowing various limited exceptions whereby GenAI output *may* be or become protectable by patent. For discussion, *see infra* Sec. III.A.2. But they are discussing the same concept.

For purposes of economy and convenience, the authors of this article adopt the term "GenAI-assisted" to apply to this concept for both works of authorship and inventions throughout.

[7] Under this definition, a given "GenAI-assisted" work of authorship can be either copyrightable or not copyrightable, and a given GenAI-assisted invention can be either patentable or not patentable. This paper's adoption of the term "*GenAI*-assisted" is used to focus on the use of the category of AI

2. Should GenAI-assisted software code qualify for protection by copyright or otherwise?
3. How will patent law be impacted by the use of GenAI to expand human capabilities and generate voluminous "art," and should it be amended?
4. Should the use of a "public" version of GenAI in a company's product development lifecycle presumptively constitute public disclosure invalidating patent or trade secret rights?
5. Should individuals have rights against the use of GenAI to create deepfakes appropriating their identities?
6. Are copyrighted works protected from being used in training GenAI models? If not, should the law be amended to extend such protections?

"that can create original content—such as text, images, video, audio or software code—in response to a user's prompt or request." *See What is Generative AI?*, IBM, *available at* https://www.ibm.com/topics/generative-ai.

No general predisposition for or against copyrightability or patentability with respect to the sufficiency (or lack thereof) of human contribution or otherwise should be ascribed to the adoption or application of this term.

For a discussion of the importance and the perils of terminology in this AI and IP law space, *see infra* Sec. II.A.

II. TO EFFECTIVELY REGULATE IP AND AI, WE MUST UNDERSTAND WHERE WE ARE AND HOW WE GOT HERE.

A. *Terminology*

In response to the already infamous *Mata v. Avianca* case,[8] in which some lawyers were sanctioned for filing a brief citing to several nonexistent GenAI "hallucinated" cases and quotations, several courts have issued prophylactic standing orders concerning the use of AI in court filings. One example states that if a litigant "has used artificial intelligence ('AI') in the preparation of any complaint, answer, motion, brief, or other paper, filed with the Court," then the litigant "MUST [] disclose that AI has been used in any way in the preparation of the filing."[9]

The wording of standing orders such as this is overly broad, as it compels disclosure of *all* AI tools, no matter how they are used to assist in the preparation of the court filing.[10] Many AI tools bear no risk of generating such hallucinations. For example, Grammarly is a popular AI tool that checks grammar and

[8] Mata v. Avianca, Inc., 678 F.Supp.3d 443 (S.D.N.Y. 2023).

[9] For the full text of this Standing Order, *see* https://www.paed.uscourts.gov/judges-info/senior-judges/michael-m-baylson. For a discussion of issues with this and other judicial standing orders regarding the use of AI in court filings, *see* NEW YORK STATE BAR ASSOCIATION, REPORT AND RECOMMENDATIONS OF THE NEW YORK STATE BAR ASSOCIATION TASK FORCE ON ARTIFICIAL INTELLIGENCE (Apr. 2024), at 51–52, *available at* https://fingfx.thomsonreuters.com/gfx/legaldocs/znpnkgbowvl/2024-April-Report-and-Recommendations-of-the-Task-Force-on-Artificial-Intelligence.pdf.

[10] *See id.* (recommending the use of the term "generative AI" as opposed to "artificial intelligence" to avoid "sweep[ing]" [excess information] into a disclosure obligation," for example, "the usage of computer-assisted review to cull and make a production of ESI").

provides tips for writing clarity.[11] If used exclusively for such purposes, these AI drafting tools will not create fictional case law references.

Further specifying that only *generative* AI tools need be disclosed would be a significant step in the right direction,[12] so long as the term is properly defined.[13] But more precision would still be needed regarding the definition of any such disclosure requirement, in part because it is now commonplace for companies (including Grammarly itself)[14] to tout that they are introducing generative AI assistance into their software platforms.

The purpose and way that a given AI tool is used should be central to the contents of any such use-of-AI disclosure requirement for court filings. For example, the use of general GenAI drafting tools like Grammarly probably need not be disclosed for the vast majority of use cases.

A possible exception, though, might be in the specific context of drafting patent applications, where the turn of a phrase can dramatically impact the scope of a patent claim, a patent specification disclosure, etc. There are GenAI drafting tools already on the market that are specifically geared toward the patent drafting process, promising not just improved drafting clarity but also scope of patent coverage. Should they be disclosed? And what would the U.S. Patent and Trademark Office (USPTO) do with this information if they are?

[11] *See Responsible AI that ensures your writing and reputation shine*, GRAMMARLY, https://www.grammarly.com/ (last visited July 27, 2024).

[12] See id.

[13] For a working definition of the term "generative AI" as used in this paper, *see supra* notes 6 & 7.

[14] *See, e.g.*, *Introducing generative AI assistance*, GRAMMARLY, https://support.grammarly.com/hc/en-us/articles/14528857014285-Introducing-generative-AI-assistance (last visited July 27, 2024).

Most challenging are those terms that may connote one thing but are used to mean something else. For example, the very concept of the term AI "hallucination," which has already entered the popular vernacular, is misleading. It is an anthropomorphism that "can obscure the reality that AI systems do not possess human-like thinking or understanding, which is crucial in recognizing the limitations and potential errors."[15]

Even the USPTO's innocuous sounding term "AI-assisted invention" defies simple definition. The definition provided by the USPTO from its February 2024 *Inventorship Guidance for AI-Assisted Inventions*, states in full:

> AI-assisted inventions are inventions created by natural persons using one or more AI systems. The AI system's contribution is not inventorship, even if the AI system's contributions were instrumental in the creation of the invention.[16]

At least as the USPTO uses the term, it is externally cabined because the USPTO's duty to disclose extends only to the degree an AI tool "is material to patentability."[17] As such, it is in effect limited to GenAI.

But the term "AI-*assisted*" as used by the USPTO parallels the commonly used phrase (at least in the IP world) of "AI tool." In a vacuum, this could connote the use of only nongenerative AI as a tool by a human "mastermind,"[18] thus supporting the

[15] *See AI Hallucinations* (last updated June 18, 2024), DEEPGRAM, https://deepgram.com/ai-glossary/ai-hallucinations.

[16] *USPTO Feb. 2024 AI-Assisted Invention Guidance, supra* note 6, at 10044, n.4 (citing *Thaler v. Vidal*, 43 F.4th 1207 (Fed. Cir. 2022)).

[17] *See* 37 C.F.R. § 1.56.

[18] The concept of a human "mastermind" using a technology as a tool to create a copyrightable work of authorship goes back in U.S. law at least as

human's inventorship status. The USPTO, however, actually uses these terms to cover both the use of nongenerative and generative AI.

In sum, the use of GenAI—under both the USPTO's application of its term "AI-assisted inventions" and this paper's application of the term "GenAI-assisted inventions" to apply the *Pannu* joint inventorship "significant contribution" standard as adopted by the USPTO[19]—somewhat counterintuitively may entail the contributions of the GenAI for a given invention:

far as the seminal Supreme Court case *Burrow-Giles Lithographic Co.* v. *Sarony*, 111 U.S. 53 (1884). In *Sarony*, the Court upheld the power of Congress to extend copyright protections to photography, holding that a posed photograph was protectable under copyright law and enforceable in court. By posing his subject and "selecting and arranging the costume, draperies and other various accessories in said photograph, arranging the subject so as to present graceful outlines, arranging and disposing the light and shade, suggesting and evoking the desired expression, and from such disposition, arrangement, or representation," the Supreme Court affirmed that the photograph was the photographer's "original intellectual conception," and he was the photograph's "mastermind." *Id* at 55, 59 & 61. As such, the Court held that the photograph was copyright eligible.

The concept of a human mastermind similarly, if not equally, applies to the use of technology as a tool to conceive of a patentable invention.

[19] The *Pannu* joint inventorship "significant contribution" standard was articulated in *Pannu* v. *Iolab Corp.,* 155 F.3d 1344, 1351 (Fed. Cir. 1998). As discussed below, however, it is unclear whether the USPTO's framework applying the standard to [Gen]AI-assisted inventorship determinations is proper, because the following should be treated as open questions:

1. Has the government articulated let alone established what present or imminent need exists regarding [Gen]AI-assisted inventions that might call for any change in established patent law or procedures in the first place? *See infra* Sec. II.B.1.

2. Was the USPTO legally authorized to publish its 2024 Guidance publications on [Gen]AI-assisted inventions to address any such problems or needs? *See infra* Sec. II.B.1.

- in some cases, rising to a level of conception out of the entire claimed invention that precludes human inventorship, but
- in other cases, allowing for human inventorship because even though the GenAI provides some degree of conception, it does *not* rise to a level that precludes human inventorship.[20]

Most AI-related terms defy any one- or two-sentence definition. They require a baseline understanding of underlying terms and concepts to understand and use properly.

This paper attempts to clearly define each AI term as it introduces them as necessary for the reader, but inevitably falls short given the range of technical knowledge and understanding of readers and the variability in how many of these terms are commonly used. A generally accepted and regularly updated glossary of terms for use in the legal context is sorely needed.[21] We cannot intelligently discuss let alone regulate these AI and IP legal issues if we are not talking about the same things.

> 3. Did the USPTO properly apply patent law in establishing its framework for sufficiency-of-human-contribution determinations for [Gen]AI-assisted inventions in its 2024 Guidance publications? *See infra* Secs. II.B.2.

[20] This logically follows from the USPTO's application of the *Pannu* factors, particularly *Pannu* factor 2. *USPTO Feb. 2024 AI-Assisted Invention Guidance, supra* note 6, at 10047. *See infra* Sec. III.A.2.b.

[21] The Sedona Conference, through its Technology Resource Panel, has regularly updated its *The Sedona Conference Glossary: eDiscovery and Digital Information Management*, with its most recent 5th Edition published in 2020, *available at* https://thesedonaconference.org/download-publication?fid=5376. The next edition of this Glossary will be updated to include AI-related terms and definitions.

B. *The U.S. Copyright Office (USCO) and U.S. Patent and Trademark Office (USPTO) Guidance publications on AI are not binding for sufficiency-of-human-contribution determinations or any other de facto substantive rules.*

In October 2023, President Biden issued an Executive Order on AI, which as directed to patent issues called upon the USPTO to publish guidance to patent examiners and applicants "addressing inventorship and the use of AI, including generative AI, in the inventive process, including illustrative examples in which AI systems play different roles in inventive processes and how, in each example, inventorship issues ought to be analyzed."[22] [23] The USPTO has responded by publishing its February 2024 *Inventorship Guidance for AI-Assisted Inventions*[24] and its April 2024 *Guidance on Use of Artificial Intelligence-Based Tools*.[25]

[22] Executive Order No. 14,110, 88 Fed. Reg. 25,191 (Oct. 30, 2023) [hereinafter *2023 Executive Order on AI*], at § 5.2(c)(i).

[23] Regarding copyright issues, the USCO is not ordered under the Executive Order to take any direct action. Rather, the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office (USPTO Director) is ordered to consult with the USCO and "issue recommendations to the President on potential executive actions relating to copyright and AI . . . including the scope of protection for works produced using AI and the treatment of copyrighted works in AI training." *Id.* at § 5.2(c)(iii).

[24] USPTO Feb. 2024 AI-Assisted Invention Guidance, supra note 6.

[25] U.S. Patent and Trademark Office, Guidance on Use of Artificial Intelligence-Based Tools in Practice Before the United State Patent and Trademark Office, 89 Fed. Reg. 25609 (Apr. 11, 2024) [hereinafter *USPTO Apr. 2024 AI-Based Tools Guidance*], *available at* https://www.federalregister.gov/documents/2024/04/11/2024-07629/guidance-on-use-of-artificial-intelligence-based-tools-in-practice-before-the-united-states-patent.

1. The basis of and limitations on administrative agency rulemaking authority

It is important, however, to understand that any substantive rulemaking the USCO and USPTO have engaged in on copyright and patent legal issues through their recent AI Guidance publications simply does not have the force of law.

It should be treated as an open question whether there has been a properly established present need for such government regulatory action in the first place.

The entirety of the stated purpose of the Biden Administration's order to the USPTO to publish the above-referenced guidance is "[t]o promote innovation and clarify issues related to AI and inventorship."[26] There is nothing in the order articulating let alone establishing what present or imminent problem or need exists regarding AI and inventorship issues that might call for any change in established patent law or procedures.[27]

Nor did the USPTO sufficiently establish any such need before it started issuing any de facto substantive rules in its 2024

[26] *2023 Executive Order on AI*, *supra* note 22, at § 5.2(c).

[27] *See id*. at § 5.2.

Guidance publications on AI.[28] [29] The Supreme Court has noted in the past that executive agencies require "ample latitude to 'adopt their rules and policies to the demands of changing circumstances,'"[30] but the presumption is "against changes in

[28] No such need is established by either the *USPTO Feb. 2024 AI-Assisted Invention Guidance, supra* note 6, or the predicate Request for Comment on Patenting Artificial Intelligence, 84 Fed. Reg. 44889 (Aug. 2019), *available at* https://www.federalregister.gov/documents/2019/08/27/2019-18443/request-for-comments-on-patenting-artificial-intelligence-inventions, that it references. Even assuming that "numerous commenters expressly agreed that the USPTO should provide guidance regarding inventorship and the patentability of AI-assisted inventions," *USPTO Feb. 2024 AI-Assisted Invention Guidance, supra* note 6, at 10044, this cannot serve as the basis for authority for the USPTO to issue de facto substantive rules, particularly under the guise of a Guidance publication.

Such significant changes in patent law, procedure, and disclosure requirement require more notice—including detailed demonstration of need, proposed change, and possible implications—and request for comment than that provided by the USPTO. For full discussion, *see infra* Sec. III.D.

[29] In contrast, the *USCO Mar. 2023 Guidance* articulates up front both a need (providing four paragraphs describing developments, based on which "the Office concludes that public guidance is needed on the registration of works containing AI-generated content") and the statutory basis of its authority. *See supra* note 6, at 16191.

[30] Motor Vehicles Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co, 463 U.S. 29 (1983). For a comprehensive discussion on the law governing administrative agency policy change and the checking of unjustified inconsistency, *see* William W. Buzbee, *The Tethered President: Consistency and Contingency in Administrative Law*, 98 B.U. L. REV. 1357–442 (Oct. 2018). Such limitations on administrative agency authority have presumably only increased with the Supreme Court's recent ruling in *Loper Bright Enterprises v. Raimondo*, 603 U.S. __, 143 S.Ct. 2429 (2024) (overruling the principle of *Chevron* deference that had directed courts to defer to an agency's reasonable interpretation of an ambiguity in a law that the agency enforces).

current policy that are not justified by the rulemaking record."[31] Agencies must engage with the "facts and circumstances that underl[ay]" an earlier action.[32] "Unexplained inconsistency" is not allowed.[33]

Whether technology has progressed such that GenAI can autonomously replicate the human mind and thus necessitate a rewrite of patent law should not be just assumed, even if the President so declared. The Biden Administration may implicitly have assumed this in ordering the Director of the USPTO to "publish guidance to USPTO examiners and applicants addressing inventorship and the use of AI, including generative AI, in the inventive process, including illustrative examples in which AI systems play different roles in inventive processes and how, in each example, inventorship issues ought to be analyzed."[34]

The USPTO has expressly "recognize[d] there are divergent views on the level of contribution AI systems can make in the invention creation process,"[35] encompassing:

- a view where AI's contributions "would not rise to the level of joint inventorship, as the core inventive

[31] *Id.* (quoting *In re* Permian Basin Area Rate Cases, 390 U.S. 747, 784 (1968)).

[32] FCC v. Fox Television Stations, Inc., 556 U.S. 502, 516 (2009).

[33] Encino Motorcars, LLC v. Navarro, 579 U.S. 211, 226 (2016) (quoting *National Cable & Telecommunications Association v. Brand X Internet Services*, 545 U.S. 967, 981 (2005)).

[34] *2023 Executive Order on AI*, *supra* note 22, at § 5.2(c)(i).

[35] USPTO Feb. 2024 AI-Assisted Invention Guidance, supra note 6, at 10047, n.30.

concepts and decisions remain within the purview of the human inventors,"[36] and

- a view where "AI is becoming powerful and creative enough to generate patentable contributions to inventions to which a human has arguably not made an inventive contribution but instead has directed the AI to endeavor towards the solution to a problem."[37]

Nevertheless, the USPTO has adopted the second view as necessary to the entire *Pannu* joint inventorship framework it sets up for sufficiency-of-human-contribution determinations for [Gen]AI-assisted inventions.[38] The USPTO has explicitly chosen sides and established a set of rules significantly changing long-standing patent law and procedure based on this choice, imposing new duties on private parties and disparately impacting different stakeholders in the patent system.

But before new duties and burdens not grounded in existing or any intervening change of law or legislated by Congress are imposed on private parties, the proponents of the new requirements must carry some burden of proof. Ipse dixit cannot suffice.

Even assuming an established need, for a federal agency to issue a "substantive" or "legislative-type" rule "affecting individual rights and obligations," the rule:

[36] *Id.* (citing *Response to the RFC from American Intellectual Property Law Association* at 3, *available at* www.regulations.gov/docket/PTO-P-2022-0045/comments).

[37] *Id.* (citing *Response to the RFC from International Federation of Intellectual Property Attorneys (FICPI)* at 3, *available at* www.regulations.gov/docket/PTO-P-2022-0045/comments*)*.

[38] *See infra* Sec. III.A.2.b.

1. "must be the product of a congressional grant of legislative authority," and
2. must be "promulgated in conformity with any procedural requirements imposed by Congress."[39]

Specifically, the agency must issue its rules subject to the requirements of the Administrative Procedure Act (APA),[40] which protect against abuse of the agency's authority.[41]

Such agency compliance with the APA is almost always achieved through the established "informal rulemaking," i.e. "notice-and-comment rulemaking" procedure, which requires specific notice to the public before issuance.[42] This "ensures the appropriate level of the public's Constitutionally safeguarded due process rights to notice and an opportunity to be heard before their government can adopt binding rules that have the force and effect of law."[43]

Agencies can issue guidance or other policy statements without any such notice-and-comment process. But they can only do this under the APA's exemptions for the publication of

[39] Chrysler Corp. v. Brown, 441 U.S. 281, 282 (1979); *see also* Paralyzed Veterans of Am. v. West, 138 F.3d 1434, 1436 (Fed. Cir. 1998).

[40] *See, generally*, Administrative Procedure Act, ch. 324, 60 Stat. 237 (1946), repealed and replaced by Pub. L. No. 89–554 (codified as 5 U.S.C. §§ 551–59).

[41] For a detailed discussion of the basis of and limitations on administrative rulemaking authority, *see* Andrew Dietrick & Jonathan Stroud, *Rules to Bind You: Problems with the USPTO's PTAB Rulemaking Procedures*, 51 N.M. L. Rev. 430, 433–36 (2021), *available at* https://digitalrepository.unm.edu/nmlr/vol51/iss2/6.

[42] 5 U.S.C. § 553(b).

[43] Dietrick, *supra* note 41, at 434, n.33.

"general statements of policy" and "interpretative rules" that do *not* constitute substantive rulemaking.[44]

2. Our Constitutional system of checks and balances at work

There has been in practice a longstanding conflict between the U.S. Federal Circuit Court of Appeals and the USPTO over the parameters of any substantive rulemaking authority the USPTO has over patent law issues. In 1996, the Federal Circuit noted in *Merck v. Kessler* that "the broadest of the PTO's rule-making powers . . . authorizes the Commissioner to promulgate regulations directed only to "the conduct of proceedings in the [PTO]"; it does NOT grant the Commissioner the authority to issue substantive rules."[45] Congress subsequently granted the USPTO certain rulemaking authority in the 1999 American Inventors Protection Act[46] and the 2011 America Invents Act (AIA).[47] In particular, the AIA formed the Patent Trial and Appeal Board (PTAB), making it the primary adjudicative body for patent postissuance reviews,[48] and granted the USPTO the authority to promulgate "sweeping rules governing proceedings in the PTAB."[49]

The USPTO has been criticized by some for "routinely issu[ing] precedential rules and tak[ing] significant action with

[44] 5 U.S.C. § 553(b)(A).

[45] Merck & Co. v. Kessler, 80 F.3d 1543, 1549–50 (Fed. Cir. 1996).

[46] American Inventors Protection Act, Pub. L. No. 106-113, § 311, 113 Stat. 1501A-552–67 (1999).

[47] Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011).

[48] *Id.* at 313–14.

[49] Dietrick, *supra* note 41, at 439.

substantive effect, [but] calling them guidance, policy documents, or administrative rulings."[50]

In fairness, at least with respect to this tidal wave of technical AI and IP law issues, some may argue—the Supreme Court's recent ruling in *Loper Bright Enterprises v. Raimondo* notwithstanding[51]—that the USCO and USPTO do not have the luxury of waiting for complete guidance from Congress or the courts. Patent applications continue to roll in, and they will increasingly fall under the category of "GenAI-assisted inventions." The USCO and USPTO have a duty to process them and to inform and update applicants about the criteria they apply for registering copyrights or granting patents. Our government and society are trying to fly this GenAI plane as we are building it.

In its 2024 Guidance publications on AI, the USPTO includes the following disclaimer:

> This guidance does not constitute substantive rulemaking and does not have the force and effect of law. The guidance sets out agency policy with respect to the USPTO's interpretation of the inventorship requirements of the Patent Act in view of decisions by the Supreme Court of the United States (Supreme Court) and the United States Court of Appeals for the Federal Circuit (Federal Circuit).[52] [53]

[50] *Id.* at 431 (citing *Aqua Prods., Inc. v. Matal*, 872 F.3d 1290, 1316 (Fed. Cir. 2017) (invalidating a set of rules promulgated by the USPTO, finding that they were substantive rules only masked as procedural)).

[51] *See supra* note 30.

[52] See, e.g., USPTO Feb. 2024 AI-Assisted Invention Guidance, supra note 6, at 10045.

[53] The *USCO March 2023 Guidance* does not include a similar disclaimer statement in the copyright context. *See supra* note 6. This may simply reflect

Having said this, the proper and transparent approach by the USPTO and the USCO would be to cite the statutory basis of their authorities and utilize the informal "notice-and-comment" rulemaking procedure prescribed by the APA. While distinguishing between what constitutes substantive rulemaking on the one hand and procedural or interpretative rulemaking on another can be a real challenge at the margins, there is no reasonable debate that the USCO and USPTO have tread significantly into the substantive rulemaking arena on these AI issues.[54] "[I]mproperly characterizing a rule regarding burdens of proof as 'procedural' does not excuse failure to comply with the Director's obligations under the APA."[55]

3. We need to foster and implement a consensus process for developing the law at the intersection of AI and IP and procedures for complying with and challenging it.

It is important for all concerned to recognize that while the USPTO and USCO are certainly key stakeholders in these AI & IP legal issues, they are not the only or even the primary ones. The USPTO and USCO have considerable expertise and bring important perspectives to these issues, but other stakeholders are equally if not more important and include vantage points from the business side and the enforcement side. While the USPTO and USCO have made a practice of soliciting input from the public on other issues, they had not sufficiently done so with

a lack of historical tension on these administrative rulemaking authority issues to date, as the USCO has only prominently assumed a substantive rulemaking and quasi-judicial role with its March 2023 Guidance. *See infra* Sec. II.C.1.

[54] For discussion, *see infra* Sec. III.A.2.

[55] *Aqua Prods.*, 872 F.3d at 1320.

respect to the development of their Guidance publications on IP and AI law before issuing de facto substantive rules for [Gen]AI-assisted works of authorship and inventions. The public—namely the users of the IP system, comprising both patent owners and potential licensees or targets of enforcement actions—should drive the process of developing the AI and IP law, and not the two offices responsible primarily for the granting and issuing of patents and copyrights within it. In any event, both offices must stay within the limits of their regulatory authority as granted by Congress. They must also ensure that their regulations adhere to the decisions of the courts.

But for the U.S. to get ahead of these AI and IP legal issues and compete globally in this critical market, we need far more than to just have our branches of government check and balance each other to stay in their lanes. We need to harness the collective wisdom across our branches of government and society to manage the unique systemic challenges that GenAI is giving rise to. We need to move toward building a true "GenAI-assisted legal system and society" and away from one that is constantly reacting to these AI issues. We need to come together and foster and implement consensus processes for moving the law forward at the intersection of these AI and IP issues and also the procedures for complying with and challenging it, through the development of principles and best practice recommendations that if adopted in whole or in part would make for a better legal system.

C. *The copyright and patent qualification determination "lifecycle" from USCO and USPTO examination through federal court litigation*

The USCO has traditionally played a ministerial role in examining copyright applications, whereas the USPTO has played a more substantive quasi-judicial role. The USCO has refused to register only about 4 percent of all copyright applications in recent years.[56] Calculating the USPTO refusal rate is more complicated, with different methodologies yielding different results,[57] but it appears to be no lower than around 30 percent and is probably significantly higher than that.[58]

[56] U.S. COPYRIGHT OFFICE, ANNUAL REPORT: FISCAL YEAR 2019 (4% of 516,713 claims received), at 38, *available at* https://www.copyright.gov/reports/annual/2019/ar2019.pdf; ANNUAL REPORT FISCAL YEAR 2020 (4.6% of 509,744 claims received), at 12, *available at* https://www.copyright.gov/reports/annual/2020/ar2020.pdf; ANNUAL REPORT FISCAL YEAR 2021 (4.3% of 403,593 claims received), at 10, *available at* https://www.copyright.gov/reports/annual/2021/ar2021.pdf; ANNUAL REPORT FISCAL YEAR 2022 (3.4% of 486,428 claims received), at 18, *available at* https://www.copyright.gov/reports/annual/2022/ar2022.pdf; ANNUAL REPORT FISCAL YEAR 2023 (<3% of 481,031 claims received), at 7, *available at* https://www.copyright.gov/reports/annual/2023/ar2023.pdf.

[57] Calculating USPTO patent rejection rates is a challenge. Even though the scope of the underlying invention for a patent application is theoretically fixed, the scope of the patent application over the USPTO's examination process is anything but. Almost every patent application that ultimately issues has been rejected in whole or in part at least one time during the USPTO patent examination process, and it is not at all unusual for multiple rejections over multiple years. To overcome each rejection, the patent applicant revises the application, often significantly, amending some claims and dropping others entirely. Patent applicants often abandon their patent applications entirely after a USPTO rejection—primarily for business reasons and not necessarily due to concerns that a patent will not ultimately issue. Given all these variables, what counts as a rejection is subject to interpretation.

[58] *See* Dennis Crouch, *USPTO Grant Rate 2021*, PATENTLYO (Apr. 5, 2021), https://patentlyo.com/patent/2021/04/uspto-grant-rate.html; *see also* Stephen Schreiner, *Recent Statistics Show PTAB Invalidation Rates Continue to Climb*, IP WATCHDOG (June 25, 2024) (finding that the USPTO's Patent and Trial Review Board's total invalidation rate where all challenged claims are found invalid is currently at 71% for the first two quarters of 2024), *available at* https://ipwatchdog.com/2024/06/25/recent-statistics-show-ptab-

This is a natural consequence of the differences between these two forms of intellectual property.

The quid pro quo of any patent system is to encourage public disclosure of inventions by granting successful applicants the exclusive right to practice their inventions for a period of time.[59] The bargained for exchange of the copyright system is far more specific and limited—it primarily protects against the copying for commercial purposes of a single original work of authorship for a period of time.[60]

What is the optimal balance of roles and responsibilities with respect to these copyright and patent qualification determinations for GenAI-assisted works of authorship or inventions between the USCO/USPTO and the federal courts?

1. The USCO's examination of copyright applications has been largely ministerial and recordkeeping.

Before the advent of GenAI, there was in effect a presumption of copyrightability. Any original work of authorship automatically gains copyright protections upon creation under state copyright laws, independent of any copyright registration.[61]

invalidation-rates-continue-climb/id=178226/#:~:text=From%202015%20to%202019%2C%20the,daunting%20statistics%20for%20patent%20holders.

[59] In the U.S., an issued patent's standard term "end[s] 20 years from the date on which the application for the patent was filed . . . ." 35 U.S.C. § 154.

[60] In the U.S., "As a general rule, for works created after January 1, 1978, [U.S.] copyright protection lasts for the life of the author plus an additional 70 years." *How Long Does Copyright Protection Last?*, U.S. COPYRIGHT OFFICE, https://www.copyright.gov/help/faq/faq-duration.html#:~:text=The%20term%20of%20copyright%20for,plus%20an%20additional%2070%20years (last visited July 27, 2024).

[61] "Copyright exists automatically in an original work of authorship once it is fixed, but a copyright owner can take steps to enhance the protections," namely through federal or state copyright registration. *What is Copyright?*,

Federal registration of a copyright with the U.S. Copyright Office is not a requirement but does provide added protections and benefits, including the ability to enforce the exclusive rights of copyright through litigation in federal court.[62] The USCO states that "it refuses only a minority of claims on the basis of copyrightability, because copyright law [] sets a very low threshold for what works are sufficiently original."[63] Unless outright copying is involved, the general presumption is that two independently generated works of authorship are as unique as the minds that created them.

With little substantive analysis or investigatory work traditionally done during the copyright application process, the USCO's role in copyright examinations has been primarily ministerial and recordkeeping.

2. The USPTO's examination of patent applications has been more substantive and quasi-judicial.

The USPTO's examination of patent applications has always been more substantive than that of the USCO. The USPTO requires the applicant to disclose "all information known [] to be material to patentability,"[64] including information relevant to the following analyses.

U.S. COPYRIGHT OFFICE, https://www.copyright.gov/what-is-copyright/ (last visited July 27, 2024).

[62] *See Why Register When Protection is Automatic*, COPYRIGHT ALLIANCE, https://copyrightalliance.org/faqs/why-register-copyright/#:~:text=Bringing%20an%20Infringement%20Action%3A%20It,the%20infringement%20has%20already%20occurred (last visited July 27, 2024).

[63] U.S. COPYRIGHT OFFICE, ANNUAL REPORT: FISCAL YEAR 2019, *supra* note 56, at 38.

[64] 37 C.F.R. § 1.56.

a. USPTO examiners focus on assessing patent claim invalidity over the prior art under 35 U.S.C. §§ 102(a) and 103.

Unlike copyrights, there simply cannot be any such presumption of patentability for purported inventions. It is not only possible but commonplace for two or more people to independently develop the same inventive concept to solve a given problem. When that happens, the key question in the U.S. to determine priority rights used to be who conceived of the inventive concept first, under the long-existing "first-to-invent" system.[65] But in September 2012, with the passage of the AIA, the U.S. joined the rest of the world in moving to a "first-to-file" patent system.[66]

Such a "race-to-the-patent-office" system provides more certainty on these priority questions. But the faster applicant's patent application might still be rejected during examination, and any issued patent might even be invalidated after issuance—via either postgrant procedures before the PTAB or litigation before the federal courts—because:

- a third-party may have gotten there first with a single "anticipatory" printed publication (whether a previously issued patent or otherwise) under 35 U.S.C. § 102(a), or
- the invention might be ruled "obvious" over the combination of two or more existing pieces of prior art under 35 U.S.C. § 103.

The USPTO's examination of these issues is a far more labor-intensive process than that typically conducted by the USCO.

[65] *See US Patent First to File: Everything You Need to Know*, UPCOUNSEL (updated Feb. 1, 2023), https://www.upcounsel.com/us-patent-first-to-file.

[66] *Id.*

There are countless ways that a patent claim can be "read" on (i.e., have each and every element of the claim met by one or more pieces of prior art) and thus invalidated.

b. USPTO rejection rates applying a gating 35 U.S.C. § 101 subject-matter eligibility analysis increased significantly for software patents post-Alice (2014).

The USPTO also engages in an even more fundamental substantive analysis under 35 U.S.C. § 101 regarding subject-matter eligibility, i.e., whether the subject matter of the purported invention is categorically eligible for a patent in the first place.

The importance and number of rejections on these grounds, in particular in the business-method and software patent spaces, increased significantly after the Supreme Court's seminal *CLS Bank v. Alice* ruling in 2014.[67] Since *Alice*, both preliminary motions to dismiss and parallel PTAB proceedings to invalidate the patent on Section 101 grounds have become standard protocol for patent defendants.[68] *Alice* initiated an existential crisis for the software patenting industry that is still being worked through by the USPTO and the federal courts a decade later.

[67] Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. 208, 212 (2014) (invalidating patent claims for a computer-implemented, electronic escrow service because implementing claims on a computer was not enough to transform an abstract idea into patentable subject matter).

[68] *See* The Sedona Conference, *Commentary on Patent Litigation Best Practices: Section 101 Motions on Patentable Subject Matter Chapter* (Sept. 2016 public comment version), *available at* https://thesedonaconference.org/publication/Commentary_on_Patent_Litigation_Best_Practices_Chapter_on_Section_101_Motions_on_Patentable_Subject_Matter.

Most AI inventions are computer-implemented through software.[69] *All* AI software inventions are vulnerable to the heightened vicissitudes of 35 U.S.C. § 101 challenges and determinations for software.[70]

The USPTO has provided voluminous guidance to its patent examiners on how to conduct a 35 U.S.C. § 101 analysis.[71] The main gating step in a Section 101 subject-matter eligibility analysis is determining whether the claimed subject matter falls within the "judicial exceptions," i.e., subject matters that the courts have found to be outside of the four statutory categories

[69] Frank Chau, et al., Intellectual Property Owners, AI Patenting Handbook, 19 (March 2024) [*hereinafter IPO AI Patenting Handbook*].

[70] For discussion, *see infra* Sec. IV.E.

[71] For the USPTO's compilation of its 35 U.S.C. § 101 guidance, including 46 illustrative hypothetical examples applying to guidance to certain fact-specific situations, *see* U.S. Patent and Trademark Office, Subject matter eligibility, *available at* https://www.uspto.gov/patents/laws/examination-policy/subject-matter-eligibility (noting the USPTO's most recent set of guidance issued in 2019 has been incorporated in the Ninth Edition of the Manual of Patent Examination Procedure (MPEP)). The USPTO's guidance on Section 101 and other patent law issues is generally based on a rich body of Supreme Court and Federal Circuit case law and can be more characterized as descriptive or interpretative, at least relative to the USPTO's 2024 AI Guidance publications. *See supra* Sec. II.B.1.

The USPTO has now published its 2024 Guidance Update on Patent Subject Matter Eligibility, Including on Artificial Intelligence, 89 Fed. Reg. 58128 (July 17, 2024) [hereinafter *USPTO July 2024 Sect. 101 Updated Guidance*], *available at* https://www.federalregister.gov/documents/2024/07/17/2024-15377/2024-guidance-update-on-patent-subject-matter-eligibility-including-on-artificial-intelligence. In conjunction with this updated guidance, the USPTO has published three more illustrative hypothetical examples (Examples 47-49) specific to some common AI issues. U.S. Patent and Trademark Office, July 2024 Subject Matter Eligibility Examples, *available at* https://www.uspto.gov/sites/default/files/documents/2024-AI-SMEUpdateExamples47-49.pdf.

of patent eligible inventions (consisting of a process, machine, manufacture, or composition of matter), because they have been identified as the "basic tools of scientific and technological work," and are thus excluded from patentability because "monopolization of those tools through the grant of a patent might tend to impede innovation more than it would tend to promote it."[72] These judicial exceptions that are *not* patent eligible consist of:[73]

1. An "abstract idea," including:
   a. "mathematical concepts," such as mathematical relationships, mathematical formulas or equations, and mathematical calculations;[74]
   b. "certain methods of organizing human activity," such as economic principles or practices, commercial or legal interactions, and managing personal behavior, relationships, or interactions between people;[75] and
   c. "mental processes," i.e., concepts performed in the human mind, including observations, evaluations, judgments, and opinions;[76]

[72] *Alice*, 573 U.S. at 216 (quoting Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 569 U.S. 576, 589 (2013) and Mayo Collaborative Servs. v. Prometheus Labs. Inc., 566 U.S. 66, 71 (2012)).

[73] *See* U.S. Patent and Trademark Office, October 2019 Update: Subject Matter Eligibility, Fig. 2, at 11 (Step 2A, prong one) [hereinafter *USPTO Oct. 2019 Sect. 101 Updated Guidance*], *available at* https://www.uspto.gov/sites/default/files/documents/peg_oct_2019_update.pdf.

[74] *Id.* at 3–4.

[75] *Id.* at 4–6.

[76] *Id.* at 7–9.

2. A "law of nature";[77] and
3. A "natural phenomenon."[78]

Most relevant to AI software patents is the "mental processes" analysis. Taking a known mental process that can be "performed in the human mind" (with or without "the aid of a pen and paper") and simply claiming it as being performed on a computer is not sufficient to make it patent eligible.[79] Also important is the "mathematical concepts" analysis. A mathematical algorithm is not patentable.[80]

But even if a claimed invention is deemed to fall under a judicial exception (like many AI software claimed inventions do as an "abstract idea"/"mental process"), it still may be patent eligible—at least in theory—so long as the claimed invention is integrated into a "practical application" of that abstract idea.[81]

The USPTO and the courts have long struggled to provide consistent guidance for when a judicial exception is or is not recited (Step 2A – prong 1) or when an application is "practical" enough to overcome when a judicial exception is found (Step 2A – prong 2). This is not at all surprising, because "all inventions 'at some level embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas,'"[82] and thus could arguably be presumptively invalid under Step 2A – prong 1 of

[77] *Id*. at 2.

[78] *Id*.

[79] *Id*. at 8–9.

[80] *Id*. at 3–4.

[81] *Id*. at 10–12 (Step 2A, prong two).

[82] Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. 208, 217 (2014).

the USPTO's patent subject-matter eligibility analysis.[83] As the Supreme Court cautioned, "[W]e tread carefully in construing this exclusionary principle lest it swallow all of patent law."[84]

The USPTO's rejection rate on Section 101 grounds for AI patent applications has been historically on the order of 2-3 times higher than average: 77 percent of all office actions in the WG 2120 Technology Center (AI & Simulation/Modeling) from January to June 2024, compared to 24 percent over this same period for all patent applications across all technology centers.[85]

In the 2023 Executive Order on AI, the Biden Administration also ordered the USPTO to "issue additional guidance to USPTO patent examiners and applicants to address other considerations at the intersection of AI and IP, which could include, as the USPTO Director deems necessary, updated guidance on patent eligibility to address innovation in AI and critical and emerging technologies."[86] The USPTO has now complied, issuing in July 2024 its *Guidance Update on Patent Subject Matter Eligibility, Including on Artificial Intelligence*.[87]

[83] *USPTO July 2024 Sect. 101 Updated Guidance*, *supra* note 71, at 58134 (quoting Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66, 71 (2012)).

[84] *Alice*, 573 U.S. at 217.

[85] *See* Eli Mazour, *Section 101 Rejections Soar at USPTO; 77% of AI Tech Group's OAs Include 101 Rejections*, VOICE OF IP (June 18, 2024), *available at* https://www.voiceofip.com/p/breaking-section-101-rejections-soar. This data can be confirmed at the U.S. Patent Office's Open Data Portal (beta), *Agency Trends: Rejections in Office Actions for Patent Applications*, https://developer.uspto.gov/visualization/agency-trends-rejections-office-actions-patent-applications.

[86] *2023 Executive Order on AI*, *supra* note 22, at § 5.2(c)(ii).

[87] *USPTO July 2024 Sect. 101 Updated Guidance*, *supra* note 71.

Will this new Guidance provide the certainty necessary on these Section 101 patent subject-matter eligibility issues to support the development of the AI industry in the U.S.? Or will the ambiguity and inconsistency of the application of patent law for software inventions, including in AI, have a chilling effect on the level of investment that companies commit to developing a patent portfolio for their AI inventions and compromise the U.S.'s global competitiveness in this critical industry?[88]

c. USPTO examiners also assess any disqualifying actions by applicants, including any prefiling public disclosures under 35 U.S.C. § 102(a)–(b).

Another way to lose patent rights centers on any prefiling disclosures of an invention made by the applicant, typically for marketing or product development purposes. The general rule is that a patent applicant cannot publicly disclose its invention before filing the patent application.[89] In the U.S. (and a minority of other countries), however, a one-year grace period is statutorily mandated to give the applicant the opportunity to complete its invention or test the marketplace for its commercial embodiment before having to file for a patent application.[90]

Under 37 C.F.R. § 1.56, patent applicants have a duty to disclose all "information material to patentability,"[91] which includes any such disqualifying prefiling disclosures. As a

[88] For full discussion, *see infra* Sec. IV.E.

[89] 35 U.S.C. § 102(a) ("A person shall be entitled to a patent unless (1) the claimed invention was patented, described in a printed publication, or in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention . . . .").

[90] *See* 35 U.S.C. § 102(b).

[91] For discussion regarding application of 37 C.F.R. § 1.56 to AI patent applications, *see infra* Sec. III.D.1.b.

practical matter, a USPTO examiner's determination on this issue is based only on the information disclosed and anything else the examiner happens to come across during the examination.

35 U.S.C. § 102(b) takes on new and unique significance in our incipient AI Age, when generative AI will be increasingly used as part of the product development lifecycle by companies and individuals, in potential violation of the catchall "otherwise [made] available to the public" bar under 35 U.S.C. § 102(b).[92]

3. Both the USCO and the USPTO leave final adjudication on all issues to the federal courts.

The USCO and USPTO provide in effect only a gatekeeping function on any copyrightability or patentability issues. They both ultimately grant all applications they cannot reject based on the information provided or found during examination.

As with all federal agencies and consistent with the separation of powers under the Constitution, the USCO and USPTO leave final adjudication of any disputes on substantive issues—typically arising only during litigation when a copyright or patent infringement defendant attempts to weaken the IP owner's case—to the federal courts.[93] The degree of rigor applied for the substantive assessment of these issues during their initial

[92] For discussion, *see infra* Sec. V.

[93] Congress, however, somewhat departed from this framework with the passage of the America Invents Act (AIA) effective 2012. The AIA established the USPTO Patent Trial and Appeal Board (PTAB), which comprised a new forum, new administrative judges, and new rules to resolve issues of patent validity outside of litigation in the federal courts. Since then, patent infringement defendants have been given two parallel avenues to invalidate asserted patents: one before the PTAB and one before the federal courts. Final adjudication of PTAB rulings, however, also remains under the authority of the Federal Circuit.

examinations is an implicit balancing of two competing interests: 1.) accuracy and certainty in the quality of any issued copyrights or patents; and 2.) speed and efficiency in the examination process.

For the most part, with a notable exception for prior art searches by the USPTO, both offices in effect conduct their examinations under the assumption that the applicant's disclosures are complete. They take on, at most, only a limited investigatory role regarding the sufficiency of any disclosures, implicitly leaving the resolution of any disputes on these issues to the federal courts.

D. *From generative artificial intelligence (GenAI-)assisted to GenAI-created or GenAI-conceived works of authorship and inventions?*

Copyright law and patent law have developed over centuries, adapting to new technologies and the occasional paradigm shift as they have arisen over time. GenAI, however, theoretically undercuts one of the core premises underlying both—the source of the act of any creation or conception. Before GenAI, the motive force was *always* human.

As noted by the court in *Thaler v. Perlmutter*:

> Copyright is designed to adapt with the times. Underlying that adaptability, however, has been a consistent understanding that human creativity is the sine qua non at the core of copyrightability, even as that human creativity is channeled through new tools or into new media.[94]

[94] Thaler v. Perlmutter, 687 F. Supp. 3d 140, 146 (D.D.C. 2023).

All technological advancements in the past have readily (at least with the benefit of hindsight) slid into the category of a tool that could be used as a human being to create (e.g., the camera) or invent (e.g., the integrated circuit, which itself led to another "tool," the computer).

With GenAI, however, there may be a transition from GenAI-*assisted* written works of authorship and inventions to GenAI-*created* or *-conceived* ones, where the GenAI takes over more and more of the role of the mastermind, even though a human being may have set the GenAI on the original task that led to the finished products.

This may be more clearly the case with works of authorship. The USCO provides the following illustrative example and discussion:

> [I]f a user instructs a text generating technology to ''write a poem about copyright law in the style of William Shakespeare,'' she can expect the system to generate text that is recognizable as a poem, mentions copyright, and resembles Shakespeare's style. But the technology will decide the rhyming pattern, the words in each line, and the structure of the text. When an AI technology determines the expressive elements of its output, the generated material is not the product of human authorship.[95]

GenAI *may* also be increasingly taking on the role of the mastermind for the conception and reduction-to-practice of AI-assisted inventions. It should be noted, however, that neither Congress nor the courts have established to date that GenAI is

[95] *USCO Mar. 2023 Guidance, supra* note 6, at 16192.

fundamentally different than any other technological development in this regard.[96]

If a generic human input like "Find me a substance that cures prostate cancer" were enough to elicit a cure from the GenAI output, then this would reflect both that the GenAI conceived the solution and that the human should not be able to patent it. That is not, however, what happens when GenAI is implemented in reality. There is typically an iterative GenAI-input/output process, with the human taking a GenAI output and further refining it with another GenAI input generating a new GenAI output, over and over again. At some point, such "prompt engineering" might suffice for the human to gain patent rights over that cure. But when? And how can this be established to the satisfaction of the USPTO?

In principle, any GenAI-*assisted* invention is patentable when the AI is used as a tool by a human mastermind, whereas any wholly GenAI-*conceived* invention should not be. But unless the law evolves to allow ownership of GenAI-assisted inventions to automatically confer to a human being or to preclude such human ownership in all cases, our government and society must:

[96] For example, in *Thaler v. Vidal*, 43 F.4th 1207 (Fed. Cir. 2022), the Federal Circuit only affirmed summary judgment by the lower court affirming the USPTO's denial of inventorship rights for an inventor who specifically disclaimed making any contribution to the conception of a claimed invention. The court did not make any finding as to whether the claimed invention was otherwise patentable, or whether the GenAI in question's contributions would otherwise qualify it for inventorship if made by a human. The court noted: "While we do not decide whether an AI system can form beliefs, nothing in our record shows that one can, as reflected in the fact that Thaler submitted the requisite statements himself, purportedly on [the GenAI's] behalf." *Id.* at 1211.

- develop standards and a process for determining when a GenAI-assisted invention crosses the line to becoming a GenAI-conceived invention, and
- develop a process for how to enforce these standards.

III. ISSUE NO. 1: CAN THE POLICY OBJECTIVES UNDERLYING THE COPYRIGHT AND PATENT LEGAL REGIMES BE ATTAINED WITH SUFFICIENCY-OF-HUMAN-CONTRIBUTION DETERMINATIONS FOR GENAI-ASSISTED WORKS OF AUTHORSHIP AND INVENTIONS?

Fundamental copyright and patent qualification issues arise when GenAI is used to assist in the creation of a work of authorship or the conception and/or reduction-to-practice of an invention.

When should GenAI output be protectable under copyright and patent law? Should one be able to secure IP rights by:

- Framing a technological problem as a single GenAI input and then patenting the GenAI output itself as an invention?
- Framing a creative goal as a single GenAI input and then copyrighting the GenAI output as a work of creative writing, music, art, etc.?
- Framing a software coding goal or architecture as a single GenAI input and then copyrighting the GenAI output?

Based at least on the recent guidance of the USCO and the USPTO, the answer is no for each question, as discussed in detail in this section.

This section will further examine fundamental copyright and patent law issues that arise for GenAI-assisted works of authorship and inventions. Notably, many of these issues are not specifically raised or addressed in the USCO and the USPTO's recent Guidance publications on AI. Rather, their guidance is built upon certain assumptions on these issues. The authors of this article respectfully submit that neither these assumptions nor the guidance built upon them should be wholly accepted or rigidly implemented without closer examination.

The following should be treated as open questions:

1. Has an existing or imminent need regarding GenAI-assisted works of authorship or inventions that might call for any change in established law or procedures been established and clearly defined in the first place?[97]
2. Did the USCO and the USPTO issue de facto substantive rules in their recent Guidance publications on AI regarding sufficiency-of-human-contribution determinations for GenAI-assisted works of authorship or inventions, in violation of the Administrative Procedure Act? [98]

Regarding copyright law:

1. Is the USCO's bright-line stance against prompt engineering serving as the basis for copyrightability over GenAI output for GenAI-assisted works of authorship correct (i.e., will the federal courts apply it?)?[99]

Regarding patent law, *each* of the following should be treated as open questions regarding the USPTO's current guidance on AI:

1. Is the USPTO's *Pannu* joint inventorship framework[100] the correct foundation that should be applied for GenAI-assisted inventions under patent law (i.e.,

[97] For discussion, *see supra* Sec. II.B.1.

[98] For discussion, *see supra* Sec II.B.2.

[99] For discussion, *see infra* Sec. III.B.1.

[100] For discussion, *see infra* Sec. III.A.2.b.

will the federal courts apply it)?[101] Or is it predicated on the assumption that GenAI can autonomously replicate human conception in a way that may otherwise confer inventorship rights under patent law were it conceived by one or more humans—a presumption that actually has not been established by the courts or by Congress?

2. Did the USPTO properly apply other principles of patent law on top of its *Pannu* joint inventorship framework to develop its February 2024 Guidance's Five Guiding Principles for GenAI-assisted inventions?[102]
   a. In its April 2024 Guidance, did the USPTO effectively shift the burden of proof for patentability onto the patent applicant?
   b. Can the burden of proof for patentability be properly shifted to the patent applicant under patent law?
3. Can the USPTO's overall sufficiency-of-human-contribution determination framework for GenAI-assisted patent applications feasibly be carried out by patent examiners?[103] Or feasibly complied with by patent applicants?[104]
4. Will the resulting uncertainty for the patentability of all GenAI-assisted inventions—which may comprise most patent applications in the future—be harmful for the U.S. patent system and for U.S. innovation?

[101] For discussion, *see infra* Sec. III.B.2.a.

[102] For discussion, *see infra* Sec. III.B.2.b.

[103] For discussion, *see infra* Sec. III.C.2.

[104] For discussion, *see infra* Sec. III.D.3.b.

A. The USCO's and the USPTO's current frameworks

1. Both preclude any work of authorship or invention that is wholly generated by AI.

A core legal principle in U.S. copyright law is that human authorship is required for copyright protections to be available.[105] In the context of generative AI, this means that "[i]f a work's traditional elements of authorship were produced by a machine, the work lacks human authorship and the [U.S. Copyright] Office will not register it."[106] This principle was reaffirmed by a federal district court in *Thaler v. Perlmutter* and is currently on appeal.[107] But *Thaler* only addressed copyrightability of a work that was wholly generated by generative AI.[108]

In turn, human inventorship is also a core requirement for patentability under the U.S. patent law. According to the Federal Circuit in *Thaler v. Vidal*, the Patent Act expressly provides that inventors are "individuals" and that the term "individuals"

[105] Burrow-Giles Lithographic Co. *v.* Sarony, 111 U.S. 53, 58 (1884) (describing a copyright as "the exclusive right of a man to the production of his own genius or intellect"); *cf.* Naruto *v.* Slater, 888 F.3d 418, 426 (9th Cir. 2018) (holding that a "monkey selfie" photograph was not copyrightable because it lacked the human authorship as required under copyright law).

[106] *USCO Mar. 2023 Guidance*, *supra* note 6, at 16192. The "traditional elements of authorship" are parenthetically defined to include "literary, artistic, or musical expression or elements of selection, arrangement, etc." *See id.*

[107] Thaler v. Perlmutter, No. 22-CV-1564, 2023 WL 5333236 (D.D.C. Aug. 18, 2023), appeal docketed No. 23-5233 (D.C. Cir. Oct. 18, 2023), *see USCO Mar. 2023 Guidance*, *supra* note 6, at 16191.

[108] *Thaler*, 2023 WL 5333236, at *7 (affirming the U.S. Copyright Office's rejection of a copyright application due to lack of any "creative contribution from a human actor" for a visual work that the applicant described as "autonomously created by a computer algorithm running on a machine").

means a human being.[109] "Congress has determined that only a natural person can be an inventor, so AI cannot be."[110]

According to the USPTO's February 2024 Guidance, "the use of an AI system by a natural person(s) does not preclude a natural person(s) from qualifying as an inventor (or joint inventors) if the natural person(s) significantly contributed to the claimed invention."[111] The USCO similarly affirmed that the use of an AI system by a person does not preclude copyrightability in its March 2023 Guidance.[112]

Consistent with the above, even when an AI system has contributed to a work of authorship or invention, both the USCO and the USPTO have issued guidance stating that:

- AI systems and other non-natural persons should not and cannot be listed as authors or inventors,[113] and
- no oath or declaration should be filed on behalf of any AI system.[114]

[109] Thaler v. Vidal, 43 F.4th 1207, 1211 (Fed. Cir. 2022).

[110] *Id.* at 1213.

[111] *USPTO Feb. 2024 AI-Assisted Invention Guidance*, *supra* note 6, at 10046.

[112] *USCO Mar. 2023 Guidance*, *supra* note 6, at 16192 ("In other cases [] a work containing AI-generated material will also contain sufficient human authorship to support a copyright claim.").

[113] *USPTO Feb. 2024 AI-Assisted Invention Guidance*, *supra* note 6, at 10046. But while the USCO does not require or allow AI to be a listed author on a copyright application, it does impose a new duty to disclose the inclusion of AI-generated content in a work submitted for registration. *See infra* Sec. III.D.1.a.

[114] *Id.* at 10050.

2. When both humans and AI contribute

a. According to current USCO guidance, copyright protections are available only for the "human-authored aspects" of GenAI-assisted works of authorship.

If a work of authorship contains AI-generated material, the USCO considers "whether the AI contributions are the result of mechanical reproduction" or the result of an author's "own original mental conception, to which [the author] gave visible form."[115] When a user instructs a GenAI to write a poem, song, etc., "in the style of" X, according to the current USCO guidance, the output is not copyrightable because the expressive elements of the output are determined by the technology and not by a human.[116] "Copyright law's application in this area is limited, as it does not protect artistic style as a separate element of a work."[117]

[115] *USCO Mar. 2023 Guidance*, *supra* note 6, at 16192.

[116] *Id*.

[117] Although the USCO "acknowledges the seriousness of [] concerns" held by artists "seeking protection against AI 'outputs that imitate the artistic style of a human creator,'" the USCO "does not recommend including style as protected subject matter under [the USCO's proposed] federal digital replica law at this time." U.S. COPYRIGHT OFFICE, COPYRIGHT AND ARTIFICIAL INTELLIGENCE, PART 1: DIGITAL REPLICAS (July 2024), at 53, 54 & 56 [hereinafter *USCO July 2024 Digital Replicas Report*], *available at* https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-1-Digital-Replicas-Report.pdf. For discussion of the "several sources of protection under existing laws that may be effective against unfair or deceptive copying of artistic style" as well as "the policy reasons not to extend property-like rights to style in itself," *see id.* at 53–56 ("Sec. III. Protection of Artistic Style").

For discussion of the USCO's recommendation to Congress to pass a new federal digital replica law, *see infra* note 283.

The USCO provides explicit guidance effectively precluding the possibility of a human drafting of a GenAI input (i.e., a prompt) conferring any ownership rights over the resultant GenAI output under copyright law, stating:

- "[W]hen an AI technology receives solely a prompt from a human and produces complex written, visual, or musical works in response, the 'traditional elements of authorship' are determined and executed by the technology—not the human user,"[118] and
- "While some prompts may be sufficiently creative to be protected by copyright, that does not mean that material generated from a copyrightable prompt is itself copyrightable."[119]

The USCO notes, however, that:

- a human "can select or arrange AI-generated material in a sufficiently creative way" to make the work copyrightable, and
- an artist "may modify material originally generated by AI technology to such a degree that the modifications meet the standard for copyright protection."[120]

Importantly, the USCO states that a copyright on a work of authorship that contains AI-generated material does not protect the entire work, but rather is limited only to the "human-authored aspects" of the work.[121] When a technology tool such as GenAI is used to create a work, "what matters is the extent to which the human had creative control over the work's

[118] *Id*.

[119] *Id.* at n.27.

[120] *Id.* at 16192–93.

[121] *Id.* at 16193.

expression and 'actually formed' the traditional elements of authorship."[122] Furthermore, the USCO requires the applicant to specifically disclaim the AI-generated material for a copyright to be registered.[123]

Distinguishing within a given work of authorship between what parts are AI-generated and what parts are human-authored is easier in some forms than others. Text typically is relatively straightforward (think redlines). Graphics and music are more complicated.

*****

By the end of the summer of 2024, the USCO is scheduled to issue the section of its forthcoming comprehensive copyright and AI law report on the copyrightability of works incorporating AI-generated material.[124] This section will "analyze U.S. law's human authorship requirement and its implementation by the Office in registration decisions, including how to determine when AI-generated material can embody human authorship; survey international practices; and assess the policy arguments with respect to copyright protection for AI-generated material."[125]

[122] *Id.*

[123] *Id.* at 16192 ("When an AI technology determines the expressive elements of its output, the generated material is not the product of human authorship. As a result, that material is not protected by copyright and must be disclaimed in a registration application.").

[124] Letter from Shira Perlmutter, Register of Copyrights, to Hon. Chris Coons, et al. (Feb. 23, 2024), at 5 [hereinafter *Feb. 2024 Ltr. from Shira Perlmutter*], *available at* https://copyright.gov/laws/hearings/USCO-Letter-on-AI-and-Copyright-Initiative-Update-Feb-23-2024.pdf?loclr=blogcop.

[125] *Id.*

b. In its February 2024 Guidance, the USPTO extended the Pannu joint inventorship framework to AI-assisted inventions to create a "significant human contribution" requirement for inventorship.

The USPTO's guidance for inventions assisted by generative AI is more detailed. As announced in its February 2024 Guidance, the USPTO has adopted the existing joint inventorship framework from the Federal Circuit's opinion in *Pannu v. Iolab*[126] and applied it to this [Gen]AI-assisted inventions context, stating:

> The patent statutes require the naming of all inventors who contributed to at least one claim of a patent. The threshold question in determining the named inventor(s) is who contributed to the conception of the invention. In situations where a single person did not conceive the entire invention (*e.g.*, joint inventorship), courts have found that a person who shares in the conception of the invention is an inventor. In these situations, each named inventor in a patent application or patent, including an application or a patent for an AI-assisted invention, must have made a "significant contribution" to the claimed invention.[127]

In *Pannu*, the Federal Circuit held that in a joint inventorship dispute, to establish inventorship rights, each purported joint inventor must:

1. contribute in some significant manner to the conception or reduction to practice of the invention,

[126] *Pannu*, 155 F.3d at 1351.

[127] *USPTO Feb. 2024 AI-Assisted Invention Guidance*, *supra* note 6, at 10047.

2. make a contribution to the claimed invention that is not insignificant in quality, when that contribution is measured against the dimension of the full invention, and
3. do more than merely explain to the real inventors well-known concepts and/or the current state of the art.[128]

In its February 2024 Guidance, the USPTO published the following nonexhaustive list of principles to help inform the application of the *Pannu* factors in [Gen]AI-assisted inventions:

1. A natural person's use of an AI system in creating an AI-assisted invention does not negate the person's contributions as an inventor. The natural person can be listed as the inventor or joint inventor if the natural person contributes significantly to the AI-assisted invention.
2. Merely recognizing a problem or having a general goal or research plan to pursue does not rise to the level of conception. A natural person who only presents a problem to an AI system may not be a proper inventor or joint inventor of an invention identified from the output of the AI system. However, a significant contribution could be shown by the way the person constructs the prompt in view of a specific problem to elicit a particular solution from the AI system.
3. Reducing an invention to practice alone is not a significant contribution that rises to the level of inventorship. Therefore, a natural person who merely recognizes and appreciates the output of an AI system as an invention, particularly when the properties and

[128] *Id.*

utility of the output are apparent to those of ordinary skill, is not necessarily an inventor. However, a person who takes the output of an AI system and makes a significant contribution to the output to create an invention may be a proper inventor. Alternatively, in certain situations, a person who conducts a successful experiment using the AI system's output could demonstrate that the person provided a significant contribution to the invention even if that person is unable to establish conception until the invention has been reduced to practice.

4. A natural person who develops an essential building block from which the claimed invention is derived may be considered to have provided a significant contribution to the conception of the claimed invention even though the person was not present for or a participant in each activity that led to the conception of the claimed invention. In some situations, the natural person(s) who designs, builds, or trains an AI system in view of a specific problem to elicit a particular solution could be an inventor, where the designing, building, or training of the AI system is a significant contribution to the invention created with the AI system.

5. Maintaining "intellectual domination" over an AI system does not, on its own, make a person an inventor of any inventions created through the use of the AI system. Therefore, a person simply owning or overseeing an AI system that is used in the creation of an invention, without providing a significant

> contribution to the conception of the invention, does not make that person an inventor.[129]

In conjunction with this Guidance, the USPTO published two illustrative examples of an inventorship analysis for [Gen]AI-assisted inventions applying these principles.[130]

The USPTO has further extended the logic of the above and imposed a requirement that the patent application should be rejected "for each claim for which an examiner or other USPTO employee determines from the file record or extrinsic evidence that at least one natural person, *i.e.,* one or more named inventors, did not significantly contribute."[131] This implicitly is to prevent a human inventor contributing only to one dependent claim in a patent application and coming out with patent rights over an entire set of claims, some of which may have been exclusively generated by GenAI.

c. What quality of prompt engineering is necessary to constitute a sufficient human contribution for copyrightability or patentability?

"Prompt engineering" is "the process of writing, refining and optimizing inputs to encourage generative AI systems to

[129] *USPTO Feb. 2024 AI-Assisted Invention Guidance, supra* note 6, at 10048–49.

[130] *See id.*, at 10045; Example 1: Transaxle for Remote Control Car, USPTO [hereinafter *USPTO Example 1*], *available at* https://www.uspto.gov/sites/default/files/documents/ai-inventorship-guidance-mechanical.pdf; and Example 2: Developing a Therapeutic Compound for Treating Cancer, USPTO [hereinafter *USPTO Example 2*], *available at* https://www.uspto.gov/sites/default/files/documents/ai-inventorship-guidance-chemical.pdf.

[131] *USPTO Feb. 2024 AI-Assisted Invention Guidance, supra* note 6, at 10048–49.

create specific, high-quality outputs."[132] As one provider of AI services describes:

> Prompt engineering is an iterative process. It's essential to experiment with different ideas and test the AI prompts to see the results. You may need multiple tries to optimize for accuracy and relevance. Continuous testing and iteration reduce the prompt size and help the model generate better output. There are no fixed rules for how the AI outputs information, so flexibility and adaptability are essential.[133]

Prompt engineering is an essential skill for leveraging the power of GenAI and may even become its own career field.[134]

Based on their respective AI Guidance publications to date, the USCO and the USPTO take vastly different approaches with respect to prompt engineering and whether it can suffice to support copyright or patent rights over the GenAI output therefrom.

i. Under the USCO's current guidance, no amount of prompt engineering can confer "human authorship" to any GenAI output.

The USCO's current guidance as of March 2023 strongly indicates that whatever level of human creativity may be

[132] *What is Prompt Engineering*, IBM, https://www.ibm.com/topics/prompt-engineering (last visited July 27, 2024).

[133] *What is Prompt Engineering*, AMAZON, https://aws.amazon.com/what-is/prompt-engineering/#:~:text=Prompt%20engineering%20is%20an%20iterative,optimize%20for%20accuracy%20and%20relevance (last visited July 27, 2024).

[134] Jack Kelly, *The Hot, New High-Paying Career Is An AI Prompt Engineer*, FORBES (Mar. 6, 2024), https://www.forbes.com/sites/jackkelly/2024/03/06/the-hot-new-high-paying-career-is-an-ai-prompt-engineer/.

expressed in developing a GenAI input confers no copyright protection rights to the GenAI output under copyright law. The USCO could not have been more definitive on this in stating:

> Based on the Office's understanding of the generative AI technologies currently available, users do not exercise ultimate creative control over how such systems interpret prompts and generate material.[135]

and

> Some [GenAI] technologies allow users to provide iterative 'feedback' by providing additional prompts to the machine. For example, the user may instruct the AI to revise the generated text to mention a topic or emphasize a particular point. While such instructions may give a user greater influence over the output, the AI technology is what determines how to implement those additional instructions.[136]

This reasoning is prominently reflected in the USCO's refusal in *Théâtre D'opéra Spatial* to register a piece of digital art created with the text-to-image GenAI tool Midjourney.[137] The copyright applicant explained he "input numerous revisions and text prompts at least 624 times to arrive at the initial version of the image."[138] The Review Board of the USCO found that the

[135] *USCO Mar. 2023 Guidance*, *supra* note 6, at 16192.

[136] *Id.* at n.30.

[137] Letter from U.S. Copyright Office Review Board to Tamara S. Pester, Re: Second Request for Reconsideration for Refusal to Register Théâtre D'opéra Spatial (SR # 1-11743923581; Correspondence ID: 1-5T5320R) (Sept. 5, 2023), *available at* https://www.copyright.gov/rulings-filings/review-board/docs/Theatre-Dopera-Spatial.pdf.

[138] *Id.* at 2. The USCO Review Board summarized the applicant's failed arguments regarding his creative process as follows:

work "contains more than a de minimis amount of content generated by artificial intelligence."[139] And because the applicant was "unwilling to disclaim the AI-generated material," the work "cannot be registered as submitted."[140]

As discussed above, the USCO will register a copyright only for any "human-authored aspects" of a GenAI-assisted work of authorship, consisting in effect of only revisions made by a human on top of an GenAI output.[141] For example, in February 2023, the USCO "concluded that a graphic novel comprised of human authored text combined with images generated by the

> [The applicant] asserts a number of arguments in support of his claim. He argues that his use of Midjourney allows him to claim authorship of the image generated by the service because he provided "creative input" when he "entered a series of prompts, adjusted the scene, selected portions to focus on, and dictated the tone of the image." [He] created a text prompt that began with a "big picture description" that "focuse[d] on the overall subject of the piece." He then added a second "big picture description" to the prompt text "as a way of instructing the software that [the applicant] is combining two ideas." Next, he added "the overall image's genre and category," "certain professional artistic terms which direct the tone of the piece," "how lifelike [the applicant] wanted the piece to appear," a description of "how colors [should be] used," a description "to further define the composition," "terms about what style/era the artwork should depict," and "a writing technique that [the applicant] has established from extensive testing" that would make the image "pop." He then "append[ed the prompt] with various parameters which further instruct[ed] the software how to develop the image," resulting in a final text prompt that was "executed . . . into Midjourney to complete the process" and resulted in the creation of the Midjourney Image []. *Id.* at 6.

[139] *Id.* at 1.

[140] *Id.*

[141] *See supra* Sec. III.A.2.a.

AI service Midjourney constituted a copyrightable work."[142] The USCO, however, held that "the individual images themselves could not be protected by copyright."[143] This was consistent with the USCO's position that prompt engineering cannot constitute a sufficient human contribution to convey ownership rights to the human prompter under copyright law.

ii. Under the USPTO's current guidance, prompt engineering apparently can, at least in theory, rise to the level of the "significant human contribution" required for patentability.

In contrast, according to the USPTO's current guidance, prompt engineering apparently *can* rise to the level of the "significant contribution" by a human required for patentability, at least in principle. This appears to be provided for in the USPTO's Guiding Principle 2 applying the *Pannu* joint inventorship factors to the sufficiency-of-human-contribution determination for [Gen]AI-assisted inventions, copied again below:

> 2. Merely recognizing a problem or having a general goal or research plan to pursue does not rise to the level of conception. A natural person who only presents a problem to an AI system may not be a proper inventor or joint inventor of an invention identified from the output of the AI system. *However, a significant contribution could be shown by the way the person*

[142] *USCO Mar. 2023 Guidance*, *supra* note 6, at 16191 & n.9 (discussing Letter from U.S. Copyright Office to Van Lindberg, Re: Zarya of the Dawn (VAu001480196) (Feb. 21, 2023), at 2, *available at* https://www.copyright.gov/docs/zarya-of-the-dawn.pdf).

[143] *Id.*

> *constructs the prompt in view of a specific problem to elicit a particular solution from the AI system.*[144]

But remarkably, neither the term "prompt engineering" nor the concept of iterative prompt development is specifically discussed or even hinted at throughout the USPTO's February 2024 or April 2024 Guidance publications beyond the above. Nor do either of the two illustrative examples provided by the USPTO provide *any* examples of prompt construction by itself, let alone of any iterative prompt engineering, supporting inventorship and patentability.[145] Instead, the USPTO presents only examples directed at the far more straightforward analyses that inventive conception or experimentation done before the GenAI is involved or on top of GenAI output can support patentability.[146] And they discuss Guiding Principle 2 primarily in the negative

[144] *USPTO Feb. 2024 AI-Assisted Invention Guidance, supra* note 6, at 10048–49 (emphasis added).

[145] *See USPTO Examples 1 & 2, supra* note 130.

[146] *See, e.g., USPTO Example 1, supra* note 130, at 6 (analyzing the inventorship of a hypothetical Claim 3, finding inventorship because the inventors "made significant alterations to the alternative design as a direct result of their experimentation"); *see also, e.g., USPTO Example 2, supra* note 130, at 5 (analyzing the inventorship of a hypothetical claim, stating: "While some of these contributions could be characterized as simply identifying a problem or reducing the output of DTIP to practice, Marisa and Naz made significant contributions to the conception of the invention. Namely, Marisa and Naz synthesized the drug compounds identified as candidates from the output of DTIP, characterized these drug compounds, and structurally modified the lead drug compound to create a novel therapeutic drug compound. Therefore, Marisa and Naz both significantly contributed to the conception of the claimed invention.").

to illustrate that the mere recognition of a problem does *not* rise to the level of conception.[147]

In contrast, in its April 2024 Guidance, the USPTO highlights as a specific example of insufficient human contribution to support patentability when "an AI system assists in the drafting of the patent application and introduces alternative embodiments which the inventor(s) did not conceive and [the] applicant seeks to patent."[148] But such prompt engineering *should*, at least arguably, suffice to constitute the requisite "significant human contribution" supporting patentability. If a patent applicant has claimed a patentable invention describing a particular embodiment, why is it inappropriate to prompt a GenAI to generate alternative (and at least arguably logically following from the invention) embodiments and claim they are also covered? Or if a patent applicant has claimed a genus claim, covering a range from X to Y, then why should it be inappropriate to prompt a GenAI tool to generate embodiments within that range to comply with the 35 U.S.C. § 112 enablement requirements as imposed by *Amgen v. Sanofi*?[149]

With the USPTO, however, taking the opposite position and the USPTO's Five Guiding Principles themselves collectively precluding several categories of prompts that might otherwise

[147] *USPTO Example 1*, *supra* note 130, at 3 (analyzing the inventorship of a hypothetical Claim 1, rejecting inventorship because the GenAI prompt the purported inventors constructed "is simply a restatement of [the] general problem" and thus they did not significantly contribute to the conception of the invention that was in fact generated by the AI).

[148] See USPTO Apr. 2024 AI-Based Tools Guidance, supra note 25, at 25615.

[149] 598 U.S. 594, 612 (2023). For a discussion of using GenAI in patent drafting to meet the *Amgen v. Sanofi* and the 35 U.S.C. § 112 enablement requirement and the risks of same posed by GenAI-assisted prior art generation, *see infra* Sec. V.B.

have supported patentability, it is difficult to conceive of an example where prompt engineering by itself would actually suffice in the eyes of the USPTO—particularly when the USPTO has not provided a single positive example affirming this principle to date.

B. *Issue No. 1(a): Will the courts adopt the USCO's and the USPTO's frameworks for sufficiency-of-human-contribution determinations for GenAI-assisted works of authorship and inventions?*

It should be treated as an open question whether the federal courts will adopt their sufficiency-of-human-contribution frameworks for GenAI-assisted works of authorship and inventions under the copyright and patent laws, as detailed in this section.

1. Can prompt engineering never confer rights to the resulting GenAI output under copyright law, as presumed by the USCO?

As noted above, the USCO's position against prompt engineering as potentially supporting copyrightability has not been affirmed in federal court to date.

Some may argue and the courts may hold that the USCO Review Board wrongly decided *Théâtre D'opéra Spatial* introduced above,[150] and that the 642 prompts that the applicant entered should be construed as entailing a level of creativity meeting the low bar that has been set for copyrightability in general. Under the Supreme Court's 19th century opinion in *Sarony* discussed above, a photograph can be copyrightable because the human photographer can act as the ultimate "mastermind" behind a

[150] *See supra* Sec. III.A.2.c.i.

photograph by adjusting the composition beforehand to be captured by the camera.[151] Might a GenAI-assisted digital work of art also be copyrightable by the same reasoning, due to an iterative set of prompts created by a digital artist? Or a GenAI-assisted software program developed under the iterative prompting of a software programmer?

At least one other court outside the U.S. has applied such legal reasoning under its country's copyright laws. In *Li v. Liu*, a Chinese court found copyright infringement of an image created using Stable Diffusion, another text-to-image GenAI tool.[152] The court upheld the copyright in dispute, providing a meticulous account of the prompt engineering used by the author to create the image and a thorough legal analysis supporting its conclusion that the author used Stable Diffusion only as a tool to *assist* in creating the work.[153]

[151] *See supra* note 18.

[152] Li v. Liu, Jing 0491 Min Chu No. 11279 (Beijing Internet Court A Nov. 27, 2023), *available at* https://english.bjinternetcourt.gov.cn/pdf/BeijingInternetCourtCivilJudgment112792023.pdf.

[153] *Id.* at 12–13. The Chinese court's reasoning included:

> Generally speaking, when people use the Stable Diffusion model to generate pictures, the more different their needs are and the more specific the description of picture elements, layout, and composition is, the more personalized the picture will become. In this case, there are identifiable differences between the picture involved and the prior works. In terms of the generation process of the picture involved, the plaintiff did not draw the lines himself, or instruct the Stable Diffusion model everything on how to draw the lines and do the colors; the lines and colors that constitute the picture involved are basically done by the Stable Diffusion model, which is very different from the conventional way of people using brushes or software to draw pictures. However, the plaintiff used prompt words to work on the picture elements such as the character and how to present it, and set parameters to

> work on the picture layout and composition, which reflects the plaintiff's choice and arrangement. The plaintiff input prompt words and set parameters and got the first picture; then he added some prompt words, modified the parameters, and finally got the picture involved. Such adjustment and modification also reflect the plaintiff's aesthetic choice and personal judgment. During the trial, the plaintiff generated different pictures by changing the prompt words or the parameters. One can infer that with this model, different people can generate different pictures by entering different prompt words and setting different parameters. Therefore, the picture involved is not a "mechanical intellectual achievement". Unless there is contrary evidence, it can be found that the picture involved is independently completed by the plaintiff and reflects the plaintiff's personalized expression. In summary, the picture involved meets the element of "originality". . . .
>
> . . .The generative AI technology has changed the way people create. Just like many other technological advances in history, the process of technological development is the process of outsourcing human work to machines. Before the advent of cameras, people needed superb painting skills to reproduce an object perfectly; then the cameras made it easier to record the image of an object. Nowadays, the camera of smartphones is getting better and easier to use. However, as long as the photos taken with a smartphone reflect the photographer's original intellectual investment, they will constitute photographic works and are protected by the Copyright Law. The development of technologies and tools require less human investment, but the copyright system should remain in use in order to encourage the creation of works. Before the emergence of the AI model involved, people needed to spend time and energy learning how to paint, or to consign others to paint for them. In the second scenario, the painter will draw the lines and fill in the colors upon the client's request to complete a work of fine art. And the person who draws is normally considered a creator. This is similar to the use of AI models to generate pictures, but there is one major difference here: the creator has his own will and he will use some judgment when painting for the client. Currently, the generative AI model

2. Did the USPTO apply the law correctly in adopting and applying the *Pannu* joint inventorship analysis as its framework?

    a. Does the Pannu joint inventorship analysis seamlessly apply to the GenAI-assisted invention context under patent law, as presumed by the USPTO?

In *Pannu*, the Federal Circuit held that if there are two or more purported human contributors to an invention, each must make a "significant contribution" to be considered an inventor.

The USPTO explicitly notes that "[a]lthough the *Pannu* factors are generally applied to two or more people who create an invention (*i.e.,* joint inventors), it follows that a single person who uses an AI system to create an invention is also required to make a significant contribution to the invention, according to the *Pannu* factors, to be considered a proper inventor."[154]

It is entirely possible, however, that the federal courts will ultimately decline to adopt the USPTO's *Pannu* framework and instead provide a different test. As the USPTO explicitly notes,

has no free will and is not a legal subject. Therefore, when people use an AI model to generate pictures, there is no question about who is the creator. In essence, it is a process of man using tools to create, that is, it is man who does intellectual investment throughout the creation process, the not AI model. The core purpose of the copyright system is to encourage creation. And creation and AI technology can only prosper by properly applying the copyright system and using the legal means to encourage more people to use the latest tools to create. Under such context, as long as the AI-generated images can reflect people's original intellectual investment, they should be recognized as works and protected by the Copyright Law.

[154] *USPTO Feb. 2024 AI-Assisted Invention Guidance*, *supra* note 6, at 10048.

its Guidance publications "do[] not constitute substantive rulemaking and do[] not have the force and effect of law."[155] It is the federal courts that have the authority to interpret the Patent Act and apply it to different and new situations, including the modern rise of generative AI. And Congress could step in at any time to define or change the standard through the passage of legislation.

For example, some may argue, and the courts may hold, that:

- The *Pannu* joint inventorship framework is inapposite because it was developed to address disputes between two or more human beings regarding their respective purported inventorship rights or lack thereof, not to determine when a human being has contributed to a GenAI-assisted invention enough to merit inventorship rights.[156] Instead, the key question under long-standing patent law should be whether the *human* inventor(s) conceived of every limitation in the claim(s) in comparison to the patent specification or other documented evidence, including by serving as the "mastermind" for any use of GenAI tool.
- The USPTO's application of the *Pannu* joint inventorship framework is predicated on the assumption that GenAI can *autonomously* replicate the human process of conception in a way that may otherwise confer

[155] *See, e.g.*, *id*. at 10045.

[156] As noted by one commentator, "[T]he USPTO's approach is not fully grounded in the law because it allows for patenting of an invention in a situation where no human or combination of humans fully conceived of and originated the invention. Rather, [the USPTO is] simply looking for at least one human who provided a significant contribution." Dennis Crouch, *Joint Inventorship: AI-Human Style*, PATENTLYO (Feb. 12, 2024), *available at* https://patentlyo.com/patent/2024/02/joint-inventorship-human.html.

inventorship rights under patent law if it were conceived by one or more humans. And the further assumption that adding such a "significant contribution" requirement is needed or else the USPTO would issue some patents that should not otherwise have issued. But neither assumption has been established by Congress or the courts.

- The *Pannu* "significant contribution" standard and the Five Guiding Principles presented by the USPTO to help inform its application is vague, exceedingly complicated, overly subject to interpretation by patent examiners,[157] and infeasible to comply with by patent applicants.[158] Such an ambiguous standard will be difficult if not impossible to apply consistently from case to case, examiner to examiner, or from USPTO technology center to technology center.
- The resulting uncertainty for the patentability of all GenAI-assisted inventions—which will comprise many if not most patent applications in the future—will be harmful for the U.S. patent system and U.S. innovation. The increased costs of prosecuting and litigating patents in terms of both money and time will discourage companies from applying for or enforcing patents in the first place, much like some would argue has already resulted from the rise of 35 U.S.C. § 101 patent subject-matter eligibility challenges since *Alice*.[159]

[157] For discussion, *see infra* Sec. III.C.2.

[158] For discussion, *see infra* Sec. III.D.3.b.

[159] For discussion, *see infra* Sec. IV.E.

It is important to note that joint inventorship issues are rarely explored during current USPTO patent examination practice.[160] Distinguishing between who invented what portion of an invention has historically not been of primary importance during patent examination, with the USPTO focusing instead on the question of whether the claimed invention qualifies for a patent in the first place.

The USPTO implicitly accepts that there may be some individuals who effectively free ride and get improperly named as joint inventors on any given issued patent. Some may argue that the resolution of any joint inventorship issues can and should be generally deferred by the USPTO to the federal courts, given the elevated investigatory, fact-finding, and credibility-determination requirements necessary for any such analysis.

But with the rise of GenAI-assisted inventions, such "human-plus-AI" joint-inventorship issues take on a very different dimension. It is less than clear that applying a "human-only" joint-inventorship analysis—which requires very little contribution to be included as an inventor—to this distinct AI context makes sense. Human-inventorship issues are at the heart of whether there are one or more patentable claims for AI-assisted inventions in the first instance, and any rulemaking involving their determination requires close scrutiny and due process.

[160] "Generally, the USPTO presumes those inventors named on the application data sheet [] or oath/declaration are the actual inventor or joint inventors of the application. However, examiners and other USPTO personnel should carefully evaluate the facts from the file record or other extrinsic evidence when making determinations on inventorship." *USPTO Feb. 2024 AI-Assisted Invention Guidance, supra* note 6, at 10048.

b. Did the USPTO appropriately apply principles of patent law in developing its Five Guiding Principles to apply the Pannu factors to GenAI-assisted inventions?

Nor should it be assumed that the courts will adopt the Five Guiding Principles the USPTO established to help inform the application of the *Pannu* joint inventorship factors to GenAI-assisted inventions.[161]

For example, some may argue that the phraseology of the USPTO's Guiding Principle 3 stating that "a natural person who merely recognizes and appreciates the output of an AI system as an invention . . . is not necessarily an inventor," improperly elevates "conception" to a requirement and demotes "reduction to practice" to insufficient to constitute a "significant" contribution by a human supporting patentability, effectively rewriting *Pannu* factor 1.[162] Such a change to the substantive patent law would fall outside of the USPTO's appropriate rulemaking authority and would be subject to future review by the courts and any future legislation by Congress.

And as discussed above, some would disagree with the USPTO's refusal to grant a patent when an applicant has "an AI system assist[] in the drafting of the patent application and

[161] *See supra* Sec. III.B.2.b.

[162] *See, e.g.,* American Bar Association, Intellectual Property Law Section, Letter to Under Secretary Vidal in response to Request for Comments: Inventorship Guidance for AI-Assisted Inventions (May 14, 2024), at 3 ("The Guidance reads out the "reduction to practice" from the first *Pannu* factor . . . ."), *available at* https://www.regulations.gov/comment/PTO-P-2023-0043-0051. The authors of this article cite to this Letter merely to provide one substantive critique raised by one organization in response to the USPTO's request for comment, without commenting on the merits.

introduce[] alternative embodiments which the inventor(s) did not conceive and [the] applicant seeks to patent."[163]

C. *Issue No. 1(b): Can the USCO's and the USPTO's frameworks for sufficiency-of-human-contribution determinations feasibly be applied . . . ?*

In contrast to most patent eligibility or qualification determinations by the USPTO pre-GenAI, the sufficiency-of-human-contribution determinations that the USCO and USPTO will have to make potentially for every copyright and in particular every patent application for GenAI-assisted works of authorship and inventions will require at least some degree of investigation, fact-finding, and even credibility determination.

How much of an investigatory role should the USCO and the USPTO take on with respect to this issue or in general as a matter of public policy?

1. . . . by USCO examiners?

Upon closer examination, implementing the USCO's framework of making copyright protections available only for the "human-authored aspects" of a GenAI-assisted work of authorship requires an examination process that is only marginally more substantive, if at all, than that to which the USCO is accustomed.

Based on the standard the USCO has adopted, examiners are not required to tease out of any purported work of authorship what part is attributable to human contribution from what part is attributable to GenAI contribution. As discussed above, the USCO's bright-line rule preempts any such requirement: *any*

[163] For discussion, *see supra* Sec. III.A.2.c.ii.

GenAI output is simply not copyrightable according to the USCO.[164]

It is critical to note, however, that were the federal courts or Congress to require the USCO to change its current stance and instead allow copyrightability of the direct GenAI output resulting from prompt engineering in certain circumstances, then the situation would be completely different. Copyright examiners would be thrust into the position of making a challenging substantive determination to figure out from a given GenAI output what portion is attributable to the human contributor and whether that contribution suffices to support rights to that contributor under copyright law. That would raise serious questions as to whether the USCO and its examiners can feasibly make such determinations.

But applying the USCO's current standard, such a determination is fairly straightforward. If a copyright applicant specifically identifies and discloses "the inclusion of AI-generated content" in a work submitted for registration and the applicant's "human [] contributions to the work," as broadly required under the USCO's March 2023 Guidance,[165] then the USCO has the information it needs to make an informed copyright qualification determination.

2. . . . by USPTO examiners with respect to separating out human contributions from GenAI-assisted inventions . . .

Of the different avenues the USPTO has framed by which GenAI can be implicated in the GenAI-assisted inventive process, separating out the human contributions from the GenAI

[164] For discussion, *see supra* Sec. III.A.2.c.i.

[165] *USCO Mar. 2023 Guidance*, *supra* note 6, at 16193.

contributions is relatively straightforward for most of them. For the examiner to evaluate whether there was a "significant contribution" by a human being from either designing, building, or training an AI system "in view of a specific problem to elicit a particular solution from the AI system" (USPTO Guiding Principle 4) or by modifying or conducting a successful experiment on the AI outputs (Guiding Principle 3),[166] all that may be needed is a sworn statement by the applicant along with any supporting evidence. In each of the above scenarios, the human being(s) may be presumptively acting as the "mastermind" to either create the specialized GenAI tool or to use the GenAI output as *part* of their inventive process.

However, for an applicant to establish the requisite "significant contribution [] by the way the person constructs the prompt in view of a specific problem to elicit a particular solution from the AI system" (Guiding Principle 2) is a far more challenging analysis. And one that remains completely undefined by the USPTO, as examined in detail below.

a. . . . even with complete GenAI-input/output records?

Trying to distill the human contributions from the GenAI contributions for inventive works is far more complicated than for works of authorship. Any sufficiency-of-human-contribution determination for GenAI-assisted inventions is inherently labor intensive and likely beyond the skill, training, and time made available for patent examiners, even if access to all material records is presumed.

There is no clear cut "before" and "after" that a patent applicant can provide for GenAI-assisted inventions in general,

[166] For discussion, *see infra* Sec. III.A.2.b.

particularly those involving multiple GenAI-input/output sessions across multiple prompt engineers and over an extended period of time. The safest and perhaps only way for the applicant to ensure compliance may be to disclose a complete record of *all* relevant GenAI-input/output sessions. Such an approach may theoretically be the only way for the applicant to fully discharge its duty to disclose "all information material to patentability" under 37 C.F.R. § 1.56 in at least some cases.

But even if patent examiners receive such a fulsome disclosure from the applicants, they would likely not have the time or the means to review them fully and accurately. In many cases, the complete record of GenAI inputs/outputs likely would be too voluminous and complicated for examiners to effectively review.

Moreover, such a sufficiency-of-human-contribution analysis should in principle be done on a claim-by-claim basis, and this is in fact what the USPTO requires in its February 2024 Guidance.[167] Such a requirement, however, further compounds any issues of infeasibility for the patent examiner. Patent examiners are now required to parse out what contributions to the invention were made by the human inventor(s) for a GenAI-assisted invention to a far greater degree of specificity than has ever been expected of patent examiners for non-GenAI-assisted inventions.

[167] *USPTO Feb. 2024 AI-Assisted Invention Guidance*, *supra* note 6, at 10048 ("[A] rejection under 35 U.S.C. 101 and 115 should be made for each claim for which an examiner or other USPTO employee determines from the file record or extrinsic evidence that at least one natural person, *i.e.*, one or more named inventors, did not significantly contribute.").

b. . . . or particularly with limited access to the relevant GenAI-input/output records?

The likely presumption, though, is that USPTO examiners will *not* have access to all material GenAI inputs and outputs in many cases. Maybe most cases. Perhaps even in the vast majority of cases as GenAI becomes incorporated into more inventive processes for companies.

It may be practically unreasonable to expect patent applicants to identify, let alone disclose, all relevant repositories of GenAI inputs/outputs to any given inventive process. Not without extensive efforts. And not without potentially unduly impeding the product development lifecycle efforts themselves, whose primary purpose (for everyone except perhaps the company's IP counsel) is to develop actual products and services; not to file for patents. It is easy to establish corporate policies nominally requiring researchers and engineers to collect all material GenAI inputs and outputs. There may be practical limitations, however, to successfully implementing them.

The more of a quasi-judicial role patent examiners are expected to play with respect to sufficiency-of-human-contribution determinations, the more examiners will be required to conduct investigations with respect to any undisclosed material GenAI-input/output records. But fact-finding and credibility determinations are generally best left to the litigation process and the courts, and with good reason.

Unlike the USCO, the USPTO has considerable experience with conducting substantive analyses during examination, including the prior art invalidity analyses under 35 U.S.C. §§ 102 and 103 core to any patent examination and patent subject-matter eligibility analyses under 35 U.S.C. § 101.

But patent examiners have available to them, at least in theory, a significant amount of information relevant to each of these analyses during the examination process, independent of any disclosures by the applicant. Prior art is largely publicly available, and examination time is primarily reserved for searching for and reviewing the relevant prior art. And as challenging and unpredictable as Section 101 subject-matter eligibility analyses are, so long as the applicant accurately captures the nature of the claimed invention, the examiner has all that is needed to conduct the analysis based primarily on the contents of the application itself and the guidance on Section 101 issues from the federal courts and the USPTO.

This is far from the case for any sufficiency-of-human-contribution determination for GenAI-assisted inventions. This inherently requires nonpublic, ephemeral records and information that are primarily if not exclusively within the control of the applicant.

D. *Issue No. 1(c): Can the USCO's and USPTO's frameworks for sufficiency-of-human-contribution determinations feasibly be complied with by GenAI-assisted copyright and patent applicants?*

Does the duty to disclose as currently framed by the USCO and the USPTO with respect to sufficiency-of-human-contribution determinations for AI-assisted copyright and patent applicants properly balance the examiners' need for information with what can be feasibly collected and disclosed by the applicants?

1. The USCO and the USPTO have taken contrasting approaches to the applicant's duty of disclosure for GenAI-assisted works of authorship or inventions.

The USCO and USPTO have taken vastly different procedural approaches to the specificity of guidance they provide regarding required disclosures of the use of AI by copyright and patent applicants.

a. The USCO only requires disclosure of any inclusion of GenAI-generated content and a brief explanation of the human author's contributions.

The USCO has assumed more of a quasi-judicial role with respect to these GenAI-assisted issues than it has carried out in its copyright examination process historically. In its March 2023 guidance, the USCO explicitly requires:

- "a duty to disclose the inclusion of AI-generated content in a work submitted for registration," and
- "a brief explanation of the human author's contributions to the work."[168]

The USCO provides the following guidance for how to submit applications for works containing AI-generated material:

> For example, an applicant who incorporates AI-generated text into a larger textual work should claim the portions of the textual work that is human-authored. And an applicant who creatively arranges the human and non-human content within a work should fill out the "Author Created" field to claim: "Selection, coordination, and arrangement of [describe human-authored content] created by the author and [describe AI content] generated by artificial intelligence."[169]

[168] *USCO Mar. 2023 Guidance*, *supra* note 6, at 16193.

[169] *Id.*

b. The USPTO imposes a detailed duty of disclosure for GenAI-assisted inventions.

In contrast, the USPTO, through its February 2024 Guidance, explicitly initially *disclaimed* the need for any new or specific disclosure requirement for GenAI use in the inventive process.[170] Instead the USPTO highlighted only the existing "duty to disclose all known information that is material to patentability" under 37 C.F.R. § 1.56, noting in rather contradictory, bureaucratic fashion:

> At this time, to meet their duty of disclosure, applicants rarely need to submit information regarding inventorship. The USPTO does not believe this inventorship guidance will have a major impact on applicants' disclosure requirements. However, special care should be taken by those individuals subject to this duty to ensure all material information is submitted to the USPTO to avoid any potential negative consequences.[171]

The USPTO's Guidance further noted in continued bureaucratic fashion:

> Generally, the USPTO presumes those inventors named on the application data sheet or oath/declaration are the actual inventor or joint inventors of the application. However, examiners and other USPTO personnel should carefully evaluate the facts from the file record or other extrinsic evidence when making determinations on inventorship. When the facts or evidence indicates that the named inventor or joint inventors did

[170] *USPTO Feb. 2024 AI-Assisted Invention Guidance*, *supra* note 6, at 10049.

[171] *Id.*

> not contribute significantly to the claimed invention, *i.e.*, their contributions do not satisfy the *Pannu* factors for a particular claim, a rejection under 35 U.S.C. 101 [] is appropriate.[172]

But in its subsequent April 2024 Guidance, the USPTO quietly pivoted to providing meaningful guidance, giving actual examples of what use-of-AI information it would consider to be "material."

i. Under its April 2024 Guidance, the USPTO now requires detailed disclosures down to the level of *specific* material [Gen]AI tools used.

The USPTO's April 2024 Guidance added to its duty of disclosure guidance for the first time the italicized language below:

> While there is no per se requirement to notify the USPTO when AI tools are used in the invention creation process or practicing before the USPTO, applicants and practitioners should be mindful of their duty of disclosure. *This is, if the use of an AI tool is material to*

[172] *Id.* at 10048.

> *patentability as defined in 37 CFR 1.56(b),*[173] *the use of such AI tool must be disclosed to the USPTO.*[174]

The USPTO's clarification might seem minor or obvious, but it is anything but. It forecloses the use of any empty "the applicant used AI tools common to the practice"-type disclosure statements; instead, the applicant is required to specify each individual AI tool it used that was "material to patentability."

Furthermore, given the newness and inconsistency in use of terminology related to AI, additional guidance as to what constitutes an "AI tool" subject to mandatory disclosure—and potentially subsequent invalidation of any issued patent where there was a failure to disclose such AI tool during the

[173] 37 C.F.R. § 1.56(b) states:

> (b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and
>
> > (1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or
> >
> > (2) It refutes, or is inconsistent with, a position the applicant takes in:
> >
> > > (i) Opposing an argument of unpatentability relied on by the Office, or
> > >
> > > (ii) Asserting an argument of patentability.
>
> A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

[174] *See USPTO Apr. 2024 AI-Based Tools Guidance*, *supra* note 25, at 25615 (emphasis added).

application process—is simply necessary.[175] What constitutes "material to patentability" in this context?

For example, as noted above, the use of GenAI drafting tools like Grammarly poses some interesting questions in the specific context of drafting patent applications, where the turn of a phrase can dramatically impact the scope of a patent claim.[176] Should disclosure of all such GenAI drafting tools, which have also been built into the latest versions of Microsoft Word and Google Docs, be disclosed? Should issued patents later be invalidated for any failure to do so? If there are multiple inventors, does each need to be surveyed on this specific issue and the specific GenAI drafting tools they use?

More specific guidance is needed as to what AI tools are and are not "material." And some form of safe harbor should be built in for certain good-faith technical failures to comply, to prevent these human inventorship issues for GenAI-assisted inventions from becoming even more of a trap for the unwary than they already promise to be.

ii. The USPTO's April 2024 Guidance disclosure requirement effectively shifts the burden of proof onto the applicant.

Compliance with the USPTO's April 2024 Guidance's new rule compelling the disclosure of all material AI tools used by the applicant logically will operate as an admission that any AI tool so disclosed was material to the conception and/or reduction-to-practice of the invention.

[175] For discussion of the importance of the definition of AI terms, *see supra* Sec. II.A.

[176] For discussion, *see id*.

The USPTO's rule surreptitiously shifts the burden of proof for patentability onto the applicants. Instead of the USPTO and the patent examiner bearing the burden of proving applicants do not qualify for a patent—as has been the case for every issue of patentability in the history of USPTO patent examination—GenAI-assisted patent applicants thus effectively bear the burden of affirmatively proving they made a "significant contribution" to establish their inventorship rights. From any such disclosure of material AI tools used, the USPTO examiner would be able, if not compelled, to follow up and inquire about how the applicant used any given listed AI tool and what portion of the claimed invention was conceived by that AI tool.

And even if such follow-up does not happen during the examination process itself, the disclosure (or lack thereof) of the use of such AI tools is on record for any future litigation. This provides a spotlight during any future litigation on any record keeping (or lack thereof) the patent applicant maintained of the use of such AI tools during the invention process or disclosed (or not disclosed) during the application process.

iii. Under its April 2024 Guidance, the USPTO also requires detailed disclosures down to the level of *specific* [Gen]AI inputs/outputs.

Further evidencing the abrupt shift of the burden of proof imposed by the April 2024 Guidance described above, the Guidance immediately followed with another example requiring potentially expansive disclosures down to the GenAI input/output level:

> For example, as discussed in more detail in the Inventorship Guidance for AI-Assisted Inventions, material information could include evidence that a named inventor did not significantly contribute to the invention

> because the person's purported contributions were made by an AI system. This could occur where an AI system assists in the drafting of the patent application and introduces alternative embodiments which the inventor(s) did not conceive and [the] applicant seeks to patent. If there is a question as to whether there was at least one named inventor who significantly contributed to a claimed invention developed with the assistance of AI, information regarding the interaction with the AI system *(e.g., the inputs/outputs of the AI system)* could be material and, if so, should be submitted to the USPTO.[177]

Such a requirement may logically follow in at least some cases, from the duty to disclose "*all* known information that is material to patentability" under 37 C.F.R. § 1.56 (emphasis added). In particular, if the applicant claims that its prompt engineering was a primary basis supporting patentability (under the USPTO's Guiding Principle 2), then it is difficult to imagine how any meaningful sufficiency-of-human-contribution determination can be made without going down to the AI input/output level.

iv. The USPTO's April 2024 Guidance expands the duty to disclose "all information material to patentability" well beyond any prior application of the duty.

But the USPTO does not uphold or apply 37 C.F.R. § 1.56 to its fullest extent for every issue of patentability.

[177] *USPTO Apr. 2024 AI-Based Tools Guidance*, *supra* note 25, at 25615 (emphasis added).

Based on long-standing patent law judicial precedent and USPTO examination practice, all patent applicants have a duty to disclose to the USPTO only material information they are "*aware*" of.[178]

While Rule 1.56 "materiality" is not limited to prior art, prior art is in practice the primary focus of both the patent examiner and the patent applicant regarding the applicant's duty to disclose. The first thing that the patent office "encourages" applicants to carefully examine to discharge their duty of disclosure is "prior art cited in search reports of a foreign patent office in a counterpart application."[179] In addition to presumptively being more likely to be material, another underlying reason to focus on foreign counterpart application disclosures, etc., is because they are publicly available. Patent examiners are fully capable of finding such prior art themselves, but the USPTO appropriately puts the burden on applicants to organize this information for its examiners.

There is a further duty to disclose any other prior art the applicant is aware of, in its files or otherwise, that are material to patentability. But as a practical matter, patent examiners do not investigate whether an applicant has failed to disclose any such other prior art. Nevertheless, patent applicants are generally incentivized to search for and disclose all relevant prior art in their files, in part because of the possibility of being immediately caught red-handed if they somehow slip up on the above obligation.

[178] MPEP § 2001.06 (Sources of Information under 37 CFR 1.56) (R-07.2022) (citing Brasseler, U.S.A. I, L.P. v. Stryker Sales Corp., 267 F.3d 1370, 1383 (Fed. Cir. 2001).

[179] MPEP § 2001 (Duty of Disclosure, Candor, and Good Faith (R-08.2017).

Patent applicants, however, have no duty to conduct any independent prior art search in conjunction with their application. As stated above, it is *not* the patent applicant's duty to prove that its application is patentable over the prior art; it is instead the patent examiner's burden to prove that the application is *not* patentable over the prior art. This makes sense for at least two reasons:

1. Requiring the patent applicant to prove its application is patentable would be akin to requiring the applicant to prove a negative.
2. All prior art is by definition publicly available and can theoretically be independently found by the patent examiner by conducting a prior art search during examination.

Unlike for the prior art qualification and patent subject-matter eligibility determinations discussed above,[180] however, "public use" (e.g., a prefiling prototype demonstration to solicit investment) and "on-sale bar" (i.e., a prefiling offer for sale of a product or service that embodies the invention) disqualification determinations under 35 U.S.C. § 102(a)(1) rely on information that was not necessarily made available to the general public. Public use or on-sale bar disclosures are often made confidentially. Any full analysis of such disqualifying behaviors by the patent applicant would require access to private recorded communications and information which for all intents and purposes is exclusively within the control of the applicant.

The likely presumption is that there are at least some cases where the USPTO grants patents that would not have been granted had applicants faithfully met their duty to disclose disqualifying public use or on-sale bar information during the

[180] For discussion, *see supra* Sec. III.C.2.a–b.

patent application process. Nevertheless, as a practical matter, patent examiners are not expected to fully investigate these issues during examination or to police compliance with the duty of disclosure of all information material to them. These issues are tacitly left to the courts to be developed through discovery, as needed, during any future litigation.

Human-inventorship determinations for GenAI-assisted inventions are far closer to "public use" and "on sale bar" disqualification determinations and are far more removed from invalidity and Section 101 subject-matter eligibility analyses in this regard. The only information the patent examiner will have relevant to these issues is that which the patent applicant discloses.

It should be an open question whether a higher level of disclosure by applicants for sufficiency-of-human-contribution determinations should be required than for public use and on-sale bar determinations at the patent examination stage, or whether the patent system as a whole would benefit more from deferring more of that determination to any future litigation. Particularly where, as with this issue, the USPTO's expansive application of Rule 1.56 threatens to impose a potentially undue burden for at least some patent applicants[181] and compounds the already heightened uncertainty around patentability for GenAI-assisted inventions both during patent examination and during any enforcement actions taken in the future. This has serious potential implications on the level of investment that companies, in particular startups and small and medium enterprises, are willing to make in developing any patent portfolios, and on the health of our overall patent system and our entire economy.[182]

[181] For discussion, *see infra* Sec. III.D.3.b.

[182] For discussion, *see infra* Sec. IV.E.

On the other hand, others may argue that such a disclosure requirement *can* be reasonably attainable for all companies and should be a necessary cost of business for a properly functioning patent system for the AI Age.

2. Can the burden of proof for patentability be properly shifted under patent law for any issue?

But it should be treated as an open question whether the burden of proof for patentability can under any circumstances—whether as a direct or indirect result of a USPTO's de facto substantive rulemaking or as a natural and unintentional result of a technological advancement that undercuts the very concept of human inventorship—be shifted under patent law.

The entire patent system is predicated upon the concept that the burden of proof is on the patent examiner to prove a lack of patentability, not on the applicant to prove patentability. This goes hand in hand with the duty of disclosure under 37 C.F.R. § 1.56 requiring the applicant to disclose "all information material to patentability."

Whether the required disclosure of inputs and outputs of the specifically identified GenAI system used should be maintained in the USPTO guidance or any later rulemaking should also be treated as an open question. Otherwise, the tension between the longstanding interpretation of the *limited* duties imposed under Rule 1.56 and the unprecedented and burdensome requirements of the USPTO's Guidance publications threatens to be untenable in practice for both patent examiners and applicants.

3. Can the duties of disclosure for GenAI-assisted works of authorship and inventions be feasibly complied with. . .

   a. . . . by copyright applicants?

There is no reason copyright applicants cannot comply with the USCO's duty-of-disclosure requirements for GenAI-assisted works of authorship if they maintain basic recordkeeping practices.

If the applicant records just the final GenAI output that it used as the basis for and edited or transformed to create the final work of authorship for which it seeks copyright registration, then it likely has most or all of the "before" information—the noncopyrightable GenAI-output that the applicant is obligated to specifically disclaim in its application—that it needs. And the final work of authorship that is the subject of the copyright application (the "after") can be compared with the AI-generated portion, with the applicant providing a narrative explanation as to what the human contributed and the creative thinking behind it.

The same works in reverse when the GenAI contribution is on the back end. If the applicant creates a traditional work of authorship and then uses GenAI editing tools to edit it, then the "before" and "after" records are just as easily identified, collected, and disclosed. All the applicant has to do is start with the final GenAI output for the work of authorship for which the applicant is applying for copyright protections and work backwards from there.

b. . . . by patent applicants for all information material to sufficiency-of-human-contribution determinations?

i. Documenting the relative contributions made to any inventive process is challenging and has not historically been required of the patent applicant.

There is nothing straightforward about most inventive processes. In many cases the owner does not know until after the fact (i.e., when the invention was "reduced to practice") when the inventive process began or ended, which individuals contributed, or which of the multiple pathways taken were fruitful and which were irrelevant. And there is even less of a clear connection between the inventive process, the ultimate claimed invention itself, and the text of the patent claims as originally drafted by the applicant's patent agent/attorney and then as ultimately revised to their final issued form.

Fortunately, for both patent applicant and patent examiner, there has historically been next to no call for the disclosure of any lab notebooks and the like for patent examination. That has been almost entirely the province of any future patent litigation, which is naturally limited only to already issued patents.

This is again all consistent with the patent applicant not bearing any burden of proof for patentability before the USPTO. It is further consistent with the separate fundamental patent law precept regarding 35 U.S.C. § 103 nonobviousness determinations stating that "[p]atentability shall not be negated by the manner in which the invention was made."

ii. Identifying and disclosing all material GenAI input/output records is uniquely challenging.

By extension, even the most diligent, rule-following patent applicant will struggle to comply with the USPTO's mandate to identify, collect, and disclose all GenAI input/output records material to a GenAI-assisted invention.

Determining on an individual basis which GenAI inputs/outputs are relevant to a sufficiency-of-human-contribution determination, let alone are material, is a complicated analysis. Prompt engineering is an iterative process potentially conducted across multiple sessions. There may not be a clear-cut single successful prompt engineering session; the claimed patent may well be the sum of multiple sessions. And there may have been other prompt engineering sessions carried out earlier and by multiple other people that were relevant to the ultimately successful prompt engineering sessions.

Should patent applicants be expected to secure legal counsel to interview every engineer, collect all relevant prompt engineering session GenAI-input/output records, analyze each for materiality, and then organize them for disclosure to the USPTO for each GenAI-assisted patent application? Is it reasonable to expect applicants to bear litigation-scale expenses up front during every patent application process to comply with such duties of disclosure as imposed by the USPTO? And at possible penalty of a finding of unenforceability due to inequitable conduct, sanctions, and even disbarment of the patent attorney or agent from the USPTO for any purported failures?

The USPTO's new and expansive application of the 37 C.F.R. § 1.56 duty of disclosure of "information material to patentability" impacts the individual rights and obligations of patent applicants to such a degree that it can only be reasonably interpreted as a "substantive rule," requiring compliance with the APA before implementation.[183]

More guidance from the USPTO is required here. Even if provided, questions about the feasibility for companies to comply with any duty to disclose all material GenAI input/output records will likely remain.

E. We need a better system for making sufficiency-of-human-contribution determinations.

Litigating sufficiency-of-human-contribution issues in any future enforcement action will presumptively be extremely expensive for the same reasons as stated above. This is an extremely complicated and fact-intensive exercise. And it is less than clear how any such future litigation of this issue might be made more efficient from any quasi-judicial determination of the same made by the USPTO after the imposition of the duties of disclosure as described above.

All stakeholders in the patent system should be concerned that the policy objectives underlying the current copyright and patent legal regimes might not be attainable in the incipient AI Age. These sufficiency-of-human-contribution issues for GenAI-assisted works of authorship and inventions fall outside of the framework of current IP regimes. And continued attempts to squeeze them into the existing framework may expose and enlarge the cracks within it.

The IP legal system and society have an immediate need for representatives of all stakeholders on these issues to come together and develop policies and procedures for key AI & IP issues, including:

[183] *See supra* Sec. II.B.1.

- a clear sufficiency-of-human-contribution standard for establishing human inventorship for GenAI-assisted copyright and patent applications,
- a reasonable procedure for applicants to meet this standard, and
- a reasonable procedure for future defendants against enforcement actions based on any issued copyrights or patents to challenge whether this standard has been met.

We need consensus, nonpartisan principles and best practices for complying with these issues that, if adopted in whole or in part, would result in more effective and efficient resolution of any such human-inventorship disputes for GenAI-assisted inventions—which will soon comprise most all inventions and patent applications in the future.

SUMMARY OF KEY QUESTIONS

(1) Has an existing or imminent need regarding GenAI-assisted works of authorship or inventions that might call for any change in established patent law or procedures been established and clearly defined in the first place?

(2) Have the USCO and USPTO issued de facto substantive rules in their recent Guidance publications on AI regarding sufficiency-of-human-contribution determinations for GenAI-assisted works of authorship or inventions, in violation of the Administrative Procedure Act?

(3) Regarding copyright law, is the USCO's bright-line stance against prompt engineering serving as the basis for copyrightability over GenAI output for GenAI-assisted works of authorship correct (i.e., will the federal courts adopt it?)?

(4) Regarding patent law:

(a) Is the USPTO's Pannu joint inventorship framework the correct foundation that should be applied for sufficiency-of-human-contribution determinations for GenAI-assisted inventions (i.e., will the federal courts adopt it?)? Or is it predicated on the assumption that GenAI can autonomously replicate human conception in a way that may otherwise confer inventorship rights under patent law if it were conceived by one or more humans—a presumption that has not been established by the courts or by Congress to date?

(b) Did the USPTO properly apply other principles of patent law on top of its Pannu joint inventorship framework to develop its February 2024 Guidance's Five Guiding Principles for GenAI-assisted inventions?

(i) In its April 2024 Guidance, did the USPTO effectively shift the burden of proof for patentability onto the patent applicant?

(ii) Can the burden of proof for patentability be properly shifted to the patent applicant under patent law?

(c) Can the USPTO's overall sufficiency-of-human-contribution determination framework for GenAI-assisted patent applications feasibly be carried out by patent examiners? Or feasibly complied with by patent applicants?

(d) Will the resulting uncertainty for the patentability of all [Gen]AI-assisted inventions—which will comprise most patent applications in the foreseeable future—be harmful for the U.S. patent system and for U.S. innovation?

IV. ISSUE NO. 2: ARE GENAI-ASSISTED SOFTWARE CODING AND AI SOFTWARE INNOVATIONS AT RISK OF SLIPPING THROUGH THE CRACKS OF THE IP LEGAL REGIMES?

Software programs and innovations have historically posed unique challenges for any IP analysis, which are significantly compounded when GenAI-assisted software coding or AI/software innovations are at issue.

A. Software lies somewhere in between the existing IP legal regimes.

There are no less than eight categories of "works of authorship" defined in U.S. copyright law.[184] And one of these categories—literary works—itself spans various categories of works expressed in text, from poems to (apparently) computer programs and software code.[185]

Software has been described as having "a permanently unstable place in the country's IP system because every conception of its nature has failed to advance the commercial and personal needs of all the stakeholders involved."[186]

[184] *See* 17 U.S.C. § 102(a).

[185] The copyrightability of software code was not established as of the passage of the Copyright Act of 1974. The Computer Software Copyright Act of 1980 subsequently amended the Copyright Act to include a definition for "computer programs," but without specifying where it fits within the eight categories of works of authorship enumerated in 17 U.S.C. § 102. Computer programs would appear to best fit under the category of "literary works." Pub. L. No. 96-517, 94 Stat. 3015, 3028 (1980). *See* Apple Comput., Inc. v. Franklin Comput. Corp., 714 F.2d 1240 (3d Cir. 1983) (interpreting 17 U.S.C. § 102(a) as classifying computer programs as "literary works" and holding that both the human-readable source code and the machine-readable object code forms of software are protectable by copyrights).

[186] GERARDO CON DIAZ, SOFTWARE RIGHTS: HOW PATENT RIGHTS TRANSFORMED SOFTWARE DEVELOPMENT IN AMERICA 279 (Yale Univ. Press 2019).

Is software best understood as only the written code—a mere sequence of coded instructions (e.g., is the relationship between software programs and general-purpose computers analogous to that of piano rolls to automatic piano players, with neither patentable because neither fundamentally change the devices that run them?)?[187] This generally describes the view, championed by IBM back in the first decades of computing, that software should not be patentable.[188] And if so, is software best understood as the source code as written by the programmer or as translated into its machine-readable object code form and distributed on (and stolen from) floppy disks, CD-ROMs, and now by online download, or both? [189] Either way, if software is just written text, then protecting software by copyright law would make sense.[190]

Or is software best understood as a "machine control element" generated by the computer's processing of the object code that transforms a general-purpose computer into a new

[187] *See id.* at 110–11.

[188] IBM made the same argument with respect to the punched-card operated Jacquard looms of the nineteenth century, which inspired the creation of punched-card computers. According to IBM, an individual deck of punch cards providing step-by-step instructions for a particular fabric design may be copyrightable in the same way that a "gifted mathematician" can express "highly original computational methods in a series of digital computer program cards," but neither should be patentable. *Id.* at 111–12.

[189] The answer under the current copyright law is that both source code and object code are protectable by copyright law. The USCO requires copyright applications to be submitted in the human-readable source code form. But the copyright protections extend to the translated machine-readable object code form in which the software program can be "sold" (or rather licensed) as well, which is deemed the same "expression" as the original source code form under copyright law.

[190] *See* CON DIAZ, *supra* note 186, at 111–12.

specific device?[191] Should software be treated as "radically different from any other subject matter" ever to fall under the purview of copyright, because computer programs are not just written software coding text but also *simultaneously* are "machine-control elements," and thus should be patentable?[192]

If so, then patent protections are more applicable.

The first conception of software has primarily carried the day since the advent of the software industry in the 1960s and 70s.[193] These same issues, however, often resurface with new developments in technology and in IP law, most recently with the rise (and fall) of business-method patents leading up to the Supreme Court's seminal 2014 ruling in *Alice*.

Like business-method patents, artificial intelligence is also often computer-implemented, i.e., implemented in software. GenAI raises new aspects of the same fundamental issues on 35 U.S.C. § 101 patent subject-matter eligibility that have been argued time and again over the last century with respect to software patents. The authors of this article respectfully submit that a deeper understanding of these fundamental issues—some of which seem to have been lost over time—is important for the continuing principled development of the case law on software patents.

[191] *See id.* at 132–34.

[192] *See id.* (describing the position of Robert O. Nimtz, who represented Bell Labs in the seminal U.S. Supreme Court software patenting case *Gottschalk v. Benson*, 409 U.S. 63 (1972)).

[193] *See id.* at Chapter 6 (Remaking Software Copyright, 1974-1981), 122–38. IBM led the antisoftware patenting view, which was uniquely consistent with its own self-interests. IBM benefited from bundling its hardware and software in the early years of computing; any advent of software patents would have allowed its competitors an avenue for cutting into IBM's monopoly power. *Id.*

*****

Software has never fit well within the framework of the existing IP regimes. Patents? Maybe, but challenges against software as ineligible abstract ideas under 35 U.S.C. § 101 loom paralyzingly large.[194] Federal Circuit Judge William Bryson explained post-*Alice* that:

> [software] patents, although frequently dressed up in the argot of invention, simply describe a problem, announce purely functional steps that purport to solve the problem, and recite standard computer operations to perform some of those steps. The principal flaw in these patents is that they do not contain an "inventive concept" that solves practical problems and ensures that the patent is directed to something "significantly more than" the ineligible abstract idea itself. As such, they represent little more than functional descriptions of objectives, rather than inventive solutions. In addition, because they describe the claimed methods in functional terms, they preempt any subsequent specific solutions to the problem at issue. It is for those reasons that the Supreme Court has characterized such patents as claiming "abstract ideas" and has held that they are not directed to patentable subject matter.[195]

Trade secrets? As discussed below, trade secrets are simply inapplicable for "on-premises" software—the dominant means by which software was sold for the first four or five decades of the software industry's history—which is inherently public (i.e., *not* secret).

[194] For discussion, *see supra* Sec. II.C.2.b.

[195] Loyalty Conversion Sys. Corp. v. American Airlines, Inc., 66 F.Supp.3d 829, 845 (E.D. Tex. 2014) (internal citations omitted).

Copyrights? Unlike all other copyrightable works of authorship, people want software not for its form of expression (which copyrights can protect), but for its function (which copyrights cannot protect).[196] Nobody buys software for the beauty and elegance of its software coding.

B. *Software program source code and object code: why they are valuable, and how the IP regimes protect them.*

There are a variety of reasons that software code is valuable and should be protected.

1. Object code is the form of software programs that is pirated.

Before the rise of the internet and cloud computing in the 21st century, computing primarily entailed local computer servers running locally installed software. The object code for such on-premises software is licensed by its owner to the customer to be installed and used on the customer's system. As such, the software is easily pirate-able. Copyright protections are the primary if not sole line of defense for owners against piracy of such software.

Asserting copyright protections and filing a copyright infringement suit, in particular after federal copyright registration, serves as an important deterrent to any wide-scale piracy in this model.[197] In this way, software has had more historically in common with (other) "literary works," with stopping

[196] "A 'computer program' is a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result." 17 U.S.C. § 101 (Definitions).

[197] Copyright protections are generally a better deterrent to wide-scale software piracy than any existing patent protections, because enforcing copyrights is far simpler.

rampant piracy serving as the primary goal for both. The software industry hit the ground running with the threat of piracy from its inception in the 1970s.[198]

Registering with the U.S. Copyright Office any software that has significant commercial value worth protecting was a practical necessity under the on-premises software model. But as discussed in detail below, this is less and less the case with the rise of the software-as-a-service (SaaS) model.

2. Source code is the form of software programs that can be exploited.

Even though it is not typically for sale or made available to any end user, it is the source code, not the object code, form of software programs that are considered the crown jewels of any software company. Source code is human-readable, written in a computer programming language that programmers can read, understand, and modify. The source code is translated as necessary into machine-readable object code form that can be distributed to and installed on computer systems to run the program. Human programmers cannot read, understand, or modify such object code.

With access to the source code, programmers can potentially:

- identify and remove any antipiracy protections coded into the program in question,

[198] *See* Bill Gates, *An Open Letter to Hobbyists*, Homebrew Computing Club Newsletter, Vol. 2, Iss. 1 (Feb. 3, 1976) (imploring the industry to stop sharing, free of charge, any programs they acquired or developed, including one of Microsoft's earliest programs), *available at* https://archive.org/details/hcc0201/Homebrew.Computer.Club.Volume.02.Issue.01.Len.Shustek/page/n1/mode/2up?view=theater.

- identify security vulnerabilities in the program, and exploit them by:
    - hacking into the system and accessing confidential business data, personal information, etc.,
    - inserting viruses, etc.,
- develop extensions or other software programs that can interface with the original program, e.g., through application programming interfaces (APIs),
- learn from the programming techniques used, and
- identify useful portions of program's source code and incorporate them into other programs.

Source code is readily protectable as a trade secret (whereas object code is not when it is openly distributed). While a software program's source code is also protectable by copyright, source code cannot be reverse-engineered from the object code form of the program that is distributed to the public under the on-premises software model, so source code can and is readily kept secret. And neither source code nor object code is distributed or made available to customers under the SaaS software model in the ordinary course.[199]

If the source code is made publicly available, however, as in the case of open-source software, it cannot be protected by trade secret; for the most part such software would only be protectable under copyright law.

[199] For discussion, *see infra* Sec. IV.C.3.

C. *GenAI-assisted software coding is becoming standard practice, but its protectability under current copyright law is entirely uncertain.*

Many aspects of the job of software coding are tailor-made for GenAI applications. GenAI tools can mimic or replicate more and more of the abilities of human programmers. They can "provide increased efficiencies in ideation, debugging, testing, and optimizing, among other things, which decreases coding time, expense, and investment, while freeing human developers to focus on uniquely human and creative aspects of the coding design and creation process."[200]

Furthermore, in the vision of the AI Age, everyday individuals may even become their own app developer, building personal tools tailored to their own workflows and needs using GenAI software programming tools.

Despite its growing importance and the amount of time and expertise that can be entailed in developing it, it is simply not clear if and when GenAI-assisted software coding is protectable under current copyright law.

1. Will clear standards be set for identifying the "human-authored aspects" of GenAI-assisted works of authorship and protecting them under copyright law?

One thing that can generally be presumed about the protectability of AI-software coding is that if a coding goal is presented as a single AI input and the AI-generated software code output

[200] Cisco Systems, Inc., *Copyrights, Generative AI, and the Tools of Human Ingenuity* (June 2024) at 2, (unpublished manuscript, presented at The Sedona Conference on AI and the Law, Part 2: AI and IP Law) (on file with authors).

is implemented into the software product in its entirety, then it is not copyrightable.[201]

But some may argue that copyright law protects or should be amended to protect GenAI-assisted software coding as the expressions of human authors as the "mastermind," in at least some cases, with copyrightability arising from, e.g.,

1. "human-made arrangements and modifications of materials generated by AI systems,"
2. "submitting a prompt that is independently copyrightable as a text-based work to a GenAI system to produce an output that is an independently copyrightable derivative work," or
3. "modifications made by a GenAI system of a human author's pre-existing copyrighted work."[202]

Based on the USCO's strict stance that only "human-authored aspects" of a GenAI-assisted work of authorship are copyrightable, copyright protections are available only for the portions of any GenAI-assisted software code that are human generated.

In practice, however, will owners be able to de facto enforce such copyright protections over the entirety of their software programs, including those portions that are AI-generated in some cases? Or will the pendulum swing the other way such that owners practically have no ability to protect any GenAI-assisted software programs, including even any human-authored aspects?

Should a duty be imposed requiring the owner to specify the precise code that was AI generated and to separately identify

[201] *See supra* Sec. III.A.2.a.

[202] *Cisco Systems*, *supra* note 200, at 6.

the "human-authored" code when registering for copyright with the USCO? The USCO's present guidance, issued in March 2023, goes a step toward this direction, but it is not yet clear how close or far.[203]

Until new legislation or court decisions from the federal appellate courts addressing these questions are issued, they will all be heavily litigated in any forthcoming copyright infringement suits where GenAI-assisted software code is in dispute. And if the courts ultimately do not adopt the USCO's strict stance, then complicated sufficiency-of-human-contribution determinations may become necessary in every copyright case, as it already will be in every GenAI-assisted patent case.

There will be considerable uncertainty in the marketplace while all of this gets worked out. If a company has no software patent coverage (as can generally be presumed due in large part to the extreme uncertainty of the patentability of software inventions and enforcement of software patents under patent law)[204] and it is ultimately determined the company also has no copyright protections over its GenAI-assisted software programs, then what can the company do to protect them? If, for example, a former employer or partner misappropriates a company's software program source code and publishes it, the company may have limited to no legal recourse against any member of the public who then downloads and uses it for any purpose.

[203] For discussion, *see supra* Sec. III.A.2.a.

[204] For discussion, *see supra* Sec. II.C.2.b.

2. Even if copyrightable, will the functional reverse-engineerability of GenAI-assisted software coding render software copyrighting obsolete?

The main reason a reputable company would want to have access to another company's source code is to be able to develop compatible extensions or other programs with the target software program. But should the company instead wish to directly compete with the other company and its software program in the market, then the rise of GenAI greatly facilitates the development of competing software programs.

"Clean-room design" is a functional reverse-engineering method that has been widely recognized and used as a means to avoid copyright infringement. A team examines the copyrighted software code in question and architects it. Then another team uses only the architecture provided and creates new software code to implement it. The copying of the functions of any target software program is entirely fair game and not protectable by copyright. And the particular protectable expression of the original software code in effect has been "laundered out," so to speak.

Historically, the primary disincentive against using this method has been how labor-intensive software coding has been. That cost, however, has already been and will continue to be reduced dramatically due to the rise of GenAI and its application to generating software code. The primary remaining constraints will be:

- Can GenAI replace human software coders in practice and still maintain the required level of performance? and
- Can GenAI-assisted software also avoid incorporating code that can be easily breached?

3. Most AI software is provided under the software-as-a-service (SAAS) model, which further reduces the utility of copyright protections.

Another reason copyright protections are less significant in the AI Age is that most modern AI services and software are and will be provided via software-as-a-service (SaaS).

Cloud computing has allowed for the growth of the SaaS model, where the program is run on the service provider's systems and the customer accesses the output of the software service via a web application over the cloud. No software is transferred for the core program provided as SaaS, so no copyright license is required. The customer does not have access to any software code to the core program that he or she could pirate. Instead, the customer only subscribes to the SaaS typically on a monthly or annual basis.

The efficacy of registering for copyright protection is thus further reduced in the SaaS context. The software for the web applications used to access the output of the SaaS may still be transferred (typically today by download), but such web apps are far less likely to be of stand-alone commercial value.

In the SaaS model, the core AI software program is never transferred in any form—either in object code form or in source code form. As such, straight up piracy of the SaaS software by the customer is impossible under the SaaS model, unlike for the on-premises software model of the recent past.

4. The risk of GenAI incorporating copyleft protected software code, potentially rendering GenAI-assisted software uncopyrightable

Using generative AI to generate software code gives rise to a unique copyright risk that all companies should be aware of.

The software community has a unique and proud tradition of crowdsourcing for open-source software: publicly available source code that anyone can inspect, modify, and incorporate into his or her own code. Each open-source software has its own licensing terms, with some named open-source licensing terms like Apache, MIT, BSD, and Unilicense well-known in the market. Contrary to popular misunderstanding, open-source software is not by definition "free." Instead, it can and often is incorporated into closed (i.e., proprietary) software, for commercial sale.

But one particular category of open-source software, cheekily named "copyleft" software, is an exception. Copyleft licensing terms are described as "viral," because they require all derivative works incorporating copyleft code to also be released under a copyleft license. One of the most commonly used copyleft licenses is the GNU General Public License.

This gives rise to a possible scenario where generative AI incorporates excerpts of copyleft open-source software in its training, only to have the software that it generates theoretically rendered unprotectable because of it. The enforceability of such viral copyleft provisions has not been fully tested in court in any context, let alone the GenAI context. So, it is difficult to confidently conduct any assessment of this risk, other than to know it is more than zero.

Companies wanting to directly mitigate such risk should take steps to prevent their GenAI from accessing any source code repositories that are protected by copyleft protections.

D. The "rise" of trade secrets to protect software in the AI Age?

Theft of any software provided under the SaaS model, which is likely used by most commercially valuable AI services software, is most likely to fall under the umbrella of trade secret misappropriation, where the thief had access to the software either as an employee or a partner of the service provider's company.

Should the legally required "reasonable measures" to protect the secrecy of the AI software source code be properly maintained, then a trade secret misappropriation claim will be the main avenue for protecting the AI owner's rights—and it is a potent protection at that. Software source code lends itself exceptionally well to being protected as a trade secret because it is not made available to customers or to the public in the ordinary course. Companies typically take extensive measures to protect the source code of their core software programs.

At least some GenAI software—including that of large language models (LLMs)—has additional advantages with respect to trade secret protectability, including the use of proprietary data sets to train their AI models and the hyperparameters that data scientists manually set before training an AI model. Neither can be readily reverse-engineered. If, e.g., the reports that OpenAI has only about five patent applications are correct,[205] then we can presume that OpenAI believes it can protect its LLM technology through trade secrets.

This has serious implications for any efforts to regulate or audit any GenAI for validity, reliability, or bias by the government or any third party. The quid pro quo for patent protection is the public disclosure of the technology, which facilitates both understanding and regulation. The ability to protect any

[205] *See IBM leads Google and Microsoft as race to next generation AI heats up*, IFI CLAIMS PATENT SERVS. (Feb. 6, 2023), *available at* https://www.ificlaims.com/news/view/pr-generative-ai.htm.

technology—including one as powerful and far-reaching as GenAI—as a trade secret limits any efforts to regulate it.[206]

But while the AI software provider's source code can generally be kept safe and any theft of it is protectable in court, the same threat of functional reverse-engineering by GenAI that can be implemented by competitors to evade copyright protections[207] can also be used to get around at least some trade secret protections. Trade secret law only protects innovations that cannot be independently reverse-engineered.

If a competitor successfully reverse-engineers a software program's functions without directly misappropriating any information from the owner through espionage, etc., then the owner has no trade secret or copyright claims against them. The last form of IP that would provide any recourse in this case would be from patent law, but only if the owner invested in and successfully obtained one or more patents to protect the innovations in the first place.

[206] *See, e.g.*, An Act Concerning Consumer Protections in Interactions with Artificial Intelligence Systems, Colo. Senate Bill 24-205 (May 17, 2024), *available at* https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf. As drafted, this Colorado AI Act appears to exclude any required disclosure by developers (which includes LLM providers) of *any* trade secrets. *See* Sec. 6-1-1702 (Developer duty to avoid algorithmic discrimination – required documentation), subsection (6) ("Nothing in subsections (2) to (5) of this section requires a developer to disclose a trade secret . . . ."). But any algorithmic discrimination is presumptively a product of the data sources upon which the GenAI model was trained and/or the GenAI model itself, both of which are trade secrets. And any internal effort to mitigate against algorithmic discrimination also likely itself constitutes a trade secret.

[207] *See supra* Sec. IV.C.2.

E. *To support the growth and protection of the AI industry in the U.S., clear and consistent guidance on 35 U.S.C. § 101 patent subject-matter eligibility for software/AI inventions is needed.*

Patent protections are the gold standard for the protection of intellectual property, at least for the twenty-year period while they are effective in the U.S. And they will continue to be the gold standard in our incipient AI Age, but only to the extent they are obtainable and enforceable in the first place. When the USPTO issues a patent, the owner gains the right to exclude others from using the patented technology, even when independently developed. Any company that has potentially patentable software/AI technology and the budget for the patent prosecution process should explore the possibility of seeking patent protection for its own benefit or for that of any investors or future acquirors.

Nonetheless, anecdotally, the GenAI-focused startup companies and investors of today view patent protections as far more as "nice to have but really unnecessary" than the "must have" of technology startups of the past. Many are not even exploring the possibility of starting or developing a patent portfolio, due to the high costs and uncertainties of filing for patents and in particular of enforcing them.

This may simply be a rational market response to how the patent system has struggled in recent years—in general and in particular in the software industry—to fulfill its objective of "promot[ing] the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive rights to their respective writings and discoveries" as required by the U.S. Constitution.[208]

[208] U.S. CONST., art. I, § 8, cl. 8. For discussion of the challenges of securing software patents, *see supra* Sec. II.C.2.b.

For many software/AI inventions, patent applicants bear a heightened burden to establish their invention is eligible for patent protection under 35 U.S.C. § 101 that is not borne by applicants for inventions in most other technologies.

1. The manufactured paradoxes of the software invention and now the AI invention

It is contrary to most of the fundamental precepts of inventions and patent law that a given software program when run on a general purpose computer to carry out a particular function is presumptively (however rebuttably) *not* patent eligible, whereas a special purpose computer hardwired to carry out that exact same function *is* presumptively patent eligible.[209] The opposite and far more rational principle equating both for purposes of patent eligibility was in fact expressly adopted by the Federal Circuit in *In re Alappat*, a case involving a method claim on applying a mathematical formula to smooth out the waveform of an oscilloscope (e.g., a heart monitor display) to provide a clearer picture.[210] The Federal Circuit expressly noted that

[209] Dressing up a software patent in the guise of an equivalent hardware patent to evade the "mental steps doctrine," i.e., the "abstract ideas/mental processes" judicial exception, is a strategy going back at least to Bell Labs in its patent on Error Detecting and Correcting System, U.S. Patent No. 2,552,629 (1951). *See* CON DIAZ, *supra* note 186, at 20–23. Was this yet another example of evading § 101 or other patent law principles through gamesmanship by the applicant's patent attorneys, as appears to have a point of emphasis of recent Supreme Court patent law decisions? *See* Alice Corp. Pty. Ltd. V. CLS Bank Int'l, 573 U.S. 208, 226 (2014) ("This Court has long "warn[ed] . . . against" interpreting § 101 "in ways that make patent eligibility 'depend simply on the draftsman's art.'"). Or was it a necessary strategy to protect one's inventions as required by a patent system that has struggled to remain on principled grounds on these patent subject-matter eligibility issues for software inventions?

[210] *In re* Alappat, 33 F.3d 1526, 1540 (Fed. Cir. 2008).

"certain types of mathematical subject matter, standing alone, represent nothing more than abstract ideas until reduced to some type of practical application."[211] The court, however, held the method claim at issue "is not a disembodied mathematical concept which may be characterized as an 'abstract idea,' but rather a specific machine to produce a useful, concrete, and tangible result."[212]

And yet this paradoxical inconsistency is the logical result of the creation and application of "exceptions"—in particular for "abstract ideas"—that the Supreme Court identified in *Alice* as the "basic tools of scientific and technological work" and thus excluded from patentability.[213] The USPTO developed its framework for 35 U.S.C. § 101 patent subject-matter eligibility analyses for method claims in 2014,[214] based on its interpretation of U.S. Supreme Court and Federal Circuit case law, namely *Alice*[215] and its application of the Court's earlier ruling in *Mayo Collaborative Services v. Prometheus Laboratories*.[216]

[211] *Id.* at 1543.

[212] *Id.* at 1544. *In re Alappat,* however, was abrogated along with *State Street Bank v. Signature Financial Group* in *In re Bilski*, 545 F.3d 943, 954 (Fed. Cir. 2008) (*aff'd in relevant part by* Bilski v. Kappos, 561 U.S. 593 (2010)). In *State Street Bank,* the Federal Circuit declined to create a "business method patent exception" to 35 U.S.C. § 101 patent subject-matter eligibility. State Street Bank and Trust Co. v. Signature Fin. Grp., 149 F.3d 1368, 1375 (Fed. Cir. 1998). In *Bilski,* the Federal Circuit declined to adopt the "useful, concrete, and tangible" result inquiry from the *Alappat* and *State Street Bank* line of cases in its holding that a business-method patent was not eligible for patent protection under 35 U.S.C. § 101. *Bilski*, 545 F.3d at 949.

[213] *Alice*, 573 U.S. at 216 (quoting Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 569 U.S. 576, 589 (2013).

[214] USPTO July 2024 Sect. 101 Updated Guidance, supra note 71.

[215] *Alice*, 573 U.S. at 208.

[216] Mayo Collaborative Servs. v. Prometheus Labs. Inc., 566 U.S. 66 (2012).

Applying the USPTO's *Alice*/*Mayo* framework, any software program analysis that "can be done in the human mind" is presumptively (though rebuttably) *not* patentable. The Supreme Court explained the policy justification of this in *Alice* as follows: "[The] monopolization of those tools through the grant of a patent might tend to impede innovation more than it would tend to promote it."[217] This all led to the Supreme Court's seminal holding in *Alice*—"the mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention."[218]

Necessity, however, is the mother of invention. Most inventions are conceived to replace any and all human efforts. When the human effort that is replaced is physical human labor, then that innovation is presumptively patent eligible. But when the human effort in question is "mental processes," the presumption is flipped under this "abstract idea" exception created and developed by the U.S. federal courts going back to the Supreme Court's seminal opinion in the telegraph patent case *O'Reilly v. Morse* in 1854.[219]

The invention and development of computers—from early computers hardwired for only specific calculations to the first general purpose computers that can be programmed with individual software to carry out a variety of functions replicating human mental processes—has brought about our modern

[217] *Alice*, 573 U.S. at 216 (quoting *Mayo* at 71).

[218] *Id.* at 223.

[219] *Id.* at 216 ("We have long held that [35 U.S.C. § 101] contains an important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable. We have interpreted § 101 and its predecessors in light of this exception for more than 150 years.") (citing Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 569 U.S. 576, 589 (2013) and Bilski v. Kappos, 561 U.S. 593, 601–02 (2010)).

Information Age. And yet, software inventions are particularly vulnerable to this "abstract ideas"/"mental processes" judicial exception. Software programs running on a general purpose computer routinely execute mathematical calculations, classification schemes, etc., that can otherwise be carried out in the human mind.

Artificial intelligence, including GenAI, is a continuation of this same inexorable march of technological process. GenAI is designed to replicate more advanced functions of the human mind, including creative processes and problem solving, and carry them out better and faster than any human ever could alone. In theory, GenAI relies less and less on any direction by its human programmers. Instead, it can take in new data and autonomously "figure out" how to modify its own model to make better predictions. This is a higher-level mental process at the problem solving level, but the law does not distinguish this from lower-level computational mental processes. All mental processes are equally presumptively ineligible for patent protections under the current articulation of the USPTO's *Alice/Mayo* Section 101 framework, if they can be "practically done in the human mind" and/or "with the aid of a pen and paper."[220]

2. Steering the patent law into the Information and the AI Ages

The rapid pace of technological development into the Information and now AI Ages has outpaced the U.S. patent law's ability to protect it. The metaphor of the extensive efforts required for and slow responsiveness when turning an ocean liner is an apt one here, as the development of the law on patent subject-matter eligibility under 35 U.S.C. § 101 reflects. This is

[220] *USPTO July 2024 Sect. 101 Updated Guidance*, *supra* note 71, at 58136.

particularly the case here where conflicting policy goals are implicated between such software patents and other method patents in other technological areas such as medical diagnostics and business methods. Both the federal court case law and the USPTO guidance on Section 101 patent subject-matter eligibility of all method claims—including those for software inventions—have vacillated between expansion and contraction, including over the last decade-plus since *Alice*.

a. The increased bias against the 35 U.S.C. § 101 patent subject- matter eligibility for software inventions from the Supreme Court in Alice (2014)

The Supreme Court's 2014 opinion in *Alice* constraining business-method patents was pivotal in pushing the pendulum back toward contraction. The *Alice* court adopted the two-step framework from *Mayo* for determining whether claims are directed to a patent-ineligible concept,[221] which the USPTO subsequently adopted in its Guidance publications.[222]

The Supreme Court's framework inherently disfavors software/AI inventions from patent eligibility because:

1. In Step 1 [i.e., Step 2A – prong 1 from the USPTO's framework[223]], it presumes that all claims directed to an abstract idea are presumptively not patent eligible. The Court further stated: "In any event, we need not labor to delimit the precise contours of the 'abstract ideas' category in this case."[224]

[221] *Alice*, 573 U.S. at 208.

[222] For discussion, *see infra* Sec. IV.E.2.b.

[223] *Id*.

[224] *Alice*, 573 U.S. at 221.

Given the breadth of the terms "directed to" and "abstract idea," the impact of this lack of definition is to make many software/AI claims presumptively *not* patent eligible.

2. In Step 2 [i.e., Step 2A – prong 2 from the USPTO's framework[225]], the Court examined whether "'additional [claim] elements [other than the abstract idea] transform the nature of the claim into a patent-eligible application."[226]

   The Court hinted at, but did not make explicit, a possible rule that a claim directed to an abstract idea might be transformed into a patent-eligible application if it "improve[s] the functioning of [a] computer itself" or if it "effect[s] an improvement in any other technology or technical field."[227]

   In the absence of the Court making this an explicit rule, the express holding of *Alice* that "method claims, which merely require generic computer implementation, fail to transform [] abstract idea[s] into a patent-eligible invention" casts a long shadow against any such transformation for software inventions.

[225] For discussion, *see infra* Sec. IV.E.2.b.

[226] *Alice*, 573 U.S. at 217.

[227] *Id.* at 225–26 ("Viewed as a whole, petitioner's method claims simply recite the concept of intermediated settlement as performed by a generic computer. The method claims do not, for example, purport to improve the functioning of the computer itself. Nor do they effect an improvement in any other technology or technical field. Instead, the claims at issue amount to 'nothing significantly more' than an instruction to apply the abstract idea of intermediated settlement using some unspecified, generic computer.").

b. The increased bias against the 35 U.S.C. § 101 patent subject-matter eligibility for software inventions from USPTO policy and procedure

In the immediate years after *Alice*, the USPTO issued a series of guidance and memoranda focused on individual Federal Circuit decisions applying the Supreme Court's *Alice/Mayo* test.[228] This approach proved "impractical" over time, as the "growing body of [Federal Circuit] precedent ha[d] become increasingly difficult for examiners to apply in a predictable manner, and concerns ha[d] been raised that different examiners within and between technology centers may reach inconsistent results."[229] This led to the USPTO issuing its *2019 Revised Patent Subject Matter Eligibility Guidance*, in which the USPTO "extract[ed] and synthesiz[ed] key concepts identified by the courts as abstract ideas."[230]

As noted above, in the 2023 Executive Order on AI, the Biden Administration ordered the USPTO to consider issuing updated guidance to USPTO patent examiners and applicants on patent eligibility to address innovation in AI and critical and emerging

[228] U.S. Patent and Trademark Office, 2019 Revised Patent Subject Matter Eligibility Guidance, 84 Fed. Reg. 50, 51 (Jan. 2019) [hereinafter *USPTO Jan. 2019 Revised Sect. 101 Guidance*], *available at* https://www.federalregister.gov/documents/2019/01/07/2018-28282/2019-revised-patent-subject-matter-eligibility-guidance#citation-5-p51.

[229] *Id.* at 52.

[230] *Id.* In this *Jan. 2019 Revised Sect. 101 Guidance*, the USPTO modified its original *Alice/Mayo* two-step framework to account for subsequent Supreme Court and Federal Circuit opinions holding that some patent claims were *not* "directed at" judicial exceptions even though they involved judicial exceptions. This gave rise to the convoluted "Step 2A – prong 1," "Step 2A – prong 2," and "Step 2B" nomenclature in the USPTO's Section 101 Guidance publications since then and referenced throughout this article.

technologies.[231] The USPTO has now complied, issuing in July 2024 its *Guidance Update on Patent Subject Matter Eligibility, Including on Artificial Intelligence*.[232]

In Section III of this July 2024 Guidance, the USPTO "provides an update on certain areas of the USPTO's subject-matter eligibility guidance that are particularly relevant to AI inventions, including: (1) whether a claim recites an abstract idea [Step 2A – prong 1]; and (2) whether a claim integrates a recited judicial exception into a practical application because the claimed invention improves the functioning of a computer or another technology or technical field [Step 2A – prong 2]."[233]

i. Does the claim "recite" an "abstract idea" (Step 2A – prong 1)?

Most software/AI claims "recite" an "abstract idea." As such, they are presumptively ineligible for patent protection under the framework provided by the USPTO for subject-matter eligibility determinations.

According to the USPTO's July 2024 updated guidance, patent examiners "must draw a distinction between a claim that 'recites' an abstract idea (and thus requires further eligibility analysis) and one that merely involves, or is based on, an abstract idea."[234] The USPTO's guidance for Step 2A – prong 1 consists primarily of providing three new illustrative hypothetical examples focused on AI[235] and additional examples from Federal Circuit cases "that do and do not recite an abstract idea,"

[231] *See supra* Sec. II.C.2.b.

[232] *USPTO July 2024 Sect. 101 Updated Guidance*, *supra* note 71.

[233] *Id.* at 58131.

[234] *Id.* at 58134.

[235] *See USPTO July 2024 Sect. 101 Examples 47-49*, *supra* note 71.

organized by the USPTO's three groupings of abstract ideas (as originally presented in the USPTO's October 2019 Guidance[236]):

1. mathematical concepts,
2. certain methods of organizing human activity, and
3. mental processes.[237]

For the last "mental processes" grouping, the USPTO further organized its discussion of Federal Circuit cases into the following subtopics:

- i. "A claim with limitation(s) that cannot practically be performed in the human mind does not recite a mental process."
- ii. "A claim that requires a computer may still recite a mental process."
- iii. "A claim that encompasses a human performing the step(s) mentally with the aid of a pen and paper recites a mental process."[238]

The primary if not exclusive avenue for software claims to pass Step 2A – prong 1 is if the claimed functions "cannot practically be performed in the human mind" and thus do not "recite" an "abstract idea"/"mental process." One example of this is presented in the USPTO's Section 101 Example 39 ("Method for Training a Neural Network for Facial Detection"), which expressly presents the training of a neural network—a framework of machine learning algorithms that work together to classify inputs based on a previous training process—as patent eligible.[239] The USPTO reasons that the hypothetical claim does not

[236] *USPTO Oct. 2019 Sect. 101 Updated Guidance*, *supra* note 73.

[237] *USPTO July 2024 Sect. 101 Updated Guidance*, *supra* note 71, at 58134.

[238] *Id*.

[239] *See USPTO Subject matter eligibility*, *supra* note 71, at 8–9.

recite any of the judicial exceptions under Step 2A – prong 1.[240] This is because the preprocessing claim element of "applying one or more transformations" including "mirroring, rotating, smoothing, or contrast reduction" to digital facial images "cannot be practically performed in the human mind."[241]

But for the many software/AI inventions whose claimed functions carry out a "mental process" that otherwise *can* be "performed by a human mind," the USPTO effectively presumes they are ineligible under Step 2A – prong 1. This may be rebuttable if the conditions under Step 2A – prong 2 or Step 2B are met as discussed in the next subsection. But it is still a de facto presumption of ineligibility for all such software claims.

[240] *Id.*

[241] *Id.* One study has found that USPTO examiners have reportedly been disproportionately rejecting on Section 101 grounds claims directed to training AI models with a structure similar to the cited example. *See IPO AI Patenting Handbook*, *supra* note 69, at 36 (citing a study of 200 recent AI-based patent applications that were rejected under 35 U.S.C. § 101 for office actions issued between Jan. 1 to Sept. 30, 2023, of which 30 applications that include claims directed to training AI models were rejected).

How much of this high rejection rate for those software/AI patent applications is inherent to the differences in technologies? How much may be attributable to more software/AI patent applications whose claimed software functions *can* be "practically performed in the human mind" and thus *do* "recite" an "abstract idea"/"mental process," unlike the claim in Example 39? And how much is due to less principled reasons, such as inaccurate or unclear standards or guidance from the courts or the USPTO, or the failure of patent examiners to comply with its own standards and even illustrative examples?

ii. Is the claimed "abstract idea" integrated into a "practical application" of the judicial exception (Step 2A – prong 2)?

According to the USPTO's July 2024 updated guidance, if the patent examiner determines a claim recites a judicial exception in Step 2A – prong 1, the examiner then evaluates "whether the claim as a whole integrates the recited judicial exception into a practical application of the exception, and thus is not 'directed to' the judicial exception in [Step 2A – prong 2]."[242] Patent examiners evaluate this by:

1. "identifying whether there are any additional elements recited in the claim beyond the judicial exception(s)," and
2. "evaluating those additional elements individually and in combination to determine whether they integrate the exception into a practical application of that exception."[243]

The USPTO's updated guidance specifically notes that "[m]any claims to AI inventions are eligible as improvements to the functioning of a computer or improvements to another technology or technical field."[244] This has also been referred to as "the search for a technological solution to a technological problem."[245] The USPTO further notes that "[w]hile the courts have not provided an explicit test for how to evaluate the

[242] *USPTO July 2024 Sect. 101 Updated Guidance*, *supra* note 71, at 58136.

[243] *Id.*

[244] *Id.* at 58136–37.

[245] *Id.*

improvements consideration, they have instead illustrated how it is evaluated in numerous decisions.[246]

The USPTO guidance continues:

> A key point of distinction to be made for AI inventions is between a claim that reflects an improvement to a computer or other technology described in the specification (which is eligible) and a claim in which the additional elements amount to no more than (1) a recitation of the words "apply it" (or an equivalent) or are no more than instructions to implement a judicial exception on a computer, or (2) a general linking of the use of a judicial exception to a particular technological environment or field of use (which is ineligible).[247]

and

> An important consideration in determining whether a claim improves technology is the extent to which the claim covers a particular solution to a problem or a particular way to achieve a desired outcome, as opposed to merely claiming the idea of a solution or outcome.[248]

In conjunction with its *July 2024 Updated 101 Guidance*, the USPTO has published three new illustrative hypothetical examples (Examples 47-49), each of which includes a discussion of the "improvements to functioning of a computer or other technology" consideration.[249]

[246] *Id*. The USPTO Guidance directs examiners to MPEP sections 2106.04(d)(1) and 2106.05(a) for these decisions and a detailed explanation of how USPTO personnel should evaluate this consideration. *Id.*

[247] *Id.* at 58137.

[248] *Id*.

[249] *USPTO July 2024 Sect. 101 Examples 47-49*, *supra* note 71.

Any increase in emphasis on this consideration by the courts and the USPTO should push the pendulum more toward the expansion of Section 101 patent subject-matter eligibility for software/AI inventions. But it is still built on the USPTO's *Alice/Mayo* framework, in which many software inventions are presumptively not patent eligible.

c. Should the USPTO continue to play a quasi-judicial role for Section 101 determinations for software and now AI inventions?

The USPTO has been at least in part laudably attempting to proactively address a significant gap in existing law and procedure with its regular guidance updates regarding 35 U.S.C. § 101 patent subject-matter eligibility, including its most recent July 2024 updated guidance on Section 101 and AI inventions. But the following should still be treated as open questions:

- Has the USPTO been exceeding its authority through issuing its Section 101 guidance updates?[250] Has the USPTO crossed the line from issuing "interpretations" of Supreme Court and Federal Circuit law to issuing "substantive rules," when, e.g.:
    - issuing its 2014 and January 2019 Guidance publications establishing its two-step *Alice/Mayo* framework (which in effect put a thumb on the scales against software and other method patents)?
    - issuing its October 2019 and July 2024 Guidance publications (which arguably

[250] For analogous discussion in the sufficiency-of-human-contribution determination for AI-assisted inventions context, *see supra* Sec. II.B.1.

have pushed the pendulum in the direction
of expanding software patent eligibility)?

These questions would be mooted if the federal courts or Congress would establish more explicit and comprehensive guidance addressing these Section 101 issues of law and procedure.

3. The broader implications of Section 101 patent subject-matter eligibility issues on the development of the AI industry in the U.S.

The ongoing uncertainty surrounding patent subject-matter eligibility for software/AI inventions has important implications for the U.S. economy. Historically, the patent system has provided an important avenue for smaller companies to compete with larger ones.

With the issuance of the USPTO's July 2024 updated guidance, will potential software/AI patent applicants have more confidence in their prospects for securing and being able to enforce patents on their inventions? As noted above, the USPTO's rejection rate on Section 101 grounds for AI patent applications has been historically on the order of 2-3 times higher than the average for all technologies, coming in at 77 percent for AI inventions in the first half of 2024.[251] This unequivocally discourages companies from investing in filing for patent applications in the AI space.

It is hard to say what percentage would be consistent with what one should reasonably expect in a properly functioning patent system in the AI space, but common sense dictates that it should be far closer to zero than to the recent Section 101 rejection rate of 77 percent. Even the average 24 percent Section 101

[251] *See supra* Sec. II.C.2.b.

rejection rate across all technologies may be higher than it should be. Given the time, energy, and costs required to file a basic patent application, it is safe to say that the vast majority of potential patent applicants will not file if they believe there is over a 3-in-4 chance that their application would be rejected as entirely ineligible. In a healthy patent system, every applicant should have a high degree of confidence of whether their invention is patent eligible—i.e., whether the USPTO, after conducting a prior art search finds the patent application novel and non-obvious, would issue the patent. If it were truly an objective analysis based on publicly known and understood standards available to all for software/AI inventions, then there would be far more certainty than the current Section 101 rejection rate reflects.

Such a high rate of patent eligibility rejections at the patent application stage is further compounded by the fact that even if the applicant clears the eligibility bar and the novelty and other bars and secures an issued patent from the USPTO in the first place, all of these issues are reviewed again by the federal courts when the patent owner files any enforcement action, and subsequently at each level of judicial review.

Those who support a healthy and effective patent system should hope that the invalidation rate of patents on Section 101 grounds will decrease with the issuance of the USPTO's July 2024 updated guidance, as it did in the immediate years following the USPTO's 2019 Guidance.[252]

[252] *See* Mazour, *supra* note 85 (noting that the issuance of the 2019 Revised Patent Subject Matter Eligibility Guidance led to a decrease in Section 101 rejections from 25 percent in 2018 to 15 percent in 2020; but also noting that Section 101 rejections have returned to pre-2019 Revised Patent Subject Matter Eligibility Guidance levels in the first half of 2024).

The higher the rate of Section 101 rejections for software/AI inventions—in particular at the patent application stage—the more this disproportionately favors the major large language model (LLM) providers like OpenAI and Google. They have the luxury of both:

- being generally able to rely on trade secrets to protect their intellectual property in the software/AI space[253] and
- having the resources to engage in speculative investments such as patenting in the AI space, as necessary.

A distribution of GenAI patents heavily skewed to a handful of major players further compounds anticompetitive concerns in the AI space, where these same players also have the unparalleled sets of proprietary data and access to computing power prerequisite to compete in the LLM and AI space.

4. We need an improved legal regime for making 35 U.S.C. § 101 patent subject-matter eligibility determinations for software inventions.

The federal courts and the USPTO should continue to work to ensure that patent subject-matter analyses are appropriately tailored for software/AI claimed inventions under 35 U.S.C. § 101, as necessary to support the development of a competitive AI industry—both within the U.S. and globally.

For a more principled, predictable, and effective patent system, including for Section 101 patent subject-matter eligibility determinations for software/AI inventions, the following should be treated as open questions:

[253] For discussion, *see supra* Sec. IV.D.

1. Should the federal courts and the USPTO continue to place an unfair presumption against the patent eligibility of many software/AI inventions?
    - As discussed above, the USPTO's *Alice/Mayo* two-step framework established in 2019 unfairly places a presumption against patent eligibility for software/AI inventions.
    - Would a more equitable framework entail:
        - a presumption that a software method claim *is* integrated into a practical application? And
        - the placement of the burden on the patent examiner to disprove such a presumption, as it is for almost all other technologies?
2. If, however, the two-step *Alice/Mayo* framework is maintained, should the federal courts and the USPTO reassess:

    a. the scope of the "abstract ideas" judicial exception [Step 2A – prong 1] and the procedures for determining when it applies?

    - Should the outer boundary of the "abstract ideas exception be restored to include only mathematical formulas, e.g., $E=mc^2$, as originally applied by the courts?
    - If not, should the boundary not be extended to cover all "mental processes" "that can practically done in the human mind" / "with a pen and paper?" Can there be a principled middle ground that both protects the "basic tools of scientific and technological work," but also

allows novel and nonobvious software inventions to be patent eligible?

b. the standards for the "integration into a practical application" exception to the judicial exception [Step 2A – prong 2] and the procedures for applying them?

- Can a clearer definition of what constitutes a "practical application" be developed?
    - And one that does not improperly import novelty concepts from other parts of the patent statute (namely 35 U.S.C. §§ 102 and 103) that should be entirely separate from any gating patent eligibility determination under 35 U.S.C. § 101?
    - When does an application cross the line from ineligible to eligible because it is sufficiently "practical?"
- For software inventions, the "improvements to functioning of a computer" consideration is of obvious importance.
    - The USPTO explicitly notes that "the courts have not provided an explicit test for how to evaluate the improvements consideration" and instead rely on the application of individual federal cases for their guidance.[254]

[254] *Id*. The USPTO Guidance directs examiners to MPEP sections 2106.04(d)(1) and 2106.05(a) for these decisions and a detailed explanation of how USPTO personnel should evaluate this consideration. *Id.*

  - Can the courts establish an objective legal test for this "improvements to functioning of a computer" consideration? Without this, will software/AI patent applicants continue to be subject to the de facto substantive rulemaking of the USPTO, individual USPTO technology centers, and even individual USPTO patent examiners?

The Supreme Court has denied dozens of petitions for certiorari on Section 101 issues seeking clarification on *Alice*'s "abstract-idea exception and the proper application" of the *Alice/Mayo* framework.[255] As such, the ongoing judicial and USPTO bias against the patent eligibility of many software inventions has and will continue to extend to many AI inventions as well.

Should it be determined that the required certainty and fairness is impossible under the current legal and regulatory (USPTO) regimes, then perhaps Congress should intervene.[256]

In the meantime, all stakeholders in the patent system should work together where possible to develop consensus, nonpartisan principles and best practice recommendations to help Congress, the federal courts, and the USPTO address these

[255] Congressional Research Service, Patent-Eligible Subject Matter Reform: An Overview (Jan. 3, 2024), *available at* https://crsreports.congress.gov/product/pdf/IF/IF12563.

[256] For example, in June 2023, Sen. Thomas Tillis introduced the Patent Eligibility Restoration Act of 2023, which if passed would eliminate all "judicial[ly created] exceptions" and replace them with a legislatively codified and more clearly and narrowly defined list of inventions that would not be eligible for patent protections. *See* https://www.congress.gov/bill/118th-congress/senate-bill/2140/text.

Section 101 patent subject-matter eligibility issues for software/AI inventions to move the law forward in a reasoned and just way and fulfill the patent system's objective of "promot[ing] the progress of science and useful arts" as required by the U.S. Constitution.[257]

SUMMARY OF KEY QUESTIONS

Should New Laws, Court Decisions, Or Regulations:

(1) ***Amend copyright law to more clearly protect GenAI-assisted software coding?***

(2) ***Protect any GenAI-assisted software code from the loss of any copyright protections due to any incorporation of copyleft protected open-source software?***

(3) ***Clarify and/or reassess the 35 U.S.C. § 101 patent eligibility requirements for software/AI inventions, including by:***

(a)examining whether the courts and USPTO's Alice/Mayo two-step framework should be replaced as inherently biased against software inventions?

(b)if the Alice/Mayo two-step framework is maintained, . . .

(i) ***. . . redefining the scope of the "abstract ideas" judicial exception [Step 2A – prong 1] and the procedures for determining when it applies?***

[257] For discussion, *see infra* Sec. IX.

(ii) ***. . . redefining the standards for the "integration into a practical application" exception to the judicial exception [Step 2A – prong 2] and the procedures for applying them?***

- ***Including with respect to the "improvements to functioning of a computer" consideration? Can the courts establish an objective legal test for this consideration to prevent de facto substantive rulemaking by the USPTO on this issue so central to the patent eligibility of software inventions?***

V. ISSUE NO. 3: HOW IS PATENT LAW IMPACTED BY THE USE OF GENAI TO EXPAND HUMAN CAPABILITIES AND ALSO GENERATE VOLUMINOUS "ART"?

In April 2024, the USPTO issued a Request for Comment concerning "the impact of the proliferation of Artificial Intelligence on prior art, the knowledge of a person having ordinary skill in the art, and determinations of patentability made in view of the foregoing."[258]

Absent careful adherence to the principles and case law that have defined the concept of the person having ordinary skill and the determination of what qualifies as prior art, resolution of these issues will inevitably operate to weaken the strength of patents overall—the only question is to what degree.[259]

A. *The impact of GenAI on the foundational patent law concept of the person having ordinary skill in the art (PHOSITA)*

Section 103 of the Patent Act defines the nonobviousness requirement to patentability as follows:

> A patent for a claimed invention may not be obtained . . . if the differences between the claimed

[258] *See* U.S. Patent and Trademark Office, Request for Comments Regarding the Impact of the Proliferation of Artificial Intelligence on Prior Art, the Knowledge of a Person Having Ordinary Skill in the Art, and Determinations of Patentability Made in View of the Foregoing, 89 Fed. Reg. 34217 (Apr. 30, 2024), *available at* https://www.federalregister.gov/documents/2024/04/30/2024-08969/request-for-comments-regarding-the-impact-of-the-proliferation-of-artificial-intelligence-on-prior.

[259] In the view of one commentator, the sky is the limit. *See* Tim W. Dornis, *Artificial Intelligence & Innovation: The End of Patent Law as We Know it*, 23 YALE J.L. & TECH. 97 (Fall 2020) ("With the advent of artificial intelligence (AI), the end of patent law is near."), *available at* https://yjolt.org/sites/default/files/23_yale_j.l._tech._97_ai_patent_0.pdf.

> invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a *person having ordinary skill in the art* to which the claimed invention pertains.[260]

"The person of ordinary skill [for purposes of determining obviousness] is a hypothetical person who is presumed to be aware of *all* the pertinent prior art."[261] This legal fiction has become at least theoretically closer with the "AI-fueled transformation of the once genuinely human PHOSITA into a cognitively augmented human-machine."[262] With GenAI, the PHOSITA can now directly access all of the information on the internet, with formidable obstacles of the past such as language barriers torn down by automatic and precise LLM translators. And the GenAI models can be trained to help (or self-?) identify, collect, organize, and analyze the most relevant prior art exponentially faster and better than any human ever could alone.

Remarkably, GenAI potentially may have an even greater impact on PHOSITA with respect to the elusive "motivation to combine" requirement for an invalidity-for-obviousness analysis under 35 U.S.C. § 103. It has been a longstanding requirement for an obviousness determination not only that two or more pieces of prior art must collectively read on every element of a patent claim, but that there must be some motivation to combine the prior art references and to expect the combination

[260] 35 U.S.C. § 103 (emphasis added).

[261] Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc., 807 F.2d 955, 962 (Fed. Cir. 1986) (emphasis added).

[262] Dornis, *supra* note 259, at 104.

will work as intended.[263] The evidentiary requirements for establishing the requisite motivation to combine have changed over time.

An important limitation preventing the use of Section 103 obviousness to invalidate all types of patents is the standard that only "analogous" prior art can be used. "A reference qualifies as prior art for an obviousness determination under § 103 only when it is analogous to the claimed invention."[264] "A person of ordinary skill in the art is also a person of ordinary creativity, not an automaton."[265] A prior art reference can prompt the PHOSITA whether it is from its "same field [of endeavor] or a different one."[266]

The USPTO has interpreted the federal court case law as requiring a flexible approach to both a motivation-to-combine determination and a determination of the scope of prior art and

[263] *See* KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 421 (2007) ("When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense. In that instance the fact that a combination was obvious to try might show that it was obvious under § 103.").

[264] *In re* Klein, 647 F.3d 1343, 1348 (Fed. Cir. 2011).

[265] *KSR*, 550 U.S. at 421.

[266] *Id.* at 417; *see also In re* Bigio, 381 F.3d 1320, 1325 (Fed. Cir. 2004) ("Two separate tests define the scope of analogous art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed and, (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.")

whether it is analogous[267] but as still requiring "articulated reasoning and evidentiary support."[268]

GenAI is exceptional at accessing and making connections between knowledge across different fields of science and technology. By definition, the pre-GenAI PHOSITA was limited to having knowledge and the ability to make connections within its field of knowledge and those analogous to them. A PHOSITA powered by GenAI, however, can break free of both limitations to at least some degree. It remains to be seen to what that degree will be in the eyes of the courts. As one commentator eloquently describes:

> The future AI-supported inventor may be trapped in a nightmare that Judge Learned Hand described long ago: "[A]s the law stands, the inventor must accept the position of a mythically omniscient worker in his chosen field. As the arts proliferate with prodigious fecundity, his lot is an increasingly hard one."[269]

But returning to the principles that have been used to define the PHOSITA may help rein in reliance on GenAI in rejecting patent applications or invalidating issued ones. As Judge Giles Rich explained:

> [A] person of ordinary skill in the art is . . . presumed to be one who thinks along the line of conventional

[267] *See* U.S. Patent and Trademark Office, Updated Guidance for Making a Proper Determination of Obviousness, 89 Fed. Reg. 14449, 14450–52 (Feb. 27, 2024), *available at* https://www.federalregister.gov/documents/2024/02/27/2024-03967/updated-guidance-for-making-a-proper-determination-of-obviousness.

[268] *Id.* at 14452.

[269] Dornis, *supra* note 259, at 128 (citing *Merit Mfg. v. Hero Mfg.*, 185 F.2d 350, 352 (2d Cir. 1950)).

> wisdom in the art and is not one who undertakes to innovate, whether by patient, and often expensive, systematic research or by extraordinary insights, it makes no difference which."[270]

Applying this reasoning, a PHOSITA lacks innovative ingenuity, generally does not make connections between different fields, and does not draw innovative conclusions from any such "systematic research" GenAI might produce.

B. *The use of GenAI as a permutation generator of "art"*

The business model of creating computer-generated claims and publications through natural language processing algorithms for prior art and other patenting purposes has existed for at least a decade. Around 2014, a French company called Cloem reportedly started offering a service "us[ing] brute-force computing to mechanically compose text for thousands of patent claims covering potentially novel inventions and also to generate defensive publications to prevent others from obtaining patent protection in the same field."[271]

The libertarian organization All Prior Art uses GenAI to generate prior art "to democratize ideas, provide an impetus for change in the patent system, and to preempt patent trolls."[272]

Should such "art" as automatically generated by GenAI qualify as a prior art "printed publication" under 35 U.S.C. § 102(b)? This has not been tested in court and will likely depend on:

[270] Standard Oil Co. v. Am. Cyanamid Co., 774 F.2d 448, 454 (Fed. Cir. 1985).

[271] Ben Hattenbach & Joshua Glucoft, *Patents in an Era of Infinite Monkeys and Artificial Intelligence*, 19 STAN. TECH. L. REV. 32 (2015), at 35.

[272] ALL PRIOR ART, http://allpriorart. com/about (last visited July 27, 2024).

1. Whether the courts find the GenAI-produced "art" was "made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence[] can locate it" such that it was "publicly accessible?"[273]
2. Whether the courts find the GenAI-produced "art" fulfills the enablement requirement under 35 U.S.C. § 112?[274] Such an analysis would likely entail making new law establishing whether such Gen-AI produced "art" should benefit from the presumption that all prior art is enabled for purposes of an invalidity-for-anticipation analysis under 35 U.S.C. § 102.[275]
3. Whether the courts find that GenAI-produced "art" that has never been used or tried should not constitute prior art, because that would be contrary to the fundamental concept that prior art is the accumulation of real-world knowledge?
4. Whether the courts find the GenAI-produced "art" is analogous to patented technology in question, as

[273] Suffolk Techs., LLC v. AOL Inc., 752 F.3d 1358, 1364 (Fed. Cir. 2014). For discussion of the publicly-accessible determination, *see* Hattenbach, *supra* note 271, at 37–38.

[274] For discussion of the enablement determination for prior art printed publications, *see* Hattenbach, *supra* note 271, at 38–39.

[275] *See In re* Antor Media Corp., 689 F.3d 1282, 1289 (Fed. Cir. 2012) (holding that during patent prosecution, "an examiner is entitled to reject claims as anticipated by a prior art publication or patent without conducting an inquiry into whether or not that prior art reference is enabling," and "[a]s long as an examiner makes a proper prima facie case of anticipation by giving adequate notice under § 132, the burden shifts to the applicant to submit rebuttal evidence of nonenablement"). For discussion of the enablement determination for prior art printed publications, *see* Hattenbach, *supra* note 271, at 38–39.

> required for any invalidity-for-obviousness analysis under 35 U.S.C. § 103?[276]

Even if AI-generated "art" is categorically excluded from serving as printed publication prior art under 35 U.S.C. § 102(b), if it reads on every element of a given patent claim, some may argue that this itself serves as evidence of obviousness under 35 U.S.C. § 103.

There is an additional wrinkle that illustrates the unique problems that only arise with the sheer scale of volume that an arms race of automatic permutation generation might bring about. It is common for a patent application to have a broad "genus" claim that encompasses many "species" (i.e., embodiments) within it. In *Amgen v. Sanofi*, the Supreme Court concluded that the patentee's patent specification did not provide an enabling disclosure for the full scope of the claimed genus.[277] And "a prior art disclosure merely needs to describe *one* of the potentially millions of embodiments that falls within a genus claimed in a patent application to support a lack of novelty rejection."[278]

GenAI is a tailor-made tool for generating permutations of embodiments to cover the entire range of a genus claim. But the more permutations that a patent applicant has generated and discloses in its specification to mitigate an enablement rejection under *Amgen*, the more likely it is to have each and every claim

[276] For discussion of the analogous art/obviousness determination, *see supra* Sec. V.A; *see also* Hattenbach, *supra* note 271, at 39–43.

[277] Amgen Inc. v. Sanofi, 598 U.S. 594, 613 (2023).

[278] Lucas R. Yordy, *The Library of Babel for Prior Art: Using Artificial Intelligence to Mass Produce Prior Art in Patent Law*, 74 VAND. L. REV. 521 (2021), at 547 (emphasis added) (citing MPEP § 2131.02(I) (9th ed. Rev. 08.2017, Jan. 2017) (citing *In re Gosteli,* 872 F.2d 1008 (Fed. Cir. 1989)), *available at* https://scholarship.law.vanderbilt.edu/vlr/vol74/iss2/1.

read on by a random output of a GenAI permutation generator employed by a third party to create defensive prior art to invalidate this or an analogous technology's patent claims.

SUMMARY OF KEY QUESTIONS

Should new laws, court decisions, or regulations calibrate the degree to which innovations are patentable in the AI Age by:

(1) Setting the degree to which the knowledge and skill of PHOSITA should expand due to its adoption of GenAI?

(2) Determining if and when GenAI-generated "art" should constitute a prior art printed publication, including with respect to:

(a) the "publicly accessible" requirement?

(b) the enablement requirement under 35 U.S.C. § 112?

(c) any requirement that any "art" must have been actually used or tried to constitute prior art?

(d) the "analogous prior art" requirement?

VI. ISSUE NO. 4: SHOULD THE USE OF PUBLIC GENAI IN A COMPANY'S PRODUCT DEVELOPMENT LIFECYCLE PRESUMPTIVELY CONSTITUTE PUBLIC DISCLOSURE INVALIDATING PATENT OR DESTROYING TRADE SECRET RIGHTS?

A. *The prohibition against public disclosures of inventions before filing a patent application or of trade secrets in general*

The general rule under patent law is that a patent applicant cannot publicly disclose its invention before filing the patent application.[279] [280] The same logic applies for trade secrets but on a more permanent basis: the owner must take "reasonable measures" to protect the secrecy of the information in question on an ongoing basis in order to claim it as a trade secret.[281]

These prohibitions against public disclosure take on new and unique significance in our incipient AI Age, as generative AI is increasingly used as part of the product development lifecycle by companies and individuals. Many have observed that the use of a "public" GenAI such as a nonenterprise version of OpenAI's ChatGPT where all inputs and outputs are owned and used for model-training purposes by the LLM provider may presumptively be viewed as in violation. The

[279] 35 U.S.C. § 102(a) ("A person shall be entitled to a patent unless (1) the claimed invention was patented, described in a printed publication, or in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention . . . .").

[280] In the U.S. (and a minority of other countries), however, a one-year grace period is statutorily mandated to give the applicant the opportunity to complete and/or assess the marketplace for their invention before having to file for a patent application. *See* 35 U.S.C. § 102(b).

[281] *See* Defend Trade Secrets Act of 2016 (DTSA), 18 U.S.C. §§ 1831–39 (requiring trade secrets to be the subject of "reasonable measures" to maintain secrecy to be protectable).

commonsense way to mitigate this risk is to exclusively use enterprise versions of generative AI and ensure the contract precludes the LLM provider from saving or using any inputs/outputs to further train its GenAI models. That, however, is easier said than done in practice.

The implications of extending invalidating public disclosures to include GenAI inputs/outputs

According to a Salesforce November 2023 survey:

- 55 percent of all employees have used unapproved generative AI tools at work, and
- 40 percent of all workplace generative AI users have used banned tools at work.[282]

The temptation for software programmers to use GenAI to assist in their product development efforts is directly analogous to that for students to use GenAI to write their research papers. GenAI promises to help us to do many things better and far more efficiently. Particularly in the post-COVID workplace where working outside of the office on personal devices is now common practice, the temptation is compounded because the likelihood of getting caught by the employer is minimal when employees use their own personal computers or devices.

It is only when litigation ensues—in some cases well over a decade after the invention is fully conceived and the application is filed with and the patent is ultimately issued by the USPTO—that at least some instances of employees improperly using GenAI during the inventive process will be discovered. Any records of GenAI inputs/outputs that are part of the inventive process would be discoverable through the litigation process, as

[282] *More than Half of Generative AI Adopters Use Unapproved Tools at Work*, SALESFORCE (Nov. 15, 2023), https://www.salesforce.com/news/stories/ai-at-work-research/.

would the private computer that the engineer used to make or access them.

Does it make sense as a matter of public policy to disqualify companies from securing or enforcing patents under these or other similar circumstances, in particular only years after the fact when litigation arises? Or to destroy companies' trade secret rights for the same reason?

For established companies, putting a new employment policy in place is one thing. Getting all employees to comply is another thing entirely. But at least major companies have more resources to take the requisite "reasonable measures" and set policies, run employee training programs, and monitor and enforce these policies.

Less-established companies, in particular startup companies, simply do not have such excess resources. And their core intellectual property is more likely to be their key to building their "competitive moat." Such uncertainty regarding the validity or enforceability of fundamental IP rights such as these, let alone for a reason as ancillary as this one, significantly lowers their potential value and the likelihood that any company will invest in them.

Furthermore, should companies and individuals be incentivized to set policies to destroy all records of GenAI inputs and outputs to mitigate the risk of them subsequently being used to invalidate patents and trade secrets years after the fact? In particular when the destruction of all such records greatly impairs if not precludes the possibility of accurately assessing human-inventorship issues that are arguably far more substantively important?

KEY QUESTION:

Should new laws, court decisions, or regulations exclude GenAI inputs/outputs from constituting public disclosures invalidating any patent or trade secret rights?

VII. ISSUE NO. 5: SHOULD INDIVIDUALS HAVE RIGHTS AGAINST THE USE OF GENAI TO CREATE DEEPFAKES APPROPRIATING THEIR IDENTITIES?

A. There is no comprehensive set of federal laws against deepfakes.

There is simply no argument for any right to:

- create deepfakes (i.e., an AI-generated video, audio, etc., capable of portraying someone doing something they did not do),
- distribute and pass them off as real, and
- disclaim liability for any harm suffered.

Certainly not without the victim's consent. And even more certainly when it involves digitally removing an individual's clothes and portraying the individual as committing sexual acts.

Even if "honestly presented" as fake, there should be the fundamental right and means to prevent one's likeness from such "nudification." And society has a significant interest in protecting against GenAI deepfakes being intentionally created and presented as real for the purpose of affecting political elections, etc., First Amendment concerns notwithstanding. But no such comprehensive protections are in place, at least under current law.

There is currently no federal law granting any "right of publicity" preventing the unauthorized commercial use of an individual's name, likeness, or other recognizable aspects of one's persona. The right of publicity is but a patchwork of state and common law.[283] Only about half of the U.S. states have any

[283] For a survey of the relevant existing legal frameworks that "provide protection against the unauthorized use of aspects of an individual's persona," including state law (e.g., right of privacy; right of publicity; and state regulations of digital replicas), federal law (e.g., the Copyright Act; the

specific "right of publicity" law, with some states' laws being more established than others. People domiciled in the other states have little to any legal recourse if their identities are used without their authorization in any fashion and for any purpose.

There are, however, several pending Congressional bills directed toward these issues for the AI Age. For example:

- In January 2024, the No AI FRAUD Act was introduced that would establish intellectual property rights on individual's likeness and voice against AI-generated fakes and forgeries.[284]
- In July 2024, the NO FAKES Act was introduced that would create a new federal right "to protect the voice and visual likenesses of creators and individuals from the proliferation of digital replicas created without their consent," i.e., a "digital reproduction right."[285]

Federal Trade Commission Act; the Lanham Act; and the Communications Act), and private agreements, *see USCO July 2024 Digital Replicas Report*, *supra* note 117, at 8–22. The USCO expressly interprets the copyright law as not covering the right of publicity and most protections against unauthorized digital replicas, because "[c]opyright does not [] protect an individual's identity in itself, even when incorporated into a work of authorship." *Id.* at 17.

The USCO provides this survey to "review the protections available under current laws and the gaps in their capacity to respond to today's threats," and to recommend that Congress pass a federal law "assessing the need for federal protection specifically with respect to unauthorized digital replicas." *Id.* at 7. Such protection would be an important part of any broader right of publicity in the AI Age. *Id.*

[284] *See* The No Artificial Intelligence Fake Replicas and Unauthorized Duplications Act of 2024, H.R. 6943, 118th Congress, § 3(b) (2024) [hereinafter *No AI FRAUD Act*], *available at* https://www.congress.gov/bill/118th-congress/house-bill/6943/text.

[285] *See* The Nurture Originals, Foster Art, and Keep Entertainment Safe Act, at § 2(b) ("Digital Replication Right") & § 2(g) ("Rule of Construction")

- In January 2024, the DEFIANCE Act was introduced to provide a "civil action relating to disclosure of intimate images," including nonconsensual sexually-explicit 'deepfake' images and videos.[286]

B. *Should LLM providers bear liability for providing the tools for the generation of deepfakes?*

Should the LLM providers that provide the tools for the generation of deepfakes be liable for any harm that is caused when their customers generate deepfakes? And should LLM providers be able to immunize themselves against any such liability through their contracts?

The competing policy interests can be summarized as:

- the rights of individuals to protect themselves against deepfakes and hold those who support their creation accountable, versus
- the goal of supporting the U.S. GenAI industry to compete for preeminence in the global GenAI economy, including by limiting their regulatory obligations and legal liabilities.

KEY QUESTION:

Should Congress pass a federal "right of publicity" law preventing unauthorized use of an individual's name, likeness, or other recognizable aspects of one's persona for commercial, political, or pornographic purposes?

(2024) [hereinafter *NO FAKES Act*], *available at* https://www.coons.senate.gov/imo/media/doc/no_fakes_act_bill_text.pdf.

[286] *See* The Disrupt Explicit Forged Images and Non-Consensual Edits Act of 2024, S. 3696, 118th Congress, §3 ("Civil Action Relating to Disclosure of Intimate Images") (2023–24), *available at* https://www.congress.gov/bill/118th-congress/senate-bill/3696/text.

VIII. ISSUE NO. 6: SHOULD WORKS OF AUTHORSHIP BE PROTECTED FROM UNAUTHORIZED USE FOR TRAINING GENAI MODELS?

A. *Issue No. 6(a): Does existing copyright law limit the unauthorized use of works of authorship for training GenAI models?*

In sum, for a copyright infringement claim, copyright owners must prove they own the copyrighted work, and that the defendant misappropriated their exclusive right to reproduce and distribute it and all derivative works based on it.[287] Derivative works must be "substantially similar" to the copyrighted work to be infringing.

Establishing the "substantially similar" requirement in generative AI cases is particularly challenging. This should not be a surprise. Unless a prompt specifically instructs AI to generate "an image similar to X," the output will not look like X. It is going to be a composite of numerous inputs, not appearing to be substantially similar to any of them.

"Substantial similarity" is even harder to establish with text, which is much easier to plagiarize without proper attribution. Replace a couple of choice words and play with the sentence structure, and you have "made" someone else's idea your own. This is not necessarily improper. In fact, it happens to at least some degree in most writing, particularly any sort of research paper.

[287] *See* 17 U.S.C. § 106 (Exclusive rights in copyrighted works); *How to Prove Copyright Infringement*, COPYRIGHT ALLIANCE, https://copyrightalliance.org/education/copyright-law-explained/copyright-infringement/how-to-prove-copyright-infringement/ (last visited July 27, 2024).

Generative AI is not conceptually doing anything different than anyone doing research and analysis. Or when a content creator is inspired by other musicians or artists. It just does it better than any human being could in several respects, including the volume of information it "considers" when generating its output.

As such, the numerous creator lawsuits asserting copyright infringement against GenAI providers for training their AI models on copyrighted works may face an uphill battle under existing copyright law. The first wave of substantive judicial rulings on these issues should come in over the next year or two.

In the meantime, by around September 2024, the USCO is scheduled to issue the section of its forthcoming comprehensive copyright and AI law report on the "legal implications of training AI models on copyrighted works"[288] as well as the allocation of potential liability for AI-generated outputs that may infringe.[289]

[288] For a list of 2024 GenAI copyright infringement cases, *see Feb. 2024 Ltr. from Shira Perlmutter*, *supra* note 124, at 6, n.20 (listing Concord Music Group, Inc. v. Anthropic PBC, 23-cv-01092 (M.D. Tenn.); Authors Guild v. OpenAI Inc., 23-cv-08292 (S.D.N.Y.) (consolidated with Alter v. OpenAI Inc., 23-cv-10211 (S.D.N.Y.), and Basbanes v. Microsoft Corporation, 24-cv-00084 (S.D.N.Y) for pretrial purposes); J.L. v. Alphabet Inc., 23cv-03440 (N.D. Cal.); Kadrey v. Meta Platforms, Inc., 23-cv-03417 (N.D. Cal.) (consolidated with Chabon v. Meta Platforms, Inc., 23-cv-04663 (N.D. Cal.), which was closed by the court upon consolidation); (Huckabee v. Meta Platforms, Inc., 23-cv-06663 (N.D. Cal.); Getty Images (US), Inc. v. Stability AI, Inc., 23cv-0135 (D. Del.); Andersen v. Stability AI Ltd., 23-cv-0201 (N.D. Cal.)).

[289] *Feb. 2024 Ltr. from Shira Perlmutter*, *supra* note 124, at 6 (announcing planned publication date of the end of the 2023–24 fiscal year).

B. *Issue No. 6(b): Should AI providers be shielded from copyright and other liability to support the development of the AI industry in the U.S.?*

Section 230 of the Communications Decency Act of 1996 has long shielded internet platforms from liability for content created by users.[290] Title II (the "Online Copyright Infringement Liability Limitation Act") of the Digital Millenium Copyright Act of 1998 limits the liability of online service providers for copyright infringement.[291] Some credit such federal protections as being instrumental to the very success of the internet.

Will our government apply these same principles to protect GenAI LLM providers from liability for content generated using their platforms? Or should the rights of creators against the unauthorized use of their copyrighted works to train GenAI models, ultimately threatening their very livelihoods, be prioritized?[292]

Several governments around the world have created special text- and data-mining exceptions to copyright law to make it easier to collect and use information, including copyrighted works, for training AI.[293] They have done so presumably, at least

[290] 47 U.S.C. § 230, *available at* https://www.law.cornell.edu/uscode/text/47/230.

[291] 112 STAT. 2860, *available at* https://www.copyright.gov/legislation/dmca.pdf.

[292] For a discussion of the applicability of Section 230 and other potential sources of secondary liability for technology providers in the AI context, *see USCO July 2024 Digital Replicas Report*, *supra* note 117, at 36–39.

[293] For a discussion of these issues, *see* James Love, *We Need Smart Intellectual Property Laws for Artificial Intelligence*, SCI. AM. (Aug. 7, 2023), https://www.scientificamerican.com/article/we-need-smart-intellectual-property-laws-for-artificial-intelligence/.

in part, to help their AI industries compete in the global marketplace.

Depending on how one looks at it, this may create at the extremes either:

- a cautionary tale of a "race-to-the-bottom" situation that the U.S. must not fall into, or
- a clarion call that the U.S. government should not overregulate AI lest we unnecessarily put ourselves behind for global preeminence in this critical technology.[294]

Notably, both the No AI FRAUD Act and the NO FAKES ACT introduced in 2024 include a provision defining the bill to be "a law pertaining to intellectual property for the purposes of section 230(e)(2) of the Communications Act of 1934 (47 U.S.C. 230(e)(2))".[295] That provision carves out "intellectual property law" from Section 230 immunity for online service providers.[296]

SUMMARY OF KEY QUESTIONS

(1) Should new laws, court decisions, or regulations:

- ***Address the use of copyrighted works of authorship in training GenAI models, balancing:***
- ***the rights and interests of copyright holders? and***
- ***the need for AI models to be trained on voluminous data without excess obstacles? and***

[294] *Id*.

[295] *No AI FRAUD Act, supra* note 284, at § 3(j); *NO FAKES Act, supra* note 285, at § 2(g).

[296] 47 U.S.C. 230(e)(2) ("Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.").

(2) Address any liability LLM providers should bear with respect to the outputs from their LLMs, and whether they should be able to indemnify themselves from liability through contracting?

IX. CONCLUSION

Of the issues presented in this article, the only one that clearly calls for Congress to pass a new set of federal laws to regulate it is the topic of AI-generated deepfakes (Issue No. 5).

Congress might also intervene with passing new laws in respect to:

- the special substantive analytical and evidentiary issues regarding sufficiency-of-human-contributions determinations brought about by GenAI-assisted works of authorship and inventions (Issue No. 1),
- the need for clarity with respect to the patent subject-matter eligibility of AI/software patents (Issue No. 2),
- the use of GenAI to expand human capabilities and generate voluminous "art" (Issue No. 3),
- whether AI prompts/inputs should be excluded from constituting public disclosures invalidating any patent or trade secret rights (Issue No. 4), and
- whether the unauthorized use of copyrighted works to train AI should be regulated (Issue No. 6).

Regardless of any action taken by Congress, though, the federal courts will inevitably play the primary role in interpreting the copyright, patent, trade secret, and any other IP law on these issues. Concerns that these issues are too important and fast-moving to leave to the deliberative nature of the judiciary, while understandable, are simply beside the point. Challenging legal issues such as these are generally best resolved by the deliberative process and court decisions of our judiciary. And of course, interpreting the law on these issues as set forth by the Constitution and U.S. federal law as set forth by Congress is the exclusive mandate of the judiciary.

The best way to help both Congress and in particular the federal courts address these issues is for copyright, patent, trade secret, and other IP lawyers to develop consensus, nonpartisan principles and best practice recommendations for each, to be:

- used as a resource by our lawmakers and judiciary when passing laws or ruling on cases, and
- voluntarily adopted by companies and members of the legal profession, in whole or more likely in part, in the meantime.

Such recommendations should further help achieve the goal of protecting a company's GenAI-assisted intellectual property but without generating excess "business friction" impeding the company's product development efforts. In other words, they must be feasible.

Given the wide-ranging societal implications that the rise of GenAI threatens to bring about and the speed within which they are happening, there has perhaps never been a greater need and a more urgent time for the legal profession to step up and fill these needs than today.

Moving the Law Forward
in a Reasoned & Just Way

Visit www.thesedonaconference.org