The Sedona Conference Journal

Volume 12 2011

Information Age Catch 22: The Challenge of Technology to Cross-Border Disclosure & Data Privacy

M. James Daley

Recommended Citation: M. James Daley, *Information Age Catch 22: The Challenge of Technology to Cross-Border Disclosure & Data Privacy*, 12 SEDONA CONF. J. 121 (2011).

For this and additional publications see:
https://thesedonaconference.org/publications

INFORMATION AGE CATCH 22: THE CHALLENGE OF TECHNOLOGY TO CROSS-BORDER DISCLOSURE & DATA PRIVACY

M. James Daley, Esq., CIPP[1]
Daley & Fey
Overland Park, KS

INTRODUCTION

Technology is the bittersweet "Catch 22"[2] of the information age. On the one hand, technology promises paperless productivity with the freedom of a virtual workplace. On the other hand, it spawns a kind of "Digital Attention Deficit Disorder"—an addiction-like need for instant information gratification. In theory, technology is designed to improve our quality of life and tame the jungle of unstructured data. In practice, it often creates a kind of computer co-dependence, exploding the normal boundaries of work space and time, and binding us wirelessly to local and wide area networks via an expanding array of personal mobile devices.

The way in which people communicate and connect has fundamentally shifted to collaborative and social networking technologies.[3] Americans, for example, spend nearly a quarter of their Internet time on social networking sites and blogs.[4] If Facebook were a country, with over 600 million inhabitants, it would be the third largest, behind China and India—and ahead of the United States—with more than 1 billion pieces of content shared daily.[5] More than 300,000 businesses—and 56% of Fortune 500 companies—have a presence on social networking sites.[6] And the "new" kid on the block, Twitter, is used in 60% of companies with over 300 million users and counting, with over 9 new registrations per second.[7]

---

1 The opinions expressed in this article are those of the Author and do not necessarily reflect the opinions of the author's law firm, or of The Sedona Conference®. This article builds upon a paper entitled "Catch 22 Revisited: Recent Developments in Cross-Border Discovery & Data Privacy" presented at the Second Annual Sedona Conference® International Programme on Cross-Border E-Discovery and Data Privacy held in Washington, D.C. on September 15-16, 2010. The Author would like to acknowledge the substantial contributions of Lara Ballard to this article and the previous paper.

2 A "Catch 22" is defined as a dilemma in which the only solution is denied by a circumstance inherent in the problem. For example, the "show business" Catch 22 is that you cannot get work without a talent agent, and you can't get a talent agent unless you have worked. Or, as in its namesake 1961 novel by Joseph Heller, you cannot be relieved of flight duty for mental disability unless you are irrational, and since it is rational to fear death in wartime bombing missions, it is impossible to be relieved of flight duty for mental disability. JOSEPH HELLER, CATCH 22 (1961), http://en.wikipedia.org/wiki/Catch-22.

3 THE SEDONA CONFERENCE , THE SEDONA CONFERENCE® FRAMEWORK FOR ANALYSIS OF CROSS-BORDER DISCOVERY CONFLICTS: A PRACTICAL GUIDE TO NAVIGATING THE COMPETING CURRENTS OF INTERNATIONAL DATA PRIVACY & E-DISCOVERY (Public Comment Version Aug. 2008).

4 Brian Solis, *Facebook Connects 500 Million People: Defines a New Era of Digital Society*, July 22, 2010, http://www.briansolis.com/2010/07/facebook-connects-500-million-people-defining-a-new-era-of-digital-society/.

5 *Id.*

6 Marissa McNaughton, *71% of Fastest Growing U.S. Companies have a Facebook Presence*, THE REALTIME REPORT, Feb. 1, 2011, http://therealtimereport.com/tag/umass-dartmouths-center-for-marketing-research/.

7 Shea Bennett, *40 Twitter Tips, 300M Users, A Twitter IPO and Mad Ad Men: Top 10 Twitter Stories of the Week*, ALLTWITTER, May 22, 2011, http://www.mediabistro.com/alltwitter/top-10-twitter-stories-220511_b9188.

A further sign of the times is that 45% of organizations use social networking searches to screen job candidates,[8] and to market directly to customers. For example, Papa John's Pizza added 148,000 fans in one day via a Facebook marketing campaign, increasing its web traffic by 253%. Best Buy has built a specialized online blog for customers to use to rate products and services, building on research that 90% of consumers trust their peers more than marketers. One study found that an average Facebook "Like" drove $1.34 in ticket sales; and the average "Tweet," drove $.80 in ticket sales.[9]

Social networking can be abused as well. A Whole Foods Company executive who used an alias to post negative comments about a rival company earned a SEC investigation, and loss to stock value, after the FTC revealed the secret smear campaign.[10] Research reflects that about 44% of all online video is viewed in the workplace, resulting in a significant loss of productivity.[11] A recent study in Canada revealed that 75% of Canadians are using online networking while on the job.[12]

In the legal context, U.S. courts have begun to order litigants to produce relevant portions of public and private current and historical data from Facebook, MySpace and other social networking sites. In *Romana v. Steelcase Inc*., 2010 NY Slip Op 20388 (Sup. Ct. of New York, Sept. 21, 2010), the court noted that people who place their physical condition in controversy by seeking damages for personal injury may not shield from disclosure information that would be relevant to such claims. The public Facebook profile of the plaintiff reflected a very active lifestyle, including intense zip-lining, after the date of her alleged debilitating injuries.

While it is true that information is the currency of the new millennium, there are very few tools to help us process the daily flood of data noise into actionable knowledge. We are no longer "papered" to the wall—we are "programmed" **into** the wall. To coin a phrase, "That which sustains us, destroys us." The ability to balance the competing interests of cross-border disclosures and data privacy is severely diminished by this rapid rate of technological change.[13] As new technologies accelerate global communication and development, they increase the risk of collateral damage to cross-border disclosure and data privacy compliance.

Law and public policy, which exist to help bring order out of chaos, simply cannot keep pace. Cloud computing dilutes the notion of where data "resides" and who controls it. Social networking platforms such as Facebook and MySpace blur the notion of our public and private "personas." And emerging Smart Grid, RFID, Biometric, DNA identification and profiling tools threaten to make a "surveillance society" the rule, rather than the exception.

---

8 Jennifer Grasz, *45% of Employers use Facebook/Twitter to Screen Job Candidates*, OREGON BUSINESS REPORT, Aug. 24, 2009, http://oregonbusinessreport.com/2009/08/45-employers-use-facebook-twitter-to-screen-job-candidates/.

8 Sarah Kessler, *Facebook 'Likes' More Profitable than Tweets*, MASHABLE, Mar. 18, 2011, http://www.cnn.com/2011/TECH/social.media/03/17/facebook.twitter.profits.mashable/.

10 Andrew Martin, *Whole Foods Executive Used Alias*, THE NEW YORK TIMES, July 12, 2007, http://www.nytimes.com/2007/07/12/business/12foods.html; and Laura DiBiase, "Are Your Clients Smear-Savvy?", 18 AM. BANKR. INST. J. 22 (Nov. 18, 1999).

11 Alan Maurer, *Social Networking at Work Leads to Productivity Loss*, TECHJOURNALSOUTH, Aug. 24, 2010, http://www.techjournalsouth.com/2010/08/social-networking-at-work-leads-to-productivity-loss/.

12 Darah Hansen, *Social Media Explosion Sparks Debate Among Employers*, THE VANCOUVER SUN, June 7, 2011, http://www.vancouversun.com/business/technology/Social+media+explosion+sparks+debate+among+employers/4906005/story.html.

13 Natasha Singer, *Technology Outpaces Privacy (Yet Again)*, THE NEW YORK TIMES, Dec. 11, 2010, http://www.nytimes.com/2010/12/12/business/12stream.html.

As noted by the U.S. Federal Trade Commission in its landmark Preliminary Staff Report entitled "Protecting Consumer Privacy in an Era of Rapid Change," many companies—both online and offline—do not responsibly manage consumer information, and "some even appear to treat it in an irresponsible or even reckless manner."[14] The FTC's proposed framework is based on three main principles: Privacy by Design, Simplified Choice, and Greater Transparency.[15] In particular, one of the major recommendations is to implement a "Do not Track" option whereby users can "opt-out" of the capture or use of their personal information.[16] The FTC preliminary report outlines a recommended framework for all commercial entities that collect or use consumer data that can reasonably be linked to a specific consumer, computer or other device; it provides a helpful foundation for taming the technology-enhanced "Catch 22" between cross-border disclosure and data privacy.

Also in November 2010, The EU announced a proposed updating of the 1995 EU Directive aimed at developing "a comprehensive approach on personal data protection in the European Union," including the creation of an online "right to be forgotten." That is, users should be able to tell websites to permanently delete already submitted personal data, according to the EU.[17]

While emerging technologies drive unprecedented globalization, deep differences abide in cultural notions of law and privacy. These differences amplify the "Catch 22" consequences of cross-border disclosure and data privacy conflicts.[18] In relation to their impact on cross-border disclosure and data privacy, most emerging technologies can be placed in one of three functional categories: (1) Location and Activity Tracking and Social Networking; (2) Behavioural Profiling and Marketing; and (3) Cloud Computing, Data Security, and Data Privacy.

This article examines whether and to what extent emerging technologies are an important a factor for cross-border disclosure and data privacy, and whether a technology framework built on principles of accountability, transparency, and privacy by design can help harmonize competing and conflicting cross-border disclosure and data privacy concerns.

(1) Location and Activity Tracking and Social Networking Technologies

Some of the most innovative (and challenging) emerging technologies involve static and mobile location and activity tracking (i.e., geo-tracking) and social networking functions. These technology types include online tracking and flash cookies, smart grid systems, smart phone applications, RFID tracking, biometrics and DNA identification, and applications that automatically infer relationships between people, activities, locations, products, and services. They are better known by their brand names, including Google "Buzz," "Street View," "Video," "YouTube," "Google Me," "Google Maps," and "Google Apps;" Facebook and Facebook "Places;" MySpace; FourSquare; and "Wikileaks," to name a few.

---

14 Federal Trade Commission Preliminary Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Businesses and Policymakers," Dec. 2010, at i.

15 *Id.*, at vix.

16 ARMA, *Another 'Do Not Track' Bill Introduced*, June 1, 2011, http://www.arma.org/policy/policy/washingtonpolicybrief/11-06-01/Another_Do_Not_Track_Bill_Introduced.aspx.

17 John Miller, *EU Seeks Tougher Online Code in Bid to Safeguard Private Data*, THE WALL STREET JOURNAL, Nov. 5, 2010, http://online.wsj.com/article/SB10001424052748704805204575594423931135084.html.

18 *See* THE SEDONA CONFERENCE , THE SEDONA CONFERENCE FRAMEWORK FOR ANALYSIS OF CROSS-BORDER DISCOVERY CONFLICTS: A PRACTICAL GUIDE TO NAVIGATING THE COMPETING CURRENTS OF INTERNATIONAL DATA PRIVACY & E-DISCOVERY at 1 (Public Comment Version Aug. 2008).

Recently, commercial software such as "Geotime" has been adopted by global law enforcement agencies to map an individual's movements and communications on a three dimensional graphic, similar to those used in the futuristic drama, "The Minority Report." It can be used to identify relationships and links among communications and transactional information from social networking sites, satellite navigation equipment, mobile phones, financial transactions, and IP network logs. Privacy advocates are concerned that this kind of software can create virtual "dossiers" on every member of the public.[19]

The conventional wisdom is that the U.S. is far more cavalier than the rest of the world in online sharing of personal information. But in reality, U.S. users share less personal information on Facebook, Twitter, and other social networking sites, than non-U.S. users, according to a Unisys study.[20] Also, we naturally assume that teenagers share much more personal information online than adults. But a recent Canadian Study suggests that adults are often less conscious than teens of the implications of sharing personal data online.[21]

The European Union has reacted swiftly in response to the clear and present danger represented by "big brother" technologies such as "Geotime." The EU Article 29 Working Party has opined that geo-location data is personal data, and that mobile service providers need explicit user permission to collect or relay location data.[22] As a result, Apple and Google may have violated the EU Directive by collecting data without proof of the users' free and informed consent.

With Apple, the iPhone and 3G version of the iPad began logging users' locations in 2010, when Apple updated its mobile operation system. This data is copied in an unencrypted form to the host computer or laptop when a sync occurs.[23] Apple eventually responded with a free software patch that reduced the location cache on the iPhone to no more than seven days, and promised to stop backing up the cache onto personal computers, as well as to automatically delete the cache when users turn off location services.[24]

The mere purchase of a device with geo-location functionality does not constitute consent, and the default position of such services must be set to "off." In addition, the EU rules do not make any exception for company-provided devices, even to merely track vehicle speed or traffic information, and the burden is on the data controller (employer) to prove that the need to track the employee outweighs the employees' fundamental human right of privacy.[25]

The EU Data Protection Supervisor, Peter Hustinx, has demanded that companies such as Apple, Google, and Facebook comply with new EU rules for managing geo-location data.[26] Meanwhile, consumers are turning to the courts for privacy protection.[27]

19 Ryan Gallagher, *Police Buy Software to Map Suspects' Digital Movements*, THE GUARDIAN, May 11, 2011, http://www.google.com/search?q=Police+Buy+Software+to+Map+Suspects%E2%80%99+Digital+Movements&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a.

20 Matthew Schwartz, *Americans Maximize Social Network Security,* INFORMATIONWEEK, Oct. 27, 2010, http://www.informationweek.com/news/security/privacy/228000157.

21 Misty Harris, *Adults and Teens Similar in What They Disclose Online*, THE VANCOUVER SUN, May 25, 2011, http://www.vancouversun.com/technology/Adults+teens+similar+what+they+disclose+online/4836701/story.html.

22 *Geolocation Services on Smart Mobile Devices*, Article 29 Data Protection Working Party 881/11/EN, WP 185, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf (Adopted May 16 2011).

23 Nick Bilton, *Tracking File Found in iPhones*, THE NEW YORK TIMES, Apr. 20, 2011, http://www.nytimes.com/2011/04/21/business/21data.html.

24 Miguel Helft, *Jobs Says Apple Made Mistakes With iPhone Data*, THE NEW YORK TIMES, Apr. 27, 2011, http://www.nytimes.com/2011/04/28/technology/28apple.html.

25 *Id.*

26 Eric Doyle, *EU Demands Explicit Geo-Location Permissions*, EWEEKEUROPE, May 20, 2011, http://www.eweekeurope.co.uk/news/eu-demands-explicit-geo-location-permissions-29614.

27 Antone Gonsalves, *Apple May Face More Privacy Lawsuits*, INFORMATIONWEEK, Dec. 30, 2010, http://www.informationweek.com/news/security/privacy/228900196.

Corporate CIO's see smartphones as a significant and growing information security hazard. The "consumerization" of enterprise IT—employees who want to connect personal consumer devices to the enterprise network—is a major challenge for information security according to 80% of surveyed CIOs. Ninety percent of organizations provide—or will soon provide—mobile devices to their employees.

New research also suggests that unique Smartphone identifiers (UUIDs) found on iPhones and other Apple devices, which are automatically set by Apple, and stay resident on the device forever, can create serious privacy risks. A Wall Street Journal study found that over 50% of popular Smartphone applications pass one or more unique Smartphone device IDs to third-party companies. Since it is likely that third parties link user information to these unique Smartphone IDs, this can potentially allow strangers to obtain personal information without the user's knowledge or consent. Apple acknowledges that when developers associate a device's unique identifier with a user account, it creates a significant security and privacy risk.[28]

Smartphones are considered by many CIOs as the weakest corporate information security link, meaning that a Smartphone security strategy is now a critical IT requirement.[29]

Google "Buzz"

On February 9, 2010, Google launched its "Buzz" application that automatically selected people for users "to follow" based on whom users communicate most frequently with via email. And the list of people users "followed" was made public as well—meaning that Google published, in effect, a list of the people with whom Google users most frequently emailed. And "Buzz" also made the user's Picasa Photograph Web Albums and Google Reader shared items public as well.

The launch of Google Buzz sparked outcry from users that their personal information was being disclosed without their express consent. And it prompted unified criticism from global data protection authorities.[30]

On November 2, 2010, Google settled a class-action lawsuit over alleged privacy breaches related to its Buzz social networking application. The FTC found that just about everything related to Buzz was flawed. Worst of all, Buzz violated Google's own published privacy policy that promises customers that their permission will be sought before it uses private information acquired for one product in another. In the settlement, Google paid $8.5 million into a fund for privacy education.[31] Another condition of the settlement is that Google submit to privacy audits every two years for a twenty-year period.[32]

Google "Street View" and Wi-Fi

In May 2010, Google revealed that its "Street View" cars—used to create the data for Google Maps—had inadvertently collected approximately 600GB of "fragmentary data" from unsecured home wireless networks in 34 countries over the prior two years. Google

28 Jennifer Valentino-DeVries, *The Privacy Risks of ID Codes in Your Apps*, THE WALL STREET JOURNAL, May 11, 2011, http://blogs.wsj.com/digits/2011/05/11/the-privacy-risks-of-id-codes-in-your-apps/.
29 Mathew Schwartz, *CIOs See Smartphones as Data Breach Time Bomb*, INFORMATIONWEEK, Nov. 19, 2010, http://www.informationweek.com/news/security/privacy/228900196.
30 *See* http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.pdf for the text of the April 19, 2010 letter.
31 Seth Weintraub, *Buzzkill: Google settles Google Buzz privacy suit for $8.5 million donation*, FORTUNE ONLINE, Nov. 2, 2010, http://tech.fortune.cnn.com/2010/11/02/buzzkill-google-settles-google-buzz-privacy-suit-for-8million-donation/.
32 Farhad Manjoo, *No More Privacy Paranoia*, SLATE, Apr. 7, 2011, http://www.slate.com/id/2290719/.

claimed that it was unaware that the Street View cars were capturing SSIDs and MAC addresses for open (i.e., unencrypted) wireless networks, as a means of enhancing location-based GPS services on SmartPhones.

Google argued that its collection of WiFi information was not a privacy violation because it was obtained from a public location. Nevertheless, Google acknowledged that the information collected from unsecured WiFi networks could include personal information, including emails and passwords.

Even before the WiFi information capture disclosure, Google's Street View program was under fire for the lack of digital masking of human bodies. Ireland, Denmark and Austria demanded that Google destroy the data collected. Australia, Canada, the Czech Republic, Italy, Spain, South Korea, the U.S., and the Netherlands launched investigations into Google's collection of data from wireless networks in their countries. Several asked Google to hand over the data so they could investigate the nature and extent of the intrusion. In May 2010, France's CNIL issued an injunction demanding that Google stop its practice and surrender its French WiFi data. The CNIL found that the project raised serious privacy concerns, from catching unsuspecting people in the nude to capturing passwords, online bank details, email, medical prescriptions, and connections to dating websites, resulting in a record fine of $141,234.[33]

German officials demanded, and Google agreed, that Google include an online tool by which users could request that their homes not be included on Street View. Over 250,000 Germans "opted-out" of the service, and asked for their homes to be pixelated (i.e., blurred).[34]

On May 27, 2010, a federal district court in Oregon ordered Google to turn over to the court for review two copies of WiFi data collected in its Street View program.[35]

Subsequent suits filed in Washington, D.C., Illinois, California, Pennsylvania, Oregon, and Massachusetts were consolidated in August 2010 before U.S. District Court Judge James Ware in the U.S. District Court for the Northern District of California on the basis that all the lawsuits allege claims under the federal Wiretap Act and involve similar facts: *In re Google Inc. Street View Electronic Communications Litigation*, MDL No. 10-2184-JW, Dec. 14, 2010.[36]

The Federal Trade Commission also conducted an investigation, but eventually abandoned it, despite considerable public criticism.[37]

---

33 Henry Samuel, *Google handed down record fine for violating French privacy laws*, THE TELEGRAPH ONLINE, Mar. 21, 2011, http://www.telegraph.co.uk/technology/google/8395410/Google-handed-down-record-fine-for-violating-French-privacy-laws.html.

34 Cecilia King, *After Bitter Row, Google Launches Street View in Germany*, AFP, Nov. 2, 2011 http://www.google.com/hostednews/afp/article/ALeqM5grZNAAuUs_pQv5an3zP7sZUW4hNg?docId=CNG.b5c5f5dd0d39f8bbf9bc33c2299b93ae.c1.

35 See *Van Valin v. Google, Inc.*, No. 3:10-CV-557-ST (D. Ore. May 24, 2010).

36 Thomson Reuters News & Insight, *Google Street View spawns 8th Class-Action Lawsuit*, Jan. 8, 2011, http://newsandinsight.thomsonreuters.com/California/news/2011/01_-_january/google_street_view_spawns_8th_class-action_lawsuit/.

37 Sidney Hill, *Privacy Advocates Blast FTC's Inaction Over Street View Spying*, TECHNEWSWORLD, June 3, 2011, http://www.technewsworld.com/story/71132.html?wlc=1307136795.

Google Video[38] Italy

The Google Video Italy matter involved the prosecution and conviction of three Google executives—Peter Fleischer, Senior Vice President and Global Privacy Counsel; David Drummond, Chief Legal Officer; and George Reyes, retired Chief Financial Officer—for alleged violation of Italy's data protection law.[39] Mr. Fleischer is no longer with Google. Italian law tends to hold CEOs responsible for any corporate function that they did not specifically delegate to a lower official.

The case arose from two short videos posted on Google Video in Italy on September 8, 2006 that depict an autistic student being jostled and ridiculed by four classmates at a secondary school in Torino, Italy, in May 2006. In the first of the two videos, which were filmed on a student's cell phone, one of the classmates insinuated that the autistic student had Down's Syndrome and made a sarcastic reference to a local Down Syndrome support group called Vivi Down.

Vivi Down complained to the local authorities and subsequently filed a criminal complaint for defamation with the public prosecutor's office in Milan. The charges arising under the Italian data protection law were added much later. The four students responsible for the video were convicted, with Google's cooperation, and were sentenced by a juvenile court.

Italian prosecutors charged that Google was liable criminally in that they should have had a process for identifying and removing the video much sooner. Italian Prosecutor Alfredo Oblado argued that "The right to do business cannot prevail over fundamental human rights" and that "it is not freedom of expression that is at stake, but the responsibility of companies."

Legal commentators were particularly surprised by the result because under the U.S. Digital Millennium Copyright Act[40] as well as the EU e-Commerce Directive, the hosting site is not liable if it promptly removes objectionable material when notified.[41.] Google argued that to hold their executives responsible would be like prosecuting the postman for delivering a letter that was upsetting, or prosecuting the telephone operator for a harassing phone call. [42]

This case is not unique. In 1995, the Munich-based General Manager of U.S.-based CompuServ, Felix Somm, was arrested and later convicted in Germany on charges of spreading pornography because sexually explicit content was available on CompuServ in Germany.[43] This was even though Somm—like Google's executives—had absolutely nothing to do with either the creation or dissemination of the material. Somm's conviction was overturned two years later.[44]

---

38 The video was posted on Google Video shortly before Google Video acquired YouTube, which became the successor entity.

39 Article 167 of the Italian Data Protection Law (Unlawful Data Processing, Italian Personal Data Protection Code, Legislative Decree No. 196 of 30 June 2003), *available at* http://www.privacy.it/privacycode-en.html.

40 17 U.S.C. Sections 512, 1201(a)(1).

41 *See* Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, http://ec.europa.eu/internal_market/e-commerce/directive_en.htm.

42 Sylvia Poggioli & Steve Inskeep, *Google Case In Italy Raises Web Freedom Concerns,* NPR, Feb. 25, 2010, http://www.npr.org/templates/story/story.php?storyId=124068000.

43 Alan Cowell, *Ex-CompuServe Head Sentenced in Germany,* THE NEW YORK TIMES, May 29, 1998, http://www.nytimes.com/library/tech/98/05/biztech/articles/29compuserve.html.

44 Edmund L. Andrews, *German Court Overturns Pornography Ruling Against Compuserve,* THE NEW YORK TIMES, Nov. 18, 1999, http://www.nytimes.com/1999/11/18/business/international-business-german-court-overturns-pornography-ruling-against.html.

Similarly, in 2008, several courts in Argentina required Google and Yahoo to block searches and remove content posted by Argentine celebrities, including the now-former animated Argentine World Cup Football Coach, Diego Maradona.[45]

Some commentators see the Google Italy case as a sign of a more fundamental collision between liberty and privacy.[46] American law focuses primarily on reducing intrusions by the state; while continental law concentrates on ensuring affirmative protection of one's public persona vis-a-vis the state and other persons. These differences reflect the contrasting political and social ideals of American and continental law.[47]

"Google Maps" and "Google Me"

With Google's Places, users can now check in and "tag" friends, with their specific GPS coordinates, and this information is publically available if the user's privacy control has been set to "everyone."

Google has also launched a new social network called "Google Me"—a competitor to Facebook—that integrates features of a recently acquired game-oriented virtual currency company called Jambool, a social gaming company Zynga, a social networking apps company Slide, and a microblogging service Jaiku.

Google Privacy and Disclosure Concerns

In May 2011, a University of Amsterdam Professor demonstrated how easy it is to obtain private information from online resources such as Google. Using a process known as Internet data "scraping," the Professor created a database of 35 million Google Profiles in one month. The data, over 35 GB in volume, included usernames, Gmail™ addresses, educational backgrounds, work histories, Twitter conversations, links to Picasa photo albums, and other personal information.[48]

In July 2010, an independent researcher compiled the names and unique URLs of 100 million Facebook users and made them available for public download. This allowed the profile pages to be visible, even if the users changed their privacy configurations later.[49]

Facebook Privacy and Disclosure Concerns

Facebook is a social networking platform that boasts over 600 million users worldwide, and counting. In July 2009, Canadian Privacy Commissioner, Jennifer Stoddart, released findings of an investigation into Facebook's handling of personal information of its members and recommended that Facebook give members better privacy controls. In December 2009, Facebook implemented some changes and required its members to review their settings. Some users complained that the changes no longer allowed users to selectively conceal certain private information, creating a new problem.[50]

---

45 Techdirt, *Argentinian Celebrities Succeed In Forcing Search Engines To Block Search Results On Their Name,* Nov. 12, 2008, http://www.techdirt.com/articles/20081112/0215062808.shtml.
46 James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty,* 113 YALE L.J. 1151 (2004), http://www.yalelawjournal.org/images/pdfs/246.pdf.
47 *Id.*
48 Dan Goodwin, *35m Google Profiles Dumped into Private Databases*, THE REGISTER, May 25, 2011, http://www.theregister.co.uk/2011/05/25/google_profiles_database_dump/.
49 *Id.*
50 The Tech Chronicles, *Canada's privacy commissioner launches new Facebook page,* THE SAN FRANCISCO CHRONICLE, Jan. 7, 2010, http://www.sfgate.com/cgi-bin/blogs/techchron/detail?entry_id=56175.

In May 2010, German authorities announced that Facebook's privacy controls that required users to actively opt out of default settings that made their data public violate German law.[51] Under Germany's Telemedia Act, a website—even a foreign-based web service doing business in Germany—must obtain a user's permission ("opt-in") before passing personal data to a third party.

In November 2010, Facebook launched "Facemail," which integrates seamless email messaging, a social inbox, and a conversation history. Facemail retains this information "indefinitely." This can create some issues with respect to records retention, legal holds, and third-party e-discovery subpoena practice. That is, what happens if Facebook has information that the company has no longer retained because there was no legal obligation to do so at the time it was retired? Do those under legal hold need to put Facebook on notice to retain information relevant to their legal holds? What recourse does a party have if their "old" information is subpoenaed directly from Facebook, without their knowledge or consent?[52]

Data security is also an issue. Researchers at Microsoft in India and at the Max Planck Institute for Software Systems in Germany have demonstrated that although Facebook does not share sensitive profile information with advertisers, nevertheless, they are able to determine the gender, sexual preference, religious preference, political affiliation, and other personal information just by analyzing data from ads that are "clicked" by the users.[53]

In August 2010, German legislation banned the use of information from social networking sites when used in the employment process, but permitted the use of publically available information on job networking site, such as LinkedIn.[54]

Employers have also taken fire from the NLRB for employment-related discipline based upon Facebook postings. The NLRB has ruled that disciplining employees for making complaints about working conditions, workload, and staffing on Facebook or other social networking sites is an unfair labor practice.[55] Similarly, the NLRB has ruled that an employer cannot restrict an employee's right to use Twitter to discuss working conditions with co-workers.[56]

One thing is certain: Facebook is not going away. Social networking has reached a "tipping point," and CEO's as well as politicians have realized that if they are not leading the digital conversation and agenda, someone else will do it for them.[57]

---

51 As of March 2010, 7.7 million of Germany's 82 million residents were on Facebook compared with 113 million of 309 million U.S. residents.

52 Shannon Green, *Facebook Creates New Mess for EDD: Messages*, LAW.COM, Nov. 23, 2010, http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202475235725&Facebook_Creates_New_Mess_for_EDD_Messages&slreturn=1&hbxlogin=1.

53 Miguel Helft, *Marketers Can Glean Private Data on Facebook*, NEW YORK TIMES, Oct. 22, 2010, http://www.nytimes.com/2010/10/23/technology/23facebook.html.

54 *German Law Bans Facebook Research for Hiring Decisions*, INFORMATION POLICY BLOG, Aug. 29, 2010, http://www.i-policy.org/2010/08/german-law-bans-facebook-research-for-hiring-decisions.html.

55 Leigh Kamping-Carder, *NY Nonprofit Incurs NLRB Wrath Over Facebook Firing*, LAW 360, May 18, 2011, http://www.law360.com/topnews/articles/246042/ny-nonprofit-incurs-nlrb-wrath-over-facebook-firing.

56 Leigh Kamping-Carder, *NLRB Targets Reuters Over Twitter Policy*, LAW 360, Apr. 7, 2011, http://www.law360.com/topnews/articles/237504/nlrb-targets-reuters-over-twitter-policy; *see also,* Nick Madigan, *Officer Forced to Reveal Facebook Page*, THE BALTIMORE SUN, Feb. 23, 2011.

57 Matthew Fraser, *Yes, CEOs Should Facebook and Twitter*, FORBES.COM, Mar. 11, 2009, http://www.forbes.com/2009/03/11/social-networking-executives-leadership-managing-facebook.html.

Facebook "Facial Recognition" Feature

The EU plans to investigate Facebook over its new facial recognition feature that suggests people's names to tag in pictures, without their permission, as a default setting. In the U.S., the Electronic Privacy Information Center, a non-profit privacy advocacy group, is pursuing a complaint with the U.S. Federal Trade Commission with respect to this issue.[58] Google announced that it will not develop a facial recognition database in response to public input.[59]

Facebook "Places"

On August 18, 2010, Facebook launched its new "Places"[60] geo-locations service that permits users and their "friends" to track each others' movements. The new features are similar to other location startups such as Foursquare, Yelp, Gowalla and Booyah, which claim integration with "Places." Use of "Places" requires the most recent version of the Facebook application for mobile phones or moble browsers that support HTML 5 and geolocation functionality.[61]

Facebook and "Professional Ethics"

The Florida Bar Association Board of Bar Examiners visits Facebook and MySpace sites on an ad hoc basis as part of their background investigations of the "good moral character and fitness" of applicants to the bar.[62] Other states are likely to follow suit, and perhaps expand their inquiry into questions of whether such sites constitute unauthorized attorney advertising or solicitation.

MySpace

MySpace has also been accused of security shortfalls. Although its footprint has decreased 29% to 62.6 million visitors in 2011 (from 88 million in October 2010), it nevertheless is the subject of class action litigation claiming that it has sold personal data—including names, IP addresses, and Internet browsing history—to data marketing "aggregators" without the users' consent.[63]

"Twitter"

Twitter is a social networking and microblogging service with over 300 million users worldwide that enables its users to send and read other users' messages called tweets. Tweets are text-based posts of up to 140 characters displayed on the author's profile page. Tweets are publicly visible by default; however, senders can restrict message delivery to their friends list. Users may subscribe to other author tweets—this is known as following and

58 *Facebook 'Face Recognition' Feature Draws Privacy Inquiries*, THE NEW YORK TIMES, June 8, 2011, http://www.nytimes.com/2011/06/09/technology/09facebook.html.
59 Carrie Ann Skinner, *Google Won't Develop a Facial Recognition Database*, PC ADVISOR, May 19, 2011, http://www.pcadvisor.co.uk/news/internet/3280727/google-wont-develop-a-facial-recognition-database/.
60 Michael Eyal Sharon, *Who, What, When, and Now...Where,* THE FACEBOOK BLOG, Aug. 18, 2010, http://blog.facebook.com/blog.php?post=418175202130.
61 *Id.*
62 Jan Pudlow, *On Facebook? FBBE May be Planning a Visit*, THE FLORIDA BAR NEWS, Sept. 1, 2009, http://www.floridabar.org/DIVCOM/JN/jnnews01.nsf/8c9f13012b96736985256aa900624829/d288355844fc8c728525761900652232?OpenDocument.
63 See *Virtue v. MySpace Inc.*, 11-CV-1800 (E.D.N.Y. Apr. 13, 2011); also Geoffrey Fowler and Emily Steel, *MySpace, Apps Leak User Data*, THE WALL STREET JOURNAL, Oct. 23, 2010, http://online.wsj.com/article/SB10001424052702303738504575568460409331560.html.

subscribers are known as followers. All users can send and receive tweets via the Twitter website, compatible external applications (such as, for example, Smartphones), or by Short Message Service (SMS) available in certain countries.

Twitter raises obvious data privacy, data security, and confidentiality concerns. It is "viral" in nature, it is mobile, and Twitter communications may be archived outside one's control. Twitter worms attacks have been documented, and Twitter users have reported burglaries related to tweets stating they are on vacation. Text and Twitter monitoring has also been on the rise in domestic dispute contexts, *ala* Tiger Woods.

Organizations that permit Twitter for business or personal purposes are well advised to develop social media policies governing its responsible use. For example, although it may not be well understood, an organization's cross-border disclosure and data privacy compliance and legal hold obligations apply as equally to Twitter as to any other communication platform.

WikiLeaks

WikiLeaks is an international non-profit organization that launched a wiki-site in 2000 to publish submissions of private, secret, and classified media from anonymous news sources, news leaks, and whistleblowers.

In January 2011, Twitter won a legal battle for the right to reveal that it had been ordered to give U.S. security forces access to data on all 637,000 people who follow the WikiLeaks Twitter account, including source, destination email addresses, and IP addresses. This prompted immediate objections from German, Dutch, Polish, and a host of other global Data Protection Authorities.[64]

Smartphones and Security

The use of Smartphones for mobile computing is exploding. In the third quarter of 2010 alone, over 80 million Smartphones were purchased worldwide.[65] Recently, some security flaws in some major Smartphone applications were revealed that could jeopardize the privacy of hundreds of millions of users. For example, a recent Rice University study demonstrates that cell phones running the Android operating system fail to encrypt data sent to and from Facebook and Google Calendar, threatening to jeopardize the privacy of hundreds of millions of consumers—particularly those that use unsecured wireless networks.[66] Facebook warns users to exercise caution when using unsecured Wi-Fi networks, but does not explicitly state that its Smartphone App fails to encrypt traffic.[67]

The Android's Mobile applications for LinkedIn, Netflix, and Foursquare capture user names, passwords, and other forms of users' sensitive personal data in unencrypted, plain text on a mobile device, putting sensitive personal data at risk.[68] The iPhone's version of Square's mobile payments application exposes a user's transaction account history and

64 *U.S. Anti-Twitter Subpoena Fuels Data Privacy Debate*, EUOBSERVER.COM, Jan. 11, 2011, http://euobserver.com/891/31614.
65 Office of the Privacy Commissioner of Canada, *Outsmart your Smart Phone this Holiday Season*, Dec. 21, 2010, http://www.priv.gc.ca/media/nr-c/2010/nr-c_101221_e.cfm.
66 Dan Goodwin, *Security Shocker: Android Apps Send Private Data in Clear – Facebook's Persistent SSL Isn't*, THE REGISTER ONLINE, Feb. 24, 2011, http://www.theregister.co.uk/2011/02/24/android_phone_privacy_shocker/.
67 *Id.*
68 Spencer Ante, *Some Top Apps Put Data at Risk*, THE WALL STREET JOURNAL, June 8, 2011, http://blogs.wsj.com/digits/2011/06/08/some-top-apps-put-data-at-risk/.

digital signature.[69] Data Protection officials in Italy, Germany, and France are investigating whether, and to what extent, the collection of location data by Apple's iPhones and Google's Android, without prior user consent, is a violation of the new e-Privacy Directive.[70]

EU Justice Commissioner Viviane Reding has noted that "Mobile phones and computers have become tracking devices. We no longer roam unseen across the net."[71] In contrast, China plans to use mobile phones to monitor and manage traffic in real time, starting in June 2011.[72] The traffic engineering application will be based upon the geo-location data of over 17 million China Mobile subscribers. This will allow transportation engineers to optimize public and private transportation patterns, reducing the $1.8B annual cost of traffic congestion in Beijing.

Online Tracking

In its Internet Explorer 9 release in early 2011, Microsoft introduced a "do not track" option called "Tracking Protection" that allows consumers to opt out of having third-party companies track and collect their data online. This feature attempts to respond to the Preliminary FTC Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change (Dec. 2010)," which calls for a "Do Not Track" feature to be built into software applications. The limitation of the Microsoft offering is that it requires the user to manually designate a list of sites with whom they do not want to share information. This list of third-party "trackers" is not easy to develop or maintain. This "Do Not Track" functionality highlights a fundamental tension with the online advertising community that argues that a government-mandated "Do Not Track" system can negatively impact the free flow and expansion of global commerce.[73]

Retinal Tracking

Another new technology tracks what users view on a computer screen, without the use of special glasses or headgear. It relies on low levels of infrared light that are beamed at the users' eyes, and sensors that detect the reflection of the light off the user's retinas and corneas. Although still in development, it is another step forward in the potential ability to track movement, thought and intention via a ubiquitous, invisible technology, thereby raising privacy concerns.[74]

FourSquare Stalking

One unintended consequence of geo-tracking applications like Facebook Places and FourSquare is that your identity may become indelibly linked to a location, and published far beyond your wildest dream (or nightmare). This is what happened to a New York Times reporter who rather naively claimed the title of "mayor" of a restaurant, only to

69 *Id.*
70 Fahmida Rashid, *EU e-Privacy Cookie Rules Will Impact Non-European Web Companies*, IT SECURITY & NETWORK NEWS, May 23, 2011, http://www.eweek.com/c/a/Security/EU-ePrivacy-Cookie-Rules-Will-Impact-NonEuropean-Web-Companies-699225/.
71 Stephanie Bodoni, *Internet Tracking May Threaten Privacy Rights*, *EU's Reding Says*, BLOOMBERG, Feb. 9, 2011, www.bloomberg.com/news/2011-02-09/internet-tracking-may-threaten-privacy-rights-eu-s-reding-says.html+Internet+Tracking+May+Threaten+Privacy+Rights&cd =1&hl=en&ct=clnk&gl=us&client=firefox-a&source=www.google.com.
72 Jianggan Li, *Beijing to Monitor Real-Time Traffic through Mobile Platform*, FUTUREGOV, Mar. 3, 2011, http://www.futuregov.asia/articles/2011/mar/03/beijing-monitor-real-time-traffic-through-mobile-p/.
73 Tanzina Vega, *Microsoft, Spurred by Privacy Concerns, Introduced Tracking Protection to Its Browser*, THE NEW YORK TIMES, Dec. 7, 2010, http://www.nytimes.com/2010/12/08/business/media/08soft.html.
74 Troy Wolverton, *Eye Tracking' May be Coming to your Computer*, MERCURY NEWS, Mar. 21, 2011, http://www.mercurynews.com/breaking-news/ci_17637310?nclick_check=1.

be contacted personally by a secret digital admirer.[75] New applications such as Gravity allow individuals and businesses to "mine" Facebook and Twitter traffic. Countermeasures to these tools, such as Canvas Networks and Disconnect, disable third-party tracking while surfing and allow some measure of anonymity.[76]

Flash Cookies

The EU's security agency, ENISA, is warning about a new type of persistent brand of online tracking cookie that can be abused for profiling and tracking.[77] These cookies, known as "flash cookies," are small files stored on a user's computer that track activity, and that can "respawn" themselves even after they have been deleted.[78]

New EU Cookie Consent Law

On May 26, 2011, the EU's new "cookie law" went into effect, requiring consent from users to store "cookies" on their computers.[79] The Directive was amended in October 2009, and states that national governments of EU member states must "ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his/her consent, having been provided with clear and comprehensive information." This amendment was required to be interpreted and implemented in each EU member state by May 2011. However, according to most regulators and commentators, the EU's revised Privacy and Electronic Communications Regulations went into effect without sufficient clarity, leaving businesses and organizations without clear guidance.[80]

As of May 26, 2011, only two EU member states—Estonia and Denmark—had issued a full notification to Brussels that they had integrated the "cookie consent" rule into their national laws.[81] The UK has provided a one-year "grace period" for websites to implement the new law,[82] and has provided some helpful practical instructions to UK businesses and organizations subject to the law.[83]

The EU privacy cookie law also applies to non-European web companies.[84] Indeed, any company doing business in the European Union is expected to comply with the EU's new cookie consent law.[85]

75 Jenna Wortham, *So Much for Reinventing Ourselves Online*, THE NEW YORK TIMES, Dec. 18, 2010, http://www.nytimes.com/2010/12/19/business/19ping.html.
76 *Id.*
77 Dave Neal, *ENISA Warns on Cookie Security Threats*, V3.CO.UK, Feb. 18, 2011, http://www.v3.co.uk/v3-uk/news/2030906/enisa-warns-cookie-security-threats.
78 Jennifer Valentino-DeVries, *Adobe Aims to Improve Privacy Settings in Flash*, WSJ BLOGS, Jan. 13, 2011, http://blogs.wsj.com/digits/2011/01/13/adobe-aims-to-improve-privacy-settings-in-flash/.
79 UK Information Commissioner's Office Public Guidelines, *Changes to Rules on Using Cookies and Similar Technologies for Storing Information*, May 9, 2011, http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.pdf.
80 Slobhain Butterworth, *Cookie Law Shambles Really Takes the Biscuit*, THE GUARDIAN, May 27, 2011, http://www.guardian.co.uk/law/butterworth-and-bowcott-on-law/2011/may/27/cookie-law-shambles-web-browsers; *see also* Jack Marshall, *Europe Continues to Grapple with Messy Cookie Law Situation*, CLICKZ, Nov. 4, 2010, http://www.clickz.com/clickz/news/1869453/europe-continues-grapple-messy-cookie-law-situation.
81 Kelly Fiveash, *Almost Entire EU now Violating Brussels Cookie Privacy Law*, THE REGISTER, May 26, 2011, http://www.theregister.co.uk/2011/05/26/european_cookies_law_ignored/.
82 *Id.*
83 UK Information Commissioner's Office Public Guidelines, *Changes to Rules on Using Cookies and Similar Technologies for Storing Information*, May 9, 2011, http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.pdf.
84 Fahmida Rashid, *EU e-Privacy Cookie Rules Will Impact Non-European Web Companies*, IT SECURITY & NETWORK NEWS, May 23, 2011, http://www.eweek.com/c/a/Security/EU-ePrivacy-Cookie-Rules-Will-Impact-NonEuropean-Web-Companies-699225/.
85 *Id.*

In addition, The World Wide Web Consortium (W3C), a global Internet standards group, is studying how cookie-based opt-out features can work with browser tools to communicate and enforce user privacy preferences.[86] Mozilla, Microsoft, and Apple are all introducing a "Do Not Track" feature, which will block tracking, but not the delivery of content.[87] In contrast, Google has noted that tracking can benefit Web users by providing useful and efficient suggestions as to products and services that may be of interest to them.[88] A big part of the policy challenge is that "tracking" takes several forms. It can describe following a user across multiple sites or sessions, watching repeated sessions on the same site, and correlating browsing behavior and patterns with personally identifiable information gained from user input or system screens.[89]

Another emerging technology that has caused concern for privacy advocates is "device fingerprinting," such as BlueCava or Ringleader Digital, which uniquely and persistently links to connected devices such as computers, Smartphones, and tablets. This allows advertisers to use this specific "device fingerprint" to track the behavior of the device as it moves across the web; and unlike a cookie, it cannot be deleted or lost. It persists for the entire lifecycle of the device. This creates a potential threat to privacy, because it is so durable. On the other hand, the same characteristic makes an "opt out" much more reliable and persistent that a cookie-based opt-out, which is lost when cookies are deleted, or browsers are changed.[90]

Smart Grid and Home Monitoring Technology

Wireless smart meters that monitor power usage information from homes and transmit this information to the public or private utility company are being introduced throughout the United States and globally.[91] These devices have raised concerns that public or private organizations may abuse this information, or that the additional electromagnetic radiation that it generates may be hazardous to physical health.[92] A recent survey by the Ponemon Institute indicates that respondents are most worried that the Smart Grid's collection of personal information will threaten their personal safety and security, as well as reveal personal details about their movements, activities, and general lifestyle.[93]

California has recently proposed Smart Grid data privacy standards for handling customer data.[94] The proposal requires that information only be used for its intended purpose—to calculate energy consumption and charges—unless the customer provides express written permission.[95] It also requires utility companies to use "reasonable security procedures and practices to protect a customer's unencrypted electrical or gas consumption data from unauthorized access, distribution, use modification or disclosure."[96]

86 *Id.*
87 *Id.*
88 Wendy Davis, *Web Standards Group to Tackle Do-Not-Track*, MEDIAPOSTNEWS, Apr. 23, 2011, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=149201.
89 *Id.*
90 Jack Marshall, *Device Fingerprinting Raises Privacy Fears*, CLICKZ, Mar. 21, 2011, http://www.pogowasright.org/?p=21849.
91 Fahmida Rashid, *EU e-Privacy Cookie Rules Will Impact Non-European Web Companies*, IT SECURITY & NETWORK NEWS, May 23, 2011, http://www.eweek.com/c/a/Security/EU-ePrivacy-Cookie-Rules-Will-Impact-NonEuropean-Web-Companies-699225/.
92 Felicity Barringer, *New Electricity Meters Stir Fears*, THE NEW YORK TIMES, Jan. 30, 2011, http://www.nytimes.com/2011/01/31/science/earth/31meters.html.
93 *New Ponemon Study Points to Need for Smart Grid Education*, PONEMOM.ORG, Dec. 14, 2010, http://www.ponemon.org/news-2/39.
94 Mathew Schwartz, *California Proposes Smart Grid Data Privacy Standards*, INFORMATIONWEEK, May 18, 2011, http://www.informationweek.com/news/government/state-local/229502439.
95 *Id.*
96 *Id.*

In France, CNIL has worked with the Commission for Energy Regulation (CRE) on the "smart meter" issue.[97] On October 14, 2010, the CNIL developed recommendations to limit the impact of smart meter devices on data privacy and freedoms.[98] The CNIL observed that without new security requirements, an unauthorized malicious third party could remotely cut the power supply of an individual.[99] And without proper electronic surveillance and data capture, infrastructure security attacks, such as the recent Stuxnet virus in Iran, can disrupt operation of and damage power stations, possibly causing a chain reaction on the whole electricity grid and large scale power outages.[100]

Radio Frequency Identification (RFID) Technology

RFID tagging technology is being used to track not only shipments of goods, but also locations of infants in nursery wards and toddlers in shopping centers.[101] On February 11, 2011, the Article 29 Working Party issued Opinion 9/2011 (WP 180) on the "Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications."[102] WP 180 reinforces the call made in WP 168 ("The Future of Privacy") for transparency, accountability, and Privacy by Design to be embedded in the System Development Life Cycle (SDLC) of technology, particularly as it relates to the appropriate and proportional use of RFID technologies.[103]

DNA and Biometrics

The collection and retention of DNA and other biometric identification is an increasing concern to data privacy and protection and legal professionals. The UK's highest court has found that indefinite retention of criminal suspects' DNA violates their human right to privacy.[104]

In addition, although the U.S. has used familial DNA matching for years, Canadian law enforcement authorities are questioning whether familial matching is legal under their data privacy laws, given that DNA profiling raises so many privacy, civil liberty and equity concerns.[105]

Even in the U.S., privacy concerns have been raised over the indefinite retention of newborn blood samples. Minnesota and 17 other states allow the retention of newborn blood samples for genetic and DNA testing. There is a concern that not all parents are made aware of the specific state policies and practices in this regard. The Johns Hopkins Berman Institute of Bioethics has called for a more transparent notification process going forward.[106]

97 *Recommendations for the Deployment of Electric 'Smart Meters'*, CNIL NEWS, Dec. 6, 2010, http://www.cnil.fr/english/news-and-events/news/article/recommendations-for-the-deployment-of-electric-smart-meters/.
98 *Id.*
99 *Id.*
100 *Id.*
101 Alastair Jamieson, *Parents Offered Electronic Tags for Children in Shopping Centre*, THE TELEGRAPH, Jan. 19, 2009, http://www.telegraph.co.uk/family/4286028/Parents-offered-electronic-tags-for-children-in-shopping-centre.html.
101 *Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*, Article 29 Data Protection Working Party 00327/11/EN, WP 180, http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-a29wp-opinion-11-02-2011_en.pdf (Adopted Feb. 11, 2011).
103 *Id.*
104 *Indefinite Retention of DNA Samples is Unlawful under European Human Rights Law*, OUT-LAW News, May 19, 2011, http://securlinx.blogspot.com/2011/05/indefinite-retention-of-dna-samples-is.html.
105 Douglas Quan, *U.S. Using Familial DNA in Policing*, THE VANCOUVER SUN, May 21, 2011, http://www.vancouversun.com/technology/using+familial+policing/4821789/story.html.
106 Lorna Benson, *Privacy Debate Surrounds Use of Newborns' Blood Samples*, MPR NEWS, Apr. 12, 2011, http://minnesota.publicradio.org/display/web/2011/04/12/newborn-health-screening/.

In *United States vs. Ruben Mitchell*, the Third Circuit Court of Appeals is considering whether routine DNA sampling should be considered like fingerprinting or photographing, or whether, as ruled by District Judge David S. Cercone, a warrant is required.[107]

Most recently, on January 10, 2011, a new Rule of the Equal Employment Opportunity Commission became effective to implement the Genetic Information Nondiscrimination Act of 2008 (GINA). The Act, enacted in 2008, protects job applicants, current and former employees, labor union members and apprentices, and trainees from discrimination based on their genetic information. To protect privacy, it restricts employers from requesting, purchasing, or disclosing genetic information.[108]

(2) Behavioral Marketing and Profiling

Privacy has become a commodity. Personal data is in high demand by advertising and marketing professionals, with hundreds of companies collecting and selling personal data about online usage, political views, health, shopping, and finances.[109] A class action lawsuit against Amazon.com alleges that Amazon.com fraudulently hijacks browser privacy settings to collect personal information without permission and sell it to third-parties.[110] And unlike the UK, the U.S. does not yet have a law that requires companies to honor requests to remove personal data from marketing databases.[111]

One particularly intrusive form of profiling technologies is known as "deep packet inspection," which is capable of reading and analyzing bits of data travelling across the Internet.[112] This kind of technology is used for sophisticated espionage because it can monitor all online activity—not just browser activity. Two companies, Kindsight and Phorm, offer deep packet inspection technology for marketing and advertising purposes. Kindsight says that its technology can actually distinguish whether a person is using the Internet for personal or business reasons.[113]

Last year, two UK ISPs that were testing deep packet inspection abandoned it due to privacy concerns. In the U.S, a 2008 plan to use deep packet inspection to deliver targeted advertising to broadband customers unless they opted out was also abandoned because of concerns that it would not pass FTC scrutiny. The reality is that with deep packet inspection technology, Internet Service Providers can harvest much more personal information about consumers than can applications such as Google or Facebook.[114]

On June 12, 2009, the Article 29 Working Party issued its opinion on online social networking, 01189/09/EN (WP 163).[115] WP 163 accurately observes that online personal information and activity can create a "rich profile of that person's interests and post

107 *See* Case No. 2:09cr105, (W.D.Pa. Nov. 6, 2009).
108 Howard Anderson, *Genetic Nondiscrimination Rule Unveiled*, HEALTHCAREINFOSECURITY, Nov. 10, 2010, http://www.govinfosecurity.com/articles.php?art_id=3084; *see also Regulations Under the Genetic Information Nondiscrimination Act of 2008*, http://www.federalregister.gov/articles/2010/11/09/2010-28011/regulations-under-the-genetic-information-nondiscrimination-act-of-2008.
109 Julia Angwin, *Web's Hot New Commodity: Privacy*, THE WALL STREET JOURNAL, Feb. 18, 2011, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.
110 Nick Eaton, *Suit: Amazon Fraudulently Collects, Shares Users' Personal Info*, SEATTLEPI.COM, Mar. 2, 2011, http://www.seattlepi.com/business/article/Suit-Amazon-fraudulently-collects-shares-users-1040886.php.
111 *Id.*
112 Steve Stecklow, *Shunned Profiling Technology on the Verge of a Comeback*, THE WALL STREET JOURNAL, Nov. 24, 2010, http://online.wsj.com/article/SB10001424052748704243904575630751094784516.html.
113 *Id.*
114 *Id.*
115 *Opinion 5/2009 on online social networking*, Article 29 Data Protection Working Party 01189/09/EN, WP 163, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf (Adopted June 12, 2009).

major risks such as identify theft, loss of employment or reputational damage."[116] For example, on July 4, 2010, a British tabloid published revealing photos from a social networking site of the incoming chief of the country's foreign intelligence service, MI6.[117]

Providers like Facebook and MySpace are required to implement default security and privacy settings that restrict viewing of the user's profile to self-selected "friends," to inform users of the privacy risks of sharing personal information, and to require consent before uploading information or pictures of third parties. They are also expected to require the explicit consent of the data owner (i.e., opt-in) before posting personal data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, health, or sex life." In addition, providers may not use third-party information to create profiles for non users, and must ensure that when sharing information with third parties with the users' consent (e.g., mobile phone and other web services), that users have a reporting mechanism for complaints about how the third parties are using their personal information.

All marketing activity must comply with the EU directive. Personal data should be destroyed when an account is deleted or inactive for a designated period of time. As well, users must have the right to access, correct, and delete their personal data, and it must not be used for any purpose beyond its intended use. The Article 29 Working Party also suggests that providers consider giving users the option of using pseudonyms in place of real names, but this seems to defeat the purpose of such social networking sites.

Lastly, providers are expected to give particular protection to personal information of minors. Subscription forms, rather than direct marketing are recommended for requesting personal information from minors so that the consent of parents can be sought. As well, WP 163 recommends segregating adult and minor "spaces" and requiring age verification to access either space.[118]

(3) Cloud Computing, Data Security and Privacy

Cloud Computing

Data Privacy and protection knows no boundaries—it extends to the heavens.[119]

The notion that a data subject's substantive rights transcend space raises a host of practical issues for cross-border disclosure and data privacy. Third-party data hosting, SaaS (Software as a Service) offerings, server virtualization, and cloud computing environments create new challenges for data controllers and data processors.

In this context, cloud computing is generally used to describe services through which an organization can access software operating systems, applications, databases, networking and disaster recovery infrastructure, and related services via the Internet or other networks. This often provides significant cost savings by removing the need for each organization to be its own "IT island" that is forced to react to frequent technology developments.

116 *Id.*
117 Kirsty Walker, *Farce of the Facebook spy: MI6 chief faces probe after wife exposes their life on Net,* MAIL ONLINE, July 6, 2009, http://www.dailymail.co.uk/news/article-1197757/New-MI6-chief-faces-probe-wife-exposes-life-Facebook.html.
118 *Id.*
119 *The Future of Privacy*, Article 29 Data Protection Working Party 02356/09/EN, WP 168 at 9, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf (Adopted Dec. 1, 2009). ("The EU and its Member States should guarantee this fundamental right for everybody. In a globalised world, this means that individuals can claim protection also if their data are processed outside the EU.")

A recent publication of the Data Protection Authority of the German Federal State of Schleswig-Holstein, known as the ULD,[120] suggests that many of the emerging public cloud computing environments may not satisfy requirements of the German Data Protection Act.[121] The ULD opines that companies must include EU model contractual provisions with Cloud Computing services that incorporate data controller and data processor data protection obligations (regardless of the location of the Cloud Computing environment), including measures to protect the integrity and security of the data. And to prove compliance, the company must obtain either an audit certificate by a qualified third party or a binding declaration of the Cloud Computing service to abide by data protection obligations.[122]

If a U.S. law firm, for example, wants to review personal data collected in the EU for relevance or privilege in relation to a U.S. matter, what are the data processing and transfer implications if the firm creates a remote connection, perhaps via a "thin-client" such as Citrix—that transmits only screen shots of the data and not the data itself? Does access via the Internet in this fashion constitute a prohibited processing and/or transfer of the data?[123] Understanding where the data lives, where it is stored, and who has access to it is a central issue in cloud computing compliance. Clearly, cloud computing environments greatly complicate the legal, technical, and practical issues relating to cross-border discovery and disclosure.[124]

The National Institute of Science and Technology (NIST) has issued draft guidelines for managing security and privacy in the cloud in SP 800-144: Guidelines on Security and Privacy in the Public Cloud (Feb. 2, 2011). The NIST draft guidelines suggest the following steps:

- Carefully plan the security and privacy aspects of cloud computing solutions before engaging them;
- Understand the public cloud computing environment offered by the cloud provider and ensure that a cloud computing solution satisfies organizational security and privacy requirements;
- Ensure that the client-side computing environment meets organization security and privacy requirements for cloud computing; and
- Maintain accountability over the privacy and security of data and applications implemented and deployed in public cloud computing environments.[125]

The EU has called for a "cloud friendly" and "cloud active" cloud strategy in Europe. One practical application highlighted by EU regulators is the ability to provide medical information efficiently across borders. Other applications of cloud technology in Europe include a "Cows in the Cloud" project by a Dutch company, in which sensors placed in cows' ears wirelessly relay information about their vital signs. Another project

120 *Unabhängiges Zentrum für Datenschutz Schleswig-Holstein* (ULD)
121 The German Data Protection Act (Bundesdatenschutzgesetz – BDSG) implements the EU Data Protection Directive.
122 *Id.*
123 *See*, for example, *Criminal Proceedings for Bodil Lindqvist*, European Court of Justice, Nov. 6, 2003, Case C-101/01; *see also* Opinion of Advocate General Leger, Case C-318/04 (Nov. 22, 2005) and subsequent Judgement of the European Court of Justice (May 30, 2006).
124 Mark Austrian & Michael Ryan, *Cloud Computing Meets e-Discovery*, CYBERSPACE LAWYER, v. 14, Issue 6 (July 2009).
125 Eric Chabrow, *New NIST Guidance Tackles Public Cloud Security*, BANKINFOSECURITY, Feb. 2, 2011, http://www.bankinfosecurity.eu/articles.php?art_id=3321.

uses cloud-based computer modelling to simulate responses to wild fires. However, a secure legal framework for cross-border cloud services is still lacking.[126] Another obstacle is that the hacker community has announced that cloud computing providers are a major target.[127]

The EU Commission is considering measures to help standardize terms and conditions for cloud computing services. This may include "model Service Level Agreements" or "Model End User Agreements," with standard contractual provisions to help deal with cross-border disclosure and privacy issues.[128]

On May 10, 2011, the German Federal Office for Information Security (Bundesamt fur Sicherheit in der Infromationstechnik (BSI) published its final framework on cloud computing security issues.[129]

On November 2, 2010, the CIO Council published its "Proposed Security Assessment & Authorization for U.S. Government Cloud Computing" report, Draft version 0.96, which is the product of an inter-agency team comprised of NIST, GSA, the CIO Council, and the Information Security and Identity Management Committee (ISIMC).[130]

Amazon's Cloud Crash

Amazon controls about 60% of the cloud computing market, which is expected to balloon to $148.8B in revenue by 2014, worldwide. A cloud computing crash of the type Amazon recently experienced sent ripples through the industry.[131] In effect, Amazon became a victim of its own success. It could not expand its Elastic Block Storage (EBS) architecture fast enough to meet demand, resulting in a catastrophic cascading failure, and permanent loss of 0.7% of customer data.[132]

In April 2011, a major flaw in cloud computing was exposed when Sony's global PlayStation network was breached. This resulted in the exposure of unencrypted personal information of 70 million users, including names, addresses and credit card details.[133] Amazon and Sony are not alone. In December 2010, the Microsoft Business Productivity Online Suite (BPOS) was breached in North America, Europe, and Asia.[134]

Apple's iCloud

Unlike Google's web-based concept of cloud computing, Apple's concept of cloud-based computing is application-centric. This is a less "mobile" model, but one that will

126 Honor Mahony, *EU Gets to Grips with Cloud Computing*, EU OBSERVER, Apr. 5, 2011, http://euobserver.com/893/32048.
127 *Hackers Say They are Targeting Cloud Computing*, OUT-LAW.COM, Nov. 2, 2010, http://www.out-law.com/page-11332.
128 *EU Commission May Publish Standardised Cloud Computing Terms*, OUT-LAW NEWS, May 17, 2011, http://www.i-policy.org/2011/05/eu-commission-may-publish-standardised-cloud-computing-terms.html.
129 Privacy & Information Security Blog, *German Federal Office for Information Security Issues Final Framework Paper on Information Security for Cloud Computing*, May 16, 2011, http://www.huntonprivacyblog.com/2011/05/articles/european-union-1/german-federal-office-for-information-security-issues-final-framework-paper-on-information-security-for-cloud-computing/.
130 CIO Council, Draft Proposal, *Proposed Security Assessment & Authorization for U.S. Government Cloud Computing*, Nov. 2, 2010, https://info.apps.gov/sites/default/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf.
131 Arik Hesseldahl, *Amazon's Cloud Crash is Over, But the Talking About It Isn't*, ALLTHINGSD, Apr. 25, 2011, http://allthingsd.com/20110425/amazons-cloud-crash-is-over-but-the-talking-about-it-isnt/.
132 Kevin Fogarty, *In English this Time: How Amazon let its Cloud Crash and Why it Should have Known Better*, ITWORLD, May 2, 2011, http://www.itworld.com/cloud-computing/161203/english-time-how-amazon-let-its-cloud-crash-and-why-it-should-have-known-bett.
133 Michael Atkin, *Government Urged to Embrace Cloud Computing*, ABC.NET, May 26, 2011, http://www.abc.net.au/pm/content/2011/s3228101.htm?site=goldfields.
134 Andreas Udo de Haes, *Microsoft BPOS Cloud Service Hit with Data Breach*, COMPUTERWORLD, Dec. 22, 2010, http://www.computerworld.com/s/article/9202078/Microsoft_BPOS_cloud_service_hit_with_data_breach.

provide more seamless access to documents, with a greater possibility of building in "privacy by design" functionality.[135]

Data Privacy and Digital Estate Planning

There is a new cottage industry called digital estate planning. This "digital probate service" executes your last wishes regarding your online data. One such company, LifeEnsured, will send final email messages, allow users to send a final Facebook status message, disable and delete social networking and email accounts, and convert online images to new ownership.[136]

Data Security and Privacy

High profile and major privacy breaches are increasing in severity and cost, particularly with the increase in use of laptops, Smartphones, and other mobile devices for critical business communication.[137] In a recent high profile case, police in Spain arrested members of a group known as "Anonymous" for hacking Sony Online websites and exposing personal data of over 70 million users[138] including customer names, addresses, email addresses, birth dates, phone numbers, user names, passwords, and at least 10,700 debit card numbers for users in Austria, Germany, Netherlands, and Spain,[139] and for breaching various governmental websites.[140]

In June 2011, another group known as "LuzSec" claimed responsibility for breaking into SonyPictures.com and accessing personal data belonging to more than one million customers, including passwords, emails addresses, home addresses, and dates of birth—none of which was encrypted. The same group claimed responsibility for hacking PBS.org in protest of its coverage of WikiLeaks, and for the attack on Fox.com divulging personal information of X-Factor contestants.[141]

Recently, BP lost a laptop containing the unencrypted personal data of 13,000 Gulf Oil disaster victims—including names, phone numbers, addresses, dates of birth, and social security numbers—a public relations and privacy disaster.[142] In May 2011, computer hackers breached Citigroup bank network security and accessed personal data of over 200,000 North American bank card holders.[143] And EMC's RSA security division was recently breached resulting in the compromises of millions of electronic keys.[144] X Factor Contestants were recently warned after personal information for 250,000 contestants was

135 Ryan Faas, *How the Apple iCloud Compares to Google's Cloud*, COMPUTERWORLD, June 8, 2011, http://financialbin.com/2011/06/08/how-the-apple-icloud-compares-to-googles-cloud-computerworld/.
136 Drake Martinet, *If you Die Tomorrow, Who Will Bury Your Data Six Feet Under?,* ALLTHINGSD, Apr. 8, 2011, http://allthingsd.com/20110408/if-you-die-tomorrow-who-will-bury-your-data-six-feet-under/.
137 Tonya Mohn, *Threats to Traveling Data*, THE NEW YORK TIMES, Mar. 14, 2011, http://www.nytimes.com/2011/03/15/business/15security.html.
138 *Absolute Sownage—A Concise History of Recent Sony Hacks*, ATTRITION.ORG, June 4, 2011, http://attrition.org/security/rants/sony_aka_sownage.html.
139 Nick Bilton, *Sony Finds More Cases of Hacking of Its Servers*, THE NEW YORK TIMES, May 2, 2011, http://bits.blogs.nytimes.com/2011/05/02/other-divisions-of-sony-attacked-last-week/.
140 Cassell Bryan-Low, *Spain Arrests Three in Sony Site Attack*, THE WALL STREET JOURNAL, June 11, 2011, http://online.wsj.com/article/SB10001424052702304259304576377380781996012.html.
141 Rina Richmond, *Hacker Group Claims Responsibility for New Sony Break-In*, THE NEW YORK TIMES, June 2, 2011, http://bits.blogs.nytimes.com/2011/06/02/hacker-group-claims-responsibility-for-new-sony-break-in/.
142 Sophie Curtis, *BP Spills Personal Data of 13,000 Oil Leak Victims*, Mar. 30, 2011, http://www.eweekeurope.co.uk/news/bp-spills-personal-data-of-13000-oil-leak-victims-25266.
143 *Thousands of Citi Customers at Risk after Hacker Attack*, REUTERS, June 9, 2011, http://www.msnbc.msn.com/id/43335996/ns/business-personal_finance/t/thousands-citi-customers-risk-after-hacker-attack/.
144 *Id.*

compromised by an attack on the Fox Broadcasting database.[145] A recent Bank of America breach resulted in the theft of money from over 300 North American customers, and costing the bank $10M.[146] In April 2011, Hyundai Capital in South Korea leaked personal information on 420,000 customers when its network database security was breached.[147] And in November 2010, hackers broke into the OECD computer system, one day before a scheduled EU cyber-security exercise.

Risks to web privacy in wireless environments are highlighted by a new plug-in known as "Firesheep" designed for the Firefox web browser. This applet makes it easy to intercept browser cookies used by Facebook, Twitter and others to identify their users, thereby allowing Firesheep users to log in and impersonate others. The phenomenon is known as "sidejacking," and the only effective remedy is for the websites to fully encrypt all their communications with customers—not just a portion of them.[148] The problem with the solution is that it significantly degrades Internet performance, which is a difficult *quid pro quo* to accept.

In March 2011, Twitter settled with the FTC over privacy breaches dating back to 2009, in which Twitter used default administrative passwords for its only security measures, which were easily cracked.[149]

"The Future of Privacy" and "Privacy by Design"

On December 1, 2009, the Article 29 Working Party, in a joint contribution with the Working Party on Police and Justice, issued "The Future of Privacy" (WP 168), which articulates a future vision for EU personal data protection.[150]

The vision of WP 168 is to ensure that the foundational principles of data protection survive the challenges of new technology and globalization. The relevance of these principles for emerging technology can be enhanced, according to WP 168, by:

(1) Clarifying the principles and rule of data protection (e.g., transparency and consent);

(2) Introducing the concept of "privacy by design" into the system development lifecycle of new technologies, so that privacy is "baked into" new applications;

(3) Streamlining the operation of the Data Protective Directive by removing bureaucratic burdens; and

(4) Developing one comprehensive legal framework that applies not only to civil matters, but also to police and judicial cooperation in criminal matters.

145 John Dunn, *X Factor Contestants Warned After 250,000 Data Breach*, TECHWORLD, May 4, 2011, http://www.techworld.com.au/article/385285/x_factor_contestants_warned_after_250_000_data_breach/.
146 *Insider Data Breach Costs Bank of America over $10 Million, Says Secret Service*, INFOSECURITY, May 26, 2011, http://www.infosecurity-us.com/view/18237/insider-data-breach-costs-bank-of-america-over-10-million-says-secret-service/.
147 Jonathan Hopfner, *South Korea Watchdog Probes Hyundai Capital Data Breach*, REUTERS, Apr. 10, 2011, http://www.reuters.com/article/2011/04/11/us-korea-regulator-hyundai-idUSTRE73A0DJ20110411.
148 Nick Wingfield, *Firesheep Highlights Web Privacy Problem*, THE WALL STREET JOURNAL, Oct. 25, 2010, http://blogs.wsj.com/digits/2010/10/25/firesheep-highlights-web-privacy-problem/.
149 Jacqui Cheng, *Twitter Settles with FTC Over Privacy Breaches*, PCMAGAZINE, Mar. 11, 2011, http://arstechnica.com/web/news/2011/03/twitter-settles-with-ftc-over-security-breaches.ars.
150 *The Future of Privacy*, Article 29 Data Protection Working Party 02356/09/EN, WP 169, (Adopted Dec. 1, 2009).

WP 168 calls for the adoption of a "privacy by design" principle in the new framework. This would reinforce the inclusion of default settings in new systems that would help data subjects be aware of data protection risks and to better protect their data.

In particular, with respect to a new "privacy by design" (PbD) principle, WP 168 calls for (1) biometric identifiers to be stored under the control of data subjects, such as through smart cards, rather than external databases; (2) video surveillance in public transportation systems to minimize the privacy risk for data subjects; (3) segregation of identity-related information from actual data in health information systems; and (4) providing data subjects with enabling technology access to revoke their consent and to trigger a data deletion process in all data containers, even backup and mirrored systems, to the extent practicable.

To further integration of the PbD principle, WP 168 suggests focusing on seven key objectives:

(1) Data minimization, with the aim of collecting, processing, and using no personal data, or as little personal data as possible;

(2) Control, to provide data subjects with effective controls over knowledge and access to their personal data;

(3) Transparency, by ensuring data subjects understand how their personal data are stored, processed, and used by technology systems, and giving data subjects effective access to such systems;

(4) User-friendliness, by providing data subjects with easy-to-navigate interfaces to their personal data;

(5) Confidentiality, by strengthening access and authentication security measures to ensure that only authorized persons have access to such data;

(6) Quality control, by ensuring data integrity and immutability; and

(7) Limitations on use, by guaranteeing that personal data will not proliferate beyond its intended use, by virtue of virtual management, data warehouses, cloud computing, and similar multi-user environments.

WP 168 recognizes that more than ever, data subjects are voluntarily sharing personal data in social networking, cloud computing, and other virtual environments. To help protect data subjects from themselves, WP 168 calls for embedding data protection and data privacy principles in the internal policies, practices, procedures and processes of these providers, as well as data controller organizations. This requires educating and sensitizing top management of the risks but also the benefits of data privacy. The UK has recently embarked on an initiative to identify the "privacy dividend" available to organizations who comply with data privacy and protection obligations.

This embedding process requires, according to WP 168, the following proactive measures:

(1) Adopting internal policies and processes by data controllers;

(2) Implementing compliance monitoring and enforcement mechanisms for the internal policies and processes;

(3) Conducting audit and compliance checks to assess strengths and weaknesses, and to remedy any gaps;

(4) Generating assessments of the impact of the policies and processes on personal data;

(5) Assigning accountability for data protection and privacy compliance;

(6) Certifying compliance by top executives; and

(7) Transparency of these measures to data subjects, by such measures as publishing them on the organization's intranet, conduct policies, guidebooks, and annual reports.

CONCLUSION

The emerging technologies previewed above have significantly amplified the "Catch-22" between cross-border disclosures and data privacy in the context of litigation and regulatory proceedings. Fortunately, we have a firm foundation upon which to build sustained dialogue and to seek common ground in responding to the challenge of rapidly changing technologies.

The Sedona Conference® *Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy & e-Discovery* (Public Comment Version 2008) set the stage for dialogue between the U.S. and EU on navigating the dangerous rapids of cross-border disclosure and data privacy.

The Article 29 Data Protection Working Party accepted this invitation to engage in a constructive dialogue in its Working Document WP 158.[151] The dialogue continued with the Deliberation of the French Data Protection Authority, *Commission Nationale de l'Informatique et des Libertés* (CNIL)[152] on July 23, 2009. This was followed by the formal response of The Sedona Conference® Working Group 6 on International Electronic Information Management, Discovery and Disclosure to WP 158 on October 30, 2009.[153]

151 *Working Document 1/2009 on pre-trial discovery for cross border civil litigation*, Article 29 Data Protection Working Party 00339/09/EN, WP 158, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf (Adopted Feb. 11, 2009).

152 CNIL, *Deliberation No. 2009-474 of 23 July 2009 concerning recommendations for the transfer of personal data in the context of American court proceedings known as "Discovery,"* July 23, 2009, http://www.cnil.fr/fileadmin/documents/en/D-Discovery_EN.pdf.

153 Comment of The Sedona Conference® Working Group 6 to Article 29 Data Protection Working Party's Document 1/2009 (WP 158), Oct. 30, 2009, http://www.chrisdalelawyersupport.co.uk/documents/SedonaWG6_Response_to_Article29WP158.pdf.

In early November 2009, more than 100 corporate representatives, civil organizations, and privacy experts signed the Madrid Privacy Declaration (a/k/a Madrid Resolution) that addresses a number of issues relating to cross-border transfers of personal data. And in February 2010, WG6 was invited to present its views to the Article 29 Working Party Plenary Session in Brussels, Belgium.

On December 1, 2009, the Article 29 Working Party articulated its vision of "The Future of Privacy," in WP 168, based on principles of transparency, accountability and privacy by design. These same principles were echoed one year later in December 2010 in the FTC's Proposed Framework for Businesses and Consumers for Protecting Consumer Privacy in an Era of Rapid Change.

The preliminary draft of The Sedona Conference® *International Principles on Disclosure and Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation and Discovery of Protected Data in U.S. Litigation* is a principle part of the agenda of the 3rd Annual Sedona Conference® International Programme on Cross-Border eDiscovery & Data Privacy in Lisbon, Portugal on June 22-23, 2011.

Building on this solid foundation, and with sustained communication and commitment, the future is bright for improved EU/U.S. cooperation on the difficult issues of cross-border disclosure and data privacy. This is future vision in which privacy by design plays a large role in reducing the "Catch 22" impact of emerging technologies.