# Outline of Recommended Changes for The Sedona Conference Data Privacy Primer, Second Edition (April 2024)

# Outline of Recommended Changes for The Sedona Conference Data Privacy Primer, Second Edition (April 2024)

Drafting Team Members:

Corey Dennis (Drafting Team Leader)
Esther Clovis
Anne Davis
Emily Fedeles
Josh Hansen
Jerami Kemnitz
J. Austin Moore
Matthew Prewitt
Tatiana Rice
Douglas Swetnam
Wendy Wagner
Colman McCarthy (Steering Committee Liaison)

## TABLE OF CONTENTS

- *Update for:*
  - *Deception Authority*
  - *Unfairness Authority, including developments since LabMD/Wyndham and increased use of unfairness authority.*
  - *Targeted Areas of Interest*
    - *Health Data - FTC has broad view of substantive duties and reporting obligations.*
      - *Health Breach Notification Rule*
        - *Rule Basics*
        - *Non-HIPAA health data*
        - *Notify if unauthorized access/disclosure (breach or share without authorization)*
      - *Renewed Interest:*
        - *FTC Action: Policy Statement + Rulemaking*
        - *Settlements - Expansive reading of health information*
      - *Good RX Settlement: Company shared data without authorization (cookies, pixels, etc.) and then failed to give notice*
        - *Remedy: No sharing for ads + consent for other uses + required 3rd party deletion*
    - *FTC Act. Focus on the digital advertising space for healthcare companies*
      - *BetterHealth & GoodRX*
        - *Unfairness - must prevent unauthorized access/disclosures*
        - *Deception - be transparent about practices*
      - *Location Data (data brokers) - brokers sharing sensitive location data without consent = bad*
        - *Consent. Need informed consent*
          - *X-Mode. Users not informed about recipients (and X-Mode didn't vet third-party apps to ensure they received consent to share with X-Mode)*
          - *InMarket. Misled consumers by stating only some purposes (and same issue as X-Mode for third-party apps)*
        - *Direct Harm. Invades privacy + expose to discrimination, harm, etc. based on associations with locations*

        - *Kochava + X-Mode*
    - *Secondary Harms. Need safeguards against downstream uses*
        - *Kochava - No policies/procedures to protect against harmful uses*
        - *X-Mode - No safeguards against downstream uses*
    - *Remedies.*
        - *Destruction*
        - *Notice of settlement*
        - *Limit processing without informed consent*
        - *Validate third-party consent process*
        - *Restrict third parties from associating data with sensitive locations*

2. Children's Online Privacy Protection Act (COPPA; 15 U.S.C. §§ 6501–6505) ..... 334

- *Update for COPPA Enforcement*

- *Enforcement/Compliance Mechanisms - will cover model disgorgement and data deletion as well as settlement orders (e.g., RiteAid, Facebook, Twitter)*

3. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act; 15 U.S.C. §§ 7701–13) ..... 338
4. Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"; 15 U.S.C. §§ 6101–6108) [*Amend IV(A)(4) (Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"; 15 U.S.C. §§ 6101–6108))*] ..... 343

- *Update for:*
    - *FCC Cross Bureau Task Force*
        - *https://www.fcc.gov/privacy-and-data-protection-task-force*
        - *State AG Anti-Robocall Task Force*
    - *State AG 50 State AG Anti-Robocall Task Force Formation August 2022*
        - *https://events.in.gov/event/attorney_general_todd_rokita_announces_the_formation_of_a_nationwide_bipartisan_anti-robocall_litigation_task_force*
        - *https://stateline.org/2022/08/15/state-attorneys-general-unite-against-robocalls/*
    - *Task Force National Litigation*
        - *Avid Telecom*
        - *https://www.jdsupra.com/legalnews/anti-robocall-litigation-task-force-4144001/*
    - *Task Force Issuing Warning letters*

        - *https://ncdoj.gov/protecting-consumers/telephones-telemarketing/fighting-robocalls/warning-notices/*



- *FCC Cross Bureau Task Force*
    - *https://www.fcc.gov/privacy-and-data-protection-task-force*
    - *State AG Anti-Robocall Task Force*
- *State AG 50 State AG Anti-Robocall Task Force Formation August 2022*
    - *https://events.in.gov/event/attorney_general_todd_rokita_announces_the_formation_of_a_nationwide_bipartisan_anti-robocall_litigation_task_force*
    - *https://stateline.org/2022/08/15/state-attorneys-general-unite-against-robocalls/*
- *Task Force National Litigation*
    - *Avid Telecom*
    - *https://www.jdsupra.com/legalnews/anti-robocall-litigation-task-force-4144001/*
- *Task Force Issuing Warning letters*
    - *https://ncdoj.gov/protecting-consumers/telephones-telemarketing/fighting-robocalls/warning-notices/*



- *Updates as follows to Create General Privacy Section/State Comprehensive Laws*

    - *Overview*
    - *General Scope and Applicability*
    - *Consumer Rights*
    - *Business Obligations*
    - *Rulemaking and Enforcement*

    - *Application. The laws reach activity in the state provided certain thresholds are met and an exception does not apply.*
        - *Thresholds. States generally focus on the impact in the state (consumers)*
            - *Key Considerations. What is a consumer and what is a sale?*
            - *Consumers. The number of consumers is not clearly tied to state size (e.g., California and Colorado have same threshold; Tennessee requires more than California).*

- *Sales. Does sale include targeted ads?*
- *Majority Rule. The general approach is to focus on number of consumers or volume of sales (revenue & consumers).*
  - *Revenue. Most states require >20& to >50% of revenue derived from sales, the exceptions are CO/NJ—which do not require specific revenue percentage derived from sales.*
- *Minority Approaches*
  - *Texas. The law applies to anyone who isn't a small business as defined by SBA.*
  - *California. The law applies if you meet revenue, consumer, or sale thresholds.*
  - *Tennessee/Utah. The law applies if you meet revenue requirements and either consumers or sales.*
- *Exceptions/Exemptions*
  - *Nonprofits. Most states exclude nonprofits; the exceptions are Colorado, Delaware, New Jersey, and Oregon.*
  - *Exemptions. Most states include exemptions covering state/local entities, FCRA, GLBA, HIPAA, etc.*
    - *Data vs. Entity. States vary on whether they apply data or entity exemption. Connecticut AG urging reconsideration of entity exemption.*
- *Carve Outs. Even if law applies to company, it may not apply in certain contexts.*
  - *Common Exclusion. Does not "restrict" ability to: comply with law, comply with legal process or investigations, cooperate with law enforcement in good faith, exercise/defend legal claims, perform a contract, address fraud or malicious activity.*

- *Effective Dates. States are generally giving companies one to two years of lead time for to prepare, except they are giving more time to comply with GPC requirements.*
  - *General Law*
    - *Currently in Effect: California, Colorado, Connecticut, Utah, Virginia*
    - *This Year: Oregon (7/1/24); Texas (7/1/24); Montana (10/1/24);*
    - *Next Year: Delaware (1/1/25); Iowa (1/1/25); New Hampshire (1/1/25); New Jersey (1/16/25); Tennessee (7/1/25)*
    - *2026: Indiana (1/1/26); Kentucky (1/1/26)*
  - *GPC. Some states have delayed roll outs for complying with GPC. E.g., CT (1/1/25 for GPC but 7/1/23)*

- *Consumer Rights*
  - *Affirmative Consent*
    - *Affirmative Consent*

- *Affirmative action + requirements that it is freely given, specific, informed, and unambiguous*
- *Does not include*
    - *accepting general statement*
    - *dark patterns*

- *Sensitive data collection*
- *Secondary use*
- *Children/adolescents*
- *Non-discrimination*
    - *Non-discrimination for exercising right*
    - *Can't process data in a discriminatory manner*
- *Opt-in v. opt-out consent*
- *Revoke consent*

- *Rights of knowledge, access, correction, deletion, and portability*
    - *+ Obtain list of third parties to which personal data was disclosed (DE, OR)*
- *Opt-out rights*
    - *Targeted advertising*
    - *Sale of personal data*
    - *Profiling*
    - *Universal opt-out mechanisms*
- *Additional children's rights*
    - *Opt-in for targeted advertising or sale of PI of children ages 13-15 (CA, CT, DE, MT, OR)*
- *Exercising Rights*
    - *Submission / authentication*
        - *Children / guardian*
    - *Appeals*

- *Business Obligations*
    - *Controller*
        - *Limit Collection of Personal Data*
            - *Adequate, Relevant, Reasonable*
            - *Are there multiple purposes? Needs to be consistent with business model*
            - *Needs to cover SDKs, APIs and other code tools*
        - *Limit Processing of Personal Data*
            - *Reasonably necessary*
            - *Compatible to stated purposes*
            - *Are there multiple purposes? Needs to be consistent with business model*
            - *Needs to cover SDKs, APIs and other code tools*
        - *Data Security:*

- *Establish, implement, and maintain reasonable:*
  - *Administrative data security practices,*
  - *Technical data security practices, and*
  - *physical data security practices*
- *All Data Security practices above must protect:*
  - *Confidentiality of personal data,*
  - *Integrity of personal data, and*
  - *accessibility of personal data.*
- *Incident Response:*
  - *If there's a data breach, businesses must respond promptly.*
  - *They must notify affected consumers and take steps to mitigate harm.*
  - *Reporting breaches to authorities is also required.*
- *Identity Theft*
- *Fraud*
- *Harassment,*
- *Malicious or Deceptive Activities*
- *Illegal Activity*
- *Investigate, Report or Prosecute Those Responsible*

▪ *Duty of Transparency:*

- *Businesses must provide consumers with reasonably accessible, clear and meaningful notices that include:*
  - *The categories of personal data processed by the controller*
  - *The purpose(s) for processing personal data; Is there a dual purpose?*
  - *How consumers may exercise their rights under the Comprehensive Consumer Data Protection Act*
  - *Third party sharing, if any, specifying:*
    - *The categories of personal data shared*
    - *The categories of third parties*
  - *Financial Incentive (CA)*
  - *Opt-out disclosure at time of collection*

▪ *Duty to Respect Consumer Rights:*

- *Right of inquiry to confirm whether a controller is processing the consumer's personal data*
- *Right to correct inaccuracies.*
- *Right to delete personal data provided by or about the consumer*
- *Right to obtain data:*
  - *"Specific pieces of Personal Data include final Profiling decisions, inferences, derivative data, marketing profiles, and*

*other Personal Data created by the Controller which is linked or reasonably linkable to an identified or identifiable individual."*
    - *Right of portability*
    - *Representative summary*
- *Right to opt out of processing for purposes of:*
    - *Targeted advertising*
    - *Sale of personal data;*
    - *Profiling for decisions that produce legal or similarly significant effects*
- *Timely response*
    - *30, 45, 60 days subject to sunset provisions*
    - *Free with limits, i.e. one time annually*
- *Universal Opt-Out Mechanisms*
- *Provide secure and reliable means for submitting requests*

▪ *Duty to Provide Appeal Process*
- *If controller declines consumer request, provide consumer justification for denial.*
- *If controller declines consumer request, provide consumer with instructions how to appeal the decision.*

▪ *Non-discrimination against Consumer*

▪ *Duty of Fair Dealing with Controller*
- *Must not disadvantage another Controller*

▪ *Data Protection Impact Assessments:*
- *Processing of personal data for purposes of targeted advertising*
- *The sale of personal data;*
- *Processing of personal data for profiling, if such profiling presents a reasonably foreseeable risk of:*
    - *Unfair or deceptive treatment of, or unlawful disparate impact on consumers*
    - *Financial, physical, or reputational injury to consumers*
    - *A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if such intrusion would be offensive to a reasonable person;*
    - *Other substantial injury to consumers*
    - *Any processing activities involving personal data presenting heightened risk of harm to consumers*
    - *Weigh benefits versus risks*
    - *Respond to Attorney General requests.*
- *This helps them identify vulnerabilities and take preventive measures.*

▪ *Record Keeping*

        - *Contractual Obligations and Monitoring*
        - *Employee Training:*
            - *Employees handling personal data should be trained on businesses privacy practices.*
    - *Processor*
        - *Appropriate contract*
        - *Adhere to Controller Instructions*
        - *Ensure Confidentiality of each individual processing personal data*
        - *Assist Controller in responding to Consumer requests*
        - *Assist Controller to demonstrate compliance*
        - *Ensure any sub-contractor adheres to duty of confidentiality imposed by Controller*
- *Rulemaking and Enforcement*
    - *Rulemaking. Most states (11/15) do not have rulemaking. Of the four with rulemaking, three states have broad rulemaking, and one has very limited authority.*
        - *Authority. The rulemaking is often directed by the AG (or equivalent), except that California has a dedicated enforcement agency and New Hampshire delegates the power to the Secretary of State.*
        - *Broad Grant.*
            - *Colorado and California. Colorado issued all its rules, while California is doing piecemeal: general topics now with ADMT, risk assessments, and cybersecurity audits in the work. Colorado added unique twist by specifying the opt-out mechanisms with which companies must comply.*
            - *New Jersey. TBD*
        - *Narrow Grant*
            - *New Hampshire (limited). Rulemaking will be limited to methods for exercising rights and "standards" for privacy notices.*
    - *Enforcement. The majority assign enforcement to the Attorney General who can pursue civil penalties if a company does not fix their noncompliance within the cure period.*
        - *Actor. The general rule is that the Attorney General enforces the law. The only exceptions are Colorado (which allows district attorneys) and California (which has AG + CPPA and private right of action for limited data breach claims).*
        - *Cure Period. Every state adopted a cure period (30-90 days), and half the states sunset their cure period after a set period of time.*
        - *Safe Harbor. Tennessee says no liability if comply with NIST or other documented policies, standards, procedures to safeguard privacy and update*

- *Update to add new section in Consumer Protection Segment on Tracking Technologies - Litigation / Enforcement*
  - *Cookies*
    - *What Are Cookies, first party, third party, third-party cookie proxies, cookie-blocking technology (Apple, Google)*
    - *Litigation/Regulation*
    - *U.S., States, EU, others?*
    - *California AG enforcement under CCPA (Sephora)*
    - *Internet Tracking, Google Cookie*
  - *Pixels*
    - *What Are Pixels: tracking software embedded on websites and mobile apps to track advertising campaigns, provided for free by entities like Google and Meta, but unlike cookies, more difficult to block, as they do not rely on cookies to function*
    - *Prevalence of pixel products evolving (Google Tag remains widely used, Meta pixel declining according to BuiltWith)*
    - *Terms of Use*
  - *Litigation/Regulation*
    - *HHS OCR update to Healthcare Providers (Dec 22 bulletin); Joint letter (July 2023); FTC September 2023 bulletin, – see HIPAA section?*
    - *FTC and Private Litigants*
    - *GoodRX and BetterHelp, Google and Meta FTC actions (addressed elsewhere so x-ref?)*
    - *Target entities: healthcare providers, financial services providers*
    - *Focus on consent, 3P consent*
    - *Causes of action*
      - *Wiretap (state and federal claims)*
      - *Anti-Hacking (State Claims)*
      - *California law – CIPA, UCL, CMIA, CDAFA*
  - *Other Technologies*
    - *APIs*
    - *Incognito/Private Browsing*

- *Advertising Auctions*
- *Chatbots*
- *Session Replay Software*



- *Update to address comprehensive privacy laws in the states, including focus on sensitive data*



- *Move to Genetic Privacy Section?*



- *Update to add:*
  - *Washington "My Health, My Data" Act*
    - *Broad scope*
    - *Privacy notice/consent requirements*
    - *Sale requirements*
    - *Individual rights (right of access, etc.)*
    - *Geofencing prohibition*
    - *Private right of action*
  - *Nevada's Consumer Health Data Privacy Law"*
    - *Comparison to Washington; no private right of action*

- *Connecticut Data Privacy Act amendment (SB3)*
  - *Broad scope*
  - *Privacy notice/consent requirements*
  - *Restrictions on geofencing*
- *Resources*
  - *How the New Nevada Consumer Health Law Differs from the Washington State My Health, My Data Act https://www.connectontech.com/how-the-new-nevada-consumer-health-law-differs from-the-washington-state-my-health-my-data-act/*
  - *Connecticut and Nevada Legislatures Pass Health Data Laws https://www.huntonprivacyblog.com/2023/06/27/connecticut-and-nevada-legislatures-pass-health-data-laws/*
  - *50-State Survey of Health Care Information Privacy Laws https://www.seyfarth.com/dir_docs/publications/50-state-survey-of-health-care-information-privacy-laws-2023-2024-edition.pdf*
  - *CONNECTICUT SHOWS YOU CAN HAVE IT ALL https://fpf.org/blog/connecticut-shows-you-can-have-it-all/*

- *Update to Add Separate Section on Genetic Privacy*
  - *Federal Laws Addressing Genetic Information*
    - *Genetic Information Nondiscrimination Act of 2008 (GINA)*
      - *GINA was signed into law on May 21, 2008. The goal of the legislation was to establish a national and uniform basic standard to protect the public from genetic discrimination in health insurance and employment.*
      - *The federal law sets a minimum standard of protection that must be met in all states. It does not weaken the protections provided by any state law.*
      - *GINA defines "genetic information" the same as in the Health Insurance Portability and Accountability Act (HIPAA), to include an "individual's genetic tests," "the genetic tests of family members," and "the manifestation of a disease or disorder in family members."*
      - *Title I of GINA prohibits discrimination based on genetic information in health coverage, including the prohibition of:*
      - *looking at predictive genetic information or genetic services before an individual enrolls;*
      - *"requesting or requiring" that an individual or family member take a genetic test;*
      - *restricting enrollment based on genetic information;*
      - *changing premiums based on genetic information.*
      - *Title II of GINA prohibits employers from discriminating against applicants and employees based on their genetic information or the*

*genetic information of their family members, including the prohibition of:*

- *discriminating against who they hire or how much they pay on the basis of genetic information;*
- *"requesting or requiring" that an individual or the individual's family members take a genetic test;*
- *disclosing an individual's genetic information in their possession except under specific and specially controlled circumstances.*
- *GINA allows for recovery of compensatory and punitive damages.*

- *State Laws Addressing Genetic Information Discrimination*
  - *Introduction: A number of states have enacted laws to extend GINA's protections to include life insurance, long-term care insurance, and/or disability insurance.*
    - *21 states explicitly restrict in some way the use of genetic information in life insurance*
    - *11 states—Arizona, California, Colorado, Delaware, Florida, Maine, Minnesota, Nevada, New Jersey, New York, and Oregon—require some level of informed consent or authorization related to collection or analysis of genetic information and life insurance.*
    - *18 in disability insurance*
    - *10 states—Arizona, California, Colorado, Delaware, Florida, Indiana, Maine, New Jersey, New York, and Oregon—require some level of informed consent or authorization for disability insurance.*
    - *14 in long-term care insurance.*
    - *7 states—Arizona, Delaware, Florida, Indiana, Maine, New York, and Oregon— require some level of informed consent or authorization for collection and analysis in long-term care insurance.*
    - *Several states have laws that regulate all three of the above insurance types including Arizona, California, Maine, Massachusetts, New Mexico, New York, Oregon, and Vermont.*
    - *For example, California's genetic anti-discrimination law, known as CalGINA, not only prohibits genetic discrimination in employment (GINA's scope), but also in housing, provision of emergency services, education, mortgage lending and elections.*
    - *In July 2020, Florida became the first state to completely bar insurers from canceling, limiting, denying or differing premium rates based on genetic information for life insurance, long-term care and disability insurance. The law creates an exception for medical diagnoses made on the basis of genetic information*

- *In the context of genetic testing, laws generally state that genetic information can be used as long as the information is linked to increased risk.*

▪ *State Laws Addressing Genetic Information w/ Private Right of Action*

- *Illinois Genetic Information Privacy Act of 1998 (GIPA) (410 ILCS 513/5).*
  - *GIPA (410 Illinois Compiled Statute 513), which was passed in 1998 and later amended in 2008 to align it with GINA*
  - *It provides that genetic testing information is "confidential and privileged" and prohibits requiring as a condition of employment that applicants or employees provide genetic information.*
  - *GIPA defines "genetic information" the same as in the Health Insurance Portability and Accountability Act (HIPAA) and GINA*
  - *GIPA allows the collection of actual damages or per violation damages ($2,500 per negligent violations and $15,000 for intentional or reckless violations), whichever is greater.*
- *Oregon Genetic Privacy Act of 1995 (Or. Rev. Stat. § 192.533)*
  - *Oregon law prohibits an employer from obtaining or using genetic information to discriminate against an employee or prospective employee. The law also prohibits insurance companies from using genetic information to price or decline individual policies (ORS 746.135).*
  - *Oregon law also requires that individuals be given the option to request their biological sample or health information not be used for anonymous or coded genetic research. Otherwise, these samples are available for genetic research under existing law.*
  - *Additionally, Oregon law required the Oregon Health Authority (OHA) Public Health Division to adopt rules establishing minimum research standards for the collecting and testing of genetic information (ORS 192.547).*
  - *In Oregon, it is a Class A misdemeanor to unlawfully obtain, retain, or disclose genetic information (ORS 192.543).*
  - *Oregon law also provides a civil cause of action against anyone who unlawfully obtains or discloses genetic information, with the right to obtain the greater of actual damages or set statutory damages that range from $100 (for negligent violations) to $250,000 (for knowing violations with intent to sell or use a person's genetic information for commercial purposes) (ORS 192.541).*

- *Alaska's Genetic Privacy Act (Alaska Stat. §§ 18.13.010–100)*
  - *Alaska's Genetic Privacy Act, Alaska Stat. §§ 18.13.010–100, treats genetic information, including DNA samples, as the private property of the individual. As such, the statute provides that DNA samples cannot be collected, analyzed, or disclosed without an individual's informed consent. The statute was enacted to "curtain exploitation of [citizens'] valuable genetic information" and to afford Alaskans "the right to keep their genetic information private."*
  - *Specific Provisions*
  - *The Alaska law makes it illegal for anyone to "collect a DNA sample from a person, perform a DNA analysis on a sample, retain a DNA sample or the results of a DNA analysis, or disclose the results of a DNA analysis" without first obtaining that person's informed consent. The Alaska law specifies that both the DNA sample and the results of any analysis of the sample are the exclusive property of the "person sampled or analyzed."*
  - *The Alaska law defines "DNA analysis" to mean "DNA or genetic typing and testing to determine the presence or absence of genetic characteristics in an individual," and further defines "genetic characteristics" to include "a gene, chromosome, or alteration of a gene or chromosome that may be tested to determine the risk of a disease, disorder, trait, propensity, or syndrome, or to identify an individual or a blood relative."*
  - *The Alaska law contains a number of exclusions that narrow its otherwise sweeping scope. The statute expressly defines "DNA analysis" to exclude "routine physical measurement, a test for drugs, alcohol, cholesterol, or [HIV], a chemical, blood or urine analysis, or any other diagnostic test that is widely accepted and in use in clinical practice." Thus, the law arguably has no application to routine tests a person could obtain at most doctors' offices. The statute also exempts five categories of activities, specifying that its prohibitions do not apply to genetic testing for purposes of:*
    - *criminal identifications pursuant to any jurisdiction's DNA registration system;*
    - *law enforcement, including the identification of both victims and perpetrators;*
    - *paternity testing;*

        - *screening of newborns as required by law; or*
        - *emergency medical treatment.*
    - *The Alaska law makes clear that a "general authorization for the release of medical records or medical information" does not count as the necessary informed consent to release the genetic information the law protects. The law also expressly permits a person, at any time, to revoke or amend their informed consent to analysis or disclosure of genetic information.*
    - *Enforcement*
        - *In Alaska, unlawful DNA collection, analysis, retention or disclosure is a class A misdemeanor punishable by up to one year in jail and a fine of up to $10,000. The statute specifies that a person is criminally liable only if he or she acts "knowingly," which need not include any intention to violate the law. Rather, under Alaska law, a person acts "knowingly" if he or she is aware that the circumstance making the conduct unlawful exists, or if he or she is aware of a substantial probability that the circumstance exists.*
        - *The Alaska law also creates a private right of action for anyone whose genetic information is collected, analyzed, retained, or disclosed in violation of the statute. The statute provides for statutory damages of $5,000, in addition to any actual damages suffered by the person whose genetic information was misused. If the violator profited from the violation, the statutory damages increase to $100,000.*
- *State Laws Regulating Direct-To-Consumer Genetic Testing Companies.*
    - *Arizona, California, Kentucky, Maryland, Montana, Nebraska, Tennessee, Texas, Utah, Virginia, and Wyoming have enacted privacy regulating direct-to-consumer genetic testing companies. Minnesota and Vermont have introduced similar bills during this legislative session.*
    - *These laws adopt baseline requirements–including requirements to publish privacy notices and create consumer rights of access and deletion. Notably, Montana is the only one that does not exempt de-identified or anonymized data, which has led to protest from DTC genetic testing companies. Below are two examples:*
    - *Nebraska's DTC Genetic Privacy Law*

- *On February 14, 2024, Nebraska enacted a genetic privacy law (LB 308) regulating direct-to-consumer ("DTC") genetic testing companies.*
- *LB 308 applies to companies that meet the definition of a DTC genetic testing company, which is defined as "an entity that (a) offers consumer genetic testing products or services directly to a consumer, or (b) collects, uses, or analyzes genetic data that resulted from a direct-to-consumer genetic testing product or service and was provided to the company by a consumer."*
- *Such companies will be required to comply with various obligations similar to those in other DTC genetic privacy laws, including (a) providing a written public privacy about the company's collection, use, and disclosure of genetic data; (b) obtaining consent for collection, use, and disclosure of genetic data, including for initial testing, transferring genetic data, and non-exempt research; (c) obtaining consent to retain the consumer's biological sample; and (d) providing certain data subject rights (e.g., access, deletion) to consumers, among other requirements.*
- *The law exempts certain types of data and activities from its purview. The definition of "genetic data" in LB 308 exempts de-identified data that meets a statutory standard. Protected health information ("PHI") collected by a covered entity or business associate subject to HIPAA is also exempt.*
- *The Attorney General may bring an action to enforce the provisions of the Genetic Information Privacy Act. A violation of the act is subject to $2,500 for each violation, in addition to actual damages incurred by the consumer, and costs and reasonable attorney's fees incurred by the Attorney General.*

- *Montana Genetic Information Privacy Act*
  - *Defines "genetic data" to include not just raw sequence data but also genotypic and phenotypic information and "self-reported health information." And it broadly defines "genetic testing" to include not just the lab work to extract DNA but also the "interpretation of a consumer's genetic data."*
  - *It sets comprehensive notice, use, and consent requirements for companies processing consumer genetic data.*
  - *It requires that companies provide consumers with clear information about their practices and privacy protections through a "high-level privacy policy overview."*

- *It requires consumers' express affirmative consent not just upon initial collection but also separate and additional express consent for secondary uses of the data, retention of the consumer's biological sample, and any data transfer or disclosure to third parties.*
- *It prohibits the disclosure of a consumer's genetic data to the consumer's employer and any entity offering health insurance, life insurance or long-term care insurance without the consumer's express consent.*
- *The law does not exempt de-identified data—or data that's not linked to a specific person*
- *Sole enforcement by Attorney General who may recover actual damages to the consumer; costs; reasonable attorney fees; and $2,500 for each violation.*

- *Consumer Data Privacy Laws*
  - *13 states have adopted comprehensive privacy laws, some of which define protected information to include biometric and genetic information.*
  - *The recently passed Delaware Personal Data Privacy Act (DPDPA) includes a defined term for "Genetic Data," which is not present in any other state privacy laws.*
  - *Under the DPDPA, "genetic data" is defined as "any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. For purposes of this paragraph, "genetic material" includes deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom."*
  - *7 states—Kansas, Maine, Massachusetts, New Jersey, New Mexico, Vermont, and Wisconsin—require actuarial justification for use of genetic information in life insurance.69*
  - *8 states—Idaho, Kansas, Maine, Massachusetts, New Jersey, New Mexico, Vermont, and Wisconsin—require it for use in disability insurance.70*
  - *6 states—Kansas, Maine, Maryland, Massachusetts, New Mexico and Vermont—require it for use in long-term care insurance.*
- *Treatment of Genetic Information Under EU General Data Protection Regulation*

- *The GDPR lists genetic data as "special categories of personal data" or sensitive data (Art. 9), which makes their processing for research purposes (Art. 9(2)(j)) subject to the adoption of adequate organizational and technical safeguards, such as pseudonymization (Art. 89(1)).*
- *Pseudonymization is defined in Art. 4(5) as the process through which data "can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."*
- *The GDPR explicitly defines data that have undergone pseudonymization as personal data, thus falling within the scope of the regulation.*



- *Maintain as this is background information, but update to reflect updates to the Safeguards Rule in 2021 and 2023 to require non-banking financial institutions regulated by the FTC to report data breaches and security events to FTC.*



- *Entities covered by the GLBA (as expanded by updates to Safeguards Rule, including non-banking financial institutions which as of the 2023 updates, have an obligation to report to FTC.*



- *Update for Safeguarding Rule to address covered information and broader coverage of incidents resulting in consistency with Health Breach Notification Rule.*



- *Update to new comprehensive state privacy laws, some of which include financial institution exemptions (e.g. Oregon), although consensus remains that financial institutions subject to other regulatory laws like the GLBA are exempt from the general scope of their data privacy laws.*



- *Update for CFPB actions, recent enforcement penalties, including FTC v. RCG Advances, examination procedures from CFPB.*

- *Maintain as background with updates for CFPB guidance and advisory opinions, updates to A Summary of Your Rights Under the Fair Credit Reporting Act, issued March 17, 2023.*



- *Enforcement update – keyword promotions enforcement actions against Instant Checkmate and Truthfinder – providers of consumer background reports.*



- *Update to note that 2015 legislation went nowhere re: CFPB.*



- *Proposed Updates to Paragraphs 3 and 4*
  - *3 states (add NY) have passed legislation requiring employers to give notice to employees prior to monitoring email communications or Internet access.*
  - *2021 Amendment to the NY Civil Rights Law requiring notice from employers at time of hiring re: electronic monitoring. NYS Open Legislation | NYSenate.gov*
  - *Proposed addition:*
    - *Similar to Connecticut, New York requires employers to provide prior written notice to employees if they monitor or otherwise intercept phone conversations, email, or internet access. Employers must obtain their employees*

*acknowledgement of the notice, and post the notice of electronic monitoring in a conspicuous place that can readily be viewed by employees.*

- *TX also may have rules on monitoring employees but need to verify.*

- *Proposed new para. 4*
  - *California is the only state whose comprehensive privacy law applies to employees. (CAL. CIV. CODE § 1798.145(m)(4)). For example, under the law, employers are required to provide employees with a (1) notice at collection detailing the collect, use, retention, disclosures of personal information; (2) respond to an employee's rights re-quest (subject to exceptions) regarding their personal information; and (3) provide a mechanism for employees to "opt-out" of the employer selling or sharing their personal information. (CAL. CIV. CODE § 1798.100-1798.135).*



- *Change Twitter to "X (formerly known as Twitter)"*



- *Update to add new section on Privacy Laws Outside the US EU/GDPR/UK & Other Regions (Latin American, APAC, China*
  - *Summarize the basic principles that underlie essentially every one of these laws: BASIC PRINCIPLES*

        - *Data minimization*
        - *Purpose limitation*
        - *Storage/retention limits*
        - *Lawful basis for processing*
        - *Data subject access rights*
        - *Breach notifications*
    - *Address the most difficult questions for consideration by US businesses with activities in foreign jurisdictions; SCOPE AND REQUIREMENTS*
        - *1. How do these laws define "personal information"?*
        - *2. What is the jurisdictional reach of the laws?*
            - *Offering of goods and services in the territory or to residents*
            - *Collection and processing of residents of the territory*
            - *Undertaking processing on behalf of a business located in or collecting the data of residents of those territories*
        - *3. How do foreign laws address transfers and what are the mechanisms in place that allow for transfer of data to the USA from foreign territories?*
            - *Any restrictions imposed for local storage?*
        - *Issues for global companies (intercompany data transfers)*
    - *Scope: Focus on foreign privacy laws of general applicability and those that have the greatest impact on US businesses LAWS OF KEY REGIONS*
        - *EU GDPR*
        - *UK DPA (highlight any differences from EU GDPR)*
        - *Swiss DPA (highlight any differences from EU GDPR)*
        - *China PIPL*
        - *South Korea PIPA*
        - *Singapore PDPA*
        - *India DPDA*
        - *Israel PPL*
        - *UAE PDPL*
        - *Brazil LGPD*
        - *Canada Digital Charter Implementation Act*

- *Update to add new section on Practical Considerations*
    - *Record retention (data minimization, purpose limitation)*
    - *Vendor management*
    - *Big data, emerging technologies, AI*
    - *Information security, de-identification/de-risking data*