Updates and Insights on US Data Privacy and Security

May 27, 2021

I. Update on Federal policy and rulemaking related to Data Privacy

A. The Push for a Comprehensive Federal privacy Bill

1. Despite an increased volume of attention and interest in a comprehensive (or at least reasonably consistent) federal data privacy regime, no new federal legislation for data privacy has been successful, with broad skepticism about the likelihood of a near-term bill gaining passage. As a result, although still largely driven by sectoral regulation, it is increasingly common for companies—particularly in highly regulated industries or environments—to be subject to multiple, overlapping rules and regimes for protection of personal information.
2. This patchwork of overlapping regimes creates significant legal, compliance, and operational challenges for regulated entities. It is also confusing for average consumers, and results in inconsistent protections.
3. There have been numerous Congressional hearings, meetings, proposed bills, and press events focused on federal data privacy initiatives, but privacy advocates are skeptical of the possibility of substantive federal privacy legislation in the near term.
4. Two main areas of disagreement have proven to be barriers to progress.
    a. First, proposals are divided on whether a law should include broad federal preemption of state privacy law. Opponents of broad preemption have argued that the states should serve as "laboratories of democracy" by implementing their own privacy laws instead of (or in addition to) a new federal law. Advocates of broad preemption stress the importance of a single, national set of rules for regulated entities to follow.
    b. Second, proposals are divided on whether to include a private right of action. Proponents of private lawsuits argue that individuals should be able to seek redress for violations of legally protected privacy rights, as well as supplement public enforcement. Opponents may not be against a private right of action in all cases, but are concerned about the potential costs of nuisance lawsuits—especially where proposals allow for class actions and damage multipliers.
5. In addition to these two areas of disagreement, constituencies are divided on the fundamental question of what goal or combination of goals federal privacy legislation should aim to achieve. Proposed objectives include:
    a. Unification (and/or preemption) of disparate state regulatory models;
    b. Enhancing the efficacy and transparency of consumer choice;
    c. Limiting (or, for others, increasing) liability for data breaches;
    d. Addressing concerns regarding the use of machine learning and predictive modeling;
    e. Protecting civil liberties;
    f. Increasing competition; and
    g. Protecting consumers against threat actors.

6. Numerous proposals have included compromises intended to resolve these areas of disagreement, but so far, none has gained enough traction to stand a plausible chance of becoming law.

B. Federal Trade Commission privacy enforcement and rulemaking

1. The FTC remains the primary federal regulatory agency in the area of data privacy for most U.S. companies, and its actions have received significant attention over the past decade.
2. The FTC has reached multiple settlements in matters related to data privacy, including a number of high-profile settlements focused on unfair and deceptive uses of consumer data, as well as unfair and deceptive representations regarding data privacy protections. In particular, the FTC has used its authority under Section 5, which bars unfair and deceptive acts and practices, against companies that have allegedly misled consumers about how their personal information will be safeguarded and used.
3. As the nation's primary federal regulator of issues related to data privacy, the FTC's policy objectives have significant implications for consumers, commercial actors, regulators, and the private bar. It is important, therefore, to understand how the FTC commissioners and staff are considering these topics, including how the FTC may be framing its policy objectives for the coming years.
4. The election of President Joe Biden will affect the FTC's ideological makeup and enforcement priorities. Joseph Simons, the Republican former FTC Chairman, announced his resignation in January 2021, with Democratic Commissioner Rebecca Slaughter taking over as Acting Chairwoman. President Biden nominated Democrat Lina Khan to fill the vacancy, pending Senate confirmation. Finally, President Biden has nominated Commissioner Rohit Chopra, also a Democrat, to serve as director of the Consumer Financial Protection Bureau. If he is confirmed, his departure from the FTC will create another vacancy.
5. In 2019, Acting Chairwoman Slaughter identified a number of potential shifts in policy related to data privacy,[1] beginning first with her view that the "data privacy" framework may be unduly limiting, and that seeking to address "data abuse" may be a more effective and meaningful framework for crafting regulation and protecting consumers.
    a. Data privacy generally refers to limits on the collection or sharing of data that an individual would prefer to keep private. However, Acting Chairwoman Slaughter argues that regulators may not always be able to separate problems involving collecting data about individuals from problems involving the targeting of information to individuals or other decisions made for individuals (often based on the collected data).
    b. For example, a gaming app that uses consumer data to target objectionable advertising to children may raise an issue of potential interest and concern for policymakers and consumers, but might be more readily characterized as a data abuse issue than a data privacy issue.
    c. In addition, Acting Commissioner Slaughter is concerned that targeted advertising could disproportionately harm vulnerable populations (such as children and, potentially, lower-income individuals).

[1] Federal Trade Commission, *The Near Future of U.S. Privacy Law* (Sept. 6, 2019), https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf.

6. A second policy shift identified by Acting Chairwoman Slaughter involves acknowledging the limits of "notice and consent" or "notice and choice" as a framework for consumer protection and information security.
    a. Acting Chairwoman Slaughter has explained that much of the FTC Act authority and some of the FTC's privacy enforcement actions have, up to this point, been grounded in traditional principles of notice and consent, and that the notice-and-consent framework began as a sensible application of basic consumer protection principles to privacy: tell consumers what you are doing with their data, secure their consent, and keep your promises.
        1) But in order for a notice-and-consent regime to be effective, each element must be meaningful—notice must give consumers information they need and can understand, and consumers must have a choice about whether to consent. This framework—to some—seems entirely inapplicable to the digital economy, where there is a widely-held view that neither notice nor consent is particularly meaningful.
        2) From the consumer perspective, notice is mostly in the form of lengthy click-through contracts. Few consumers can dedicate the time and legal parsing required to understand them.[2]
        3) The argument goes, then, that choice is illusory at best.[3] Consumers do not actually have bargaining power—even if they could read and understand the lengthy terms of contracts they must sign, their options are only to agree and access the service or to refuse and be denied access.
    b. In making this argument, Acting Chairwoman Slaughter has also referenced the experience of citizens and corporations grappling with the GDPR's implementation over the last year.
        1) The GDPR, she explains, has the laudable goal of improving consumers' control over their personal data. In practice, however, the rollout resulted in a significant increase in opt-in consent requests whenever a consumer opened a website.
        2) This resulted in people becoming numb to the questions; the "opt-in" became a legal fiction for consumers to ignore.
    c. Acting Chairwoman Slaughter echoes other commenters who have argued that a data privacy regime built entirely on notice and consent puts all of the burden on consumers to protect their privacy, even though consumers have very little control over that data.[4]

---

[2] *See generally* Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?* 45 J. LEGAL STUD. S69, S87, S93 (2016) (courts and laypeople show limited understanding of privacy policy terms); Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 553 (2014) (proposing that the FTC should require sellers to confirm consumers' expectations of the terms in their contracts and to affirmatively warn consumers about unfavorable terms); Florencia Marotta-Wurgler, *Competition and the Quality of Standard Form Contracts: The Case of Software License Agreements*, 5 J. EMPIRICAL LEGAL STUD. 447, 467-73 (2008) (competition in markets does not influence the quality of contractual terms offered by firms in such markets).

[3] *See* Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 29 (2014); Florencia Marotta-Wurgler, *Does Contract Disclosure Matter?*, 168 J. INSTITUTIONAL & THEORETICAL ECON. 94, 114 (2012).

[4] *See generally* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy* (What Larry Doesn't Get), 2001 STAN. TECH. L. REV. 1, 1-10 (reviewing "notice and consent" regimes); Lauren E. Willis, *Why Not Privacy by Default?,* 29 BERKELEY TECH. L.J. 61, 67 (2014) (noting limitations of choice framework).

1) This argument holds that the companies that have control over personal data should have the burden of properly using and protecting it.

2) Companies can and do track consumers across their devices and locations, and data about consumers is shared, sold, or used for targeting.

3) Much of this happens between and among companies with which consumers never choose to interact.

d. Therefore, Acting Commissioner Slaughter has argued that regulators should consider reasonable consumer expectations about data collection and data use as guideposts, but that the onus to carefully protect personal data should ultimately be placed on the companies that collect, use, and share it, and not on the consumers alone.

1) Thoughtful purpose and use limitations will be critical to protect consumers, especially when it comes to sensitive data.

2) There may also be some places where clear, prominent, plain-English notice and true consumer consent can play a valuable role.

e. Finally, a third policy shift identified by Acting Chairwoman Slaughter has involved increasing the focus on data abuses and vulnerable populations.

1) As reflected in the example discussed above, there is a view among data privacy advocates that data abuses disproportionately affect vulnerable populations. Acting Chairwoman Slaughter has said that, in her view, regulators need to ensure that laws and their enforcement reflect democratic values and principles of equality and thereby protect everyone.

2) In the data protection context, Acting Chairwoman Slaughter and other privacy advocates have encouraged studying and acknowledging the ways that certain harms fall disproportionately on disadvantaged or vulnerable populations.

3) To this end, Acting Commissioner Slaughter has cautioned against complacent adoption of a default system in which the privileged and wealthy are the only ones who are protected against data abuses (i.e., a world in which the privileged can pay for access to services with only their dollars, while others are left to pay with their data or with their willingness to be exposed to objectionable content).

f. President Biden's nominee to the FTC, Lina Khan, suggested at her recent confirmation hearing the possibility that the FTC could use its antitrust authority to address privacy issues, under the theory that the use of data to maintain a monopoly position is anti-competitive. However, it is not clear that the FTC could pursue "data-as-monopoly" enforcement in the absence of new legislation.

g. The FTC could also promulgate a privacy rule under the Magnuson-Moss Warranty Act. So-called "Mag-Moss" rulemaking has fallen into disuse in recent decades, but a bipartisan majority of current commissioners has indicated willingness to consider a privacy rulemaking—particularly in the absence of congressional action.

C. Other federal regulations

1. Although they have received relatively less attention in recent years, several other subject-specific U.S. data privacy regulations remain an important part of the regulatory landscape:

a. The Gramm-Leach-Bliley Act ("GLBA") (also known as the Financial Modernization Act of 1999)

1) The GLBA requires financial institutions to safeguard the nonpublic personal information of consumers and customers, as defined in the GLBA.

2) Under the GLBA, regulated entities must establish written policies and procedures "reasonably designed" to protect the security and confidentiality of customer information and to safeguard against potential threats to such information, as well as to prevent unauthorized access to, or use of, such information.[5]

3) The FTC, federal bank agencies, and other regulatory authorities enforce the GLBA, depending upon the type of covered entity and the applicable rule.

b. Health Insurance Portability and Accountability Act ("HIPAA")

1) HIPAA requires covered entities (including health plans, health care clearinghouses and health care providers, and certain business associates of such entities) to use reasonable technical, administrative, and physical safeguards to protect the security and confidentiality of protected health information.[6]

2) Protected health information includes individually identifiable health information transmitted or maintained electronically or in any other form or medium.[7]

3) The U.S. Department of Health and Human Services Office for Civil Rights enforces HIPAA.

c. The Children's Online Privacy Protection Act ("COPPA")

1) COPPA requires covered website operators to take certain actions with respect to information collected from children under 13. Among other things, operators must post a privacy policy, obtain parental consent before collecting personal information from children, provide parents access to their child's information to review or have deleted, and take steps to secure information collected from children.[8]

2) The FTC enforces COPPA and has brought a number of recent high-profile actions alleging failure to comply with COPPA requirements.

II. Update on Other Privacy Regulations

In the absence of comprehensive federal privacy legislation, the U.S. has witnessed a proliferation of state-specific data privacy and breach notification laws.

A. State-Specific Data Privacy Laws

1. **California Consumer Privacy Act (CCPA).** California's CCPA became effective as of January 1, 2020,[9] and is expected to have a transformative impact on data privacy legislation in the years ahead.

[5] 17 C.F.R. § 248.30(a).

[6] 45 C.F.R. §§ 164.306, 308, 310, 312.

[7] 45 C.F.R. § 160.103.

[8] 16 C.F.R. § 312.3.

[9] Cal. Civ. Code §§ 1798.100-1798.199.

a. The CCPA established a consumer right to request details from covered businesses about the collection of their personal information, the purpose of such collection, and third parties with whom the personal information has been or may be shared. Covered businesses are also required to:

   1) Delete personal information upon request (subject to certain exceptions);

   2) Disclose certain information regarding their sale of personal information; and

   3) Provide consumers the right to opt out of having their personal information sold, without discriminating against those who do opt out.

b. Covered businesses under the CCPA include any business that:

   1) Collects personal information about consumers, defined as natural persons who are California residents;

   2) Does business in California; and

   3) Meets at least one of three criteria: (a) has annual gross revenues exceeding $25 million; (b) buys, receives, sells or shares the personal information of 50,000 or more consumers, households or devices annually; or (c) derives 50 percent or more of its annual revenue from selling consumers' personal information.

   4) Like Europe's GDPR, the CCPA defines "personal information" broadly. Though the definitions under the two rules are not identical, as the CCPA also encompasses information that can be linked to "household[s]," even if not to individual consumers.

c. Remedies and Penalties under the CCPA:

   1) In its current form, the CCPA provides a private right of action only for consumers in the event certain of their non-encrypted personal information is stolen or leaked as a result of a covered business's failure to implement and maintain reasonable security procedures and practices. Remedies available to consumers under the Act are the greater of actual damages or statutory damages of $100 to $750, but notice and a 30-day opportunity to cure must be provided to the business before a consumer may seek statutory damages.

   2) Violations of other provisions of the act are subject to enforcement only by the California Attorney General, who may bring an action for a civil penalty of up to $2,500 per violation or $7,500 per intentional violation. Actions by the Attorney General for violations of the act are also subject to a 30-day notice-and-opportunity-to-cure requirement.

d. To comply with the positive notice and consent requirements of the CCPA, companies have been undergoing significant and resource-intensive projects related to data privacy. How and whether these projects will be effective in limiting corporate risk and liability should be the subject of careful consideration in the years ahead.

e. Consumers have tested the limits of the private right of action in 2020, and have filed at least 62 proposed class actions in California federal court and 14 in state court alleging violations of the CCPA.[10]

[10] *See* Allison Grande, *Calif. Privacy Suits Tested Novel Law's Limits in 1st Year*, Law360 (Mar. 3, 2021), https://www.law360.com/articles/1367934/calif-privacy-suits-tested-novel-law-s-limits-in-1st-year.

1) Less than half of these filings allege that California residents' personal information had been impacted due to a data breach, and instead allege that a company violated some other aspect of the CCPA, such as the requirements for businesses to disclose what information they're collecting and to allow consumers to opt out of the sale of their data.[11]

2) Other CCPA issues that have been raised by these actions include what it means for a company to "do business" in California and therefore be subject to liability under the law; whether non-California residents can bring these lawsuits; whether plaintiffs have Article III standing to support their claims; and whether an alleged CCPA violation outside the data breach context can support claims for infractions of different statutes, such as the state's Unfair Competition Law.[12]

3) Courts have yet to weigh in on whether these CCPA claims will be successful, but they will be an important area to monitor going forward.

f. California voters amended the CCPA by ballot initiative in 2020. The California Privacy Rights Act (CPRA) amends the CCPA in a number of ways and will go into effect in most material respects on January 1, 2023. Changes include:

1) Extending the CCPA's private right of action to include data breaches impacting email and login credentials.

2) Adding an opt-out provision for cross-context behavioral advertising.

3) Establishing the California Privacy Protection Agency (CPPA). The CPPA will be headed by a five-member board and have full administrative enforcement power to protect Californian's privacy rights.

2. **Virginia Consumer Data Protection Act (CPDA)** Virginia's CPDA will go into effect January 1, 2023 and represents a potential alternative to the CCPA/CPRA framework.

a. The CPDA establishes a framework for controlling and processing personal data in Virginia. It establishes data controller and processor obligations and grants consumer rights to access, correct, delete, and obtain a copy of personal data. The CPDA also allows consumers to opt-out of personal data processing for targeting advertising.

b. Covered businesses under the CPDA include businesses that conduct business in Virginia or target residents and that:

1) During a calendar year, control or process personal data of at least 100,000 consumers, or

2) Control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data.

3. **Illinois Biometric Information Privacy Act (BIPA).** Illinois' BIPA was enacted in 2008[13] and has given rise to hundreds of lawsuits in Illinois state and federal courts.

[11] *Id.*

[12] *Id.*

[13] 740 Ill. Comp. Stat. Ann. 14/1-14/99.

a. BIPA establishes protections for biometric identifiers and information (retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry).

b. Covered businesses under BIPA include any "private entity,"[14] meaning:

   1) Any individual, partnership, corporation, limited liability company, association, or other group, however organized.

   2) A private entity does not include a State or local government agency.

c. Remedies and Penalties under BIPA:[15]

   1) BIPA provides a private right of action for any person aggrieved by a violation in state circuit court or as a supplemental claim in federal court. A prevailing party can recover:

      a) $1,000 for each negligent violation by a private entity.

      b) $5,000 for each intentional or reckless violation by a private entity.

d. BIPA has spawned hundreds of class action suits across Illinois state courts as well as federal courts. The private right of action often intersects with other areas of law, posing novel legal questions for the judiciary. For instance:

   1) *In re: Marquita McDonald v. Symphony Bronzeville Park LLC* is an Illinois Supreme Court case yet to be decided that encapsulates how BIPA's private right of action poses issues for courts. The Appellate Court of Illinois, First District ruled that an employee's BIPA claim was not preempted by a workers' compensation exclusivity provision. This allowed the plaintiff to seek damages for employer's use of biometric time clock under BIPA.[16] The Supreme Court of Illinois will decide whether BIPA injuries such as those suffered by the plaintiff in *Symphony Bronzeville Park* should be preempted by existing employment law.

   2) *In West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan Inc.*, the Illinois Supreme Court held that a biometric privacy claim fell within a particular class of liability insurance policies. The Court found that a tanning salon that shared fingerprint information with a third-party vendor constituted an advertising injury, and that the liability insurance provider had a duty to defend the subsequent BIPA class action lawsuit.[17]

4. **Nevada Senate Bill 220 (SB 220)** went into effect on October 1, 2019 and was developed to modify and strengthen existing data privacy and security laws.[18]

   a. Nevada's privacy law gives consumers the right to opt-out of having certain collected and covered information sold to third parties. Operators must respond to verified opt-out requests from consumers within 60 days.

   b. Covered businesses include operators that:

---

[14] 740 Ill. Comp. Stat. Ann. 14/10.

[15] 740 Ill. Comp. Stat. Ann. 14/20.

[16] *See McDonald v. Symphony Bronzeville Park LLC*, 2020 IL App (1st) 192398, appeal allowed, 163 N.E.3d 746 (Ill. 2021)

[17] *See W. Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc.*, 2021 IL 125978.

[18] *See* Nev. Rev. Stat. Ann. § 603A (West).

1) Own or operate an Internet website or online service for commercial purposes;

2) Collect or maintain covered information from consumers who reside in Nevada and use or visit the Internet website or online service; and

3) Have purposely availed itself of the privilege of conducting business within the State.

c. Nevada's privacy law contains no private right of action. The State Attorney General may institute enforcement action. Remedies and penalties under Nevada's privacy laws include temporary or permanent injunctions and civil penalties of no more than $5,000 per violation.

5. **Maine's Act to Protect the Privacy of Online Customer Information (BSP Privacy Act)** went into effect July 1, 2020 and regulates internet service providers (ISP).

a. Maine's BSP Privacy Act prohibits broadband ISPs from selling, disclosing, or permitting access to customers' personal information without the customer's express opt-in consent, unless narrow exceptions are met.

b. Covered businesses under Maine's BSP Privacy Act include any provider of "broadband Internet access service." Providers must be operating within Maine when providing broadband Internet access service to customers that are billed for service received in Maine and are physically located within the State.

c. Maine's BSP Privacy Act survived a broad challenge to its constitutionality recently.[19] A federal district court held that the law was not unconstitutionally vague, that is was not an unconstitutional regulation of commercial speech, and that the Act was not preempted by implication by federal law.

6. Many state legislatures are grappling with passing data privacy laws. A common point of contention is whether to include a private right of action to allow consumers to have standing to sue covered businesses. The private right of action is often decisive in whether a bill will pass in a particular state.

a. Florida Privacy Protection Act

1) Regulation of data processors as well as various opt-in/opt-out provisions.

2) Passed in Florida State House with private right of action. Senate removed provision and progress stalled.

b. Washington Privacy Act (SB 5062) & People's Privacy Act (BH 1433)

1) House bill contained private right of action. Senate bill expressly disavowed private right of action. Legislature adjourned without passing bill.

c. Colorado (Protect Personal Data Privacy) SB 21-190

1) Provides consumers with opt-out right.

2) No private right of action. As of May 2021, the bill is still moving through the Colorado legislature.

3) Colorado legislature adjourns on June 12, 2021.

[19] *See ACA Connects - Am.'s Commc'ns Ass'n v. Frey*, 471 F. Supp. 3d 318, 326 (D. Me. 2020).

d. Texas (An act relating to the personal identifying information collected, processed, or maintained by certain businesses; imposing a civil penalty) HB 3741

1) The Texas Act creates a three-tiered structure for types of personal identifying information.

2) No private right of action. Bill was introduced on March 11, 2021.

3) Texas legislative session ends May 31, 2021.

B. State-Specific Data Breach Laws

1. All U.S. states, as well as the District of Columbia, Puerto Rico, and Guam, now have their own data breach notification laws. Although they vary in certain respects—including in their definitions of personally identifying information—most state rules cover some combination of first name or first initial with the last name of an individual, in conjunction with their social security number, driver's license number, financial number, or medical information.

2. Notification triggers and substantive notification requirements vary from state-to-state, at times significantly.

   a. There is significant variation in the specific language used to describe the trigger for the notification (e.g., notification may be required upon "discovery or notification" of a breach, when the company "becomes aware" of the breach, "knows" about the breach, "knows or has reason to know" about the breach, or simply "discovers" the breach). That said, all states require notification at some point after a breach occurs once the company discovers or knows of the breach. And in the majority of states, notification obligations are triggered by the company's "discovery" or "notification" of a breach (e.g., "discovering or being notified," "discovery or notification," or "discovers or is notified").

   b. In a majority of states, a determination of a breach alone does not trigger notification to affected individuals. Rather, most states further require companies to perform a "risk of harm" analysis before determining whether notification of the breach is required. In most instances, "harm" in this case is interpreted or defined as "substantial economic loss" by affected individuals.

3. In addition to notifying affected individuals, though, a number of states also require an additional notification to the state's attorney general, normally triggered when the breach affects more than a certain number of residents of that state. Many states require notification to the attorney general where more than 1,000 individuals are affected by the data breach, though the exact number varies. Some states also require notification to consumer reporting agencies in the event of a breach.

C. NYDFS

1. Despite being sector-specific and limited in coverage to registered entities, the New York Department of Financial Services ("NYDFS") Cybersecurity Requirements for Financial Services Companies[20]—which began phased implementation beginning September 1, 2017, and became

[20] NYDFS Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500), https://www.dfs.ny.gov/industry_guidance/cybersecurity. Covered entities for purposes of the NYDFS regulations include, in effect, any entities operating under the auspices of New York State Banking Law, Insurance Law or Financial Services Law.

fully effective as of March 2019—received significant attention for compressing notification timelines and otherwise imposing strict and specific security protections on covered entities.

a. The NYDFS cybersecurity regulations are expected to have a lasting impact on cybersecurity regulations and expectations for data privacy due to the unique combination of (1) concrete cybersecurity requirements (e.g., access controls), (2) a senior-level certification obligation, and (3) the 72-hour notice requirement after a breach.

b. Under the NYDFS regulation, covered companies must, among other things, take the following steps:

   1) Designate a Chief Information Security Officer ("CISO");

   2) Implement the required elements of a cybersecurity program, cybersecurity policies, and an incident response plan;

   3) Regulate access privileges for information systems;

   4) Ensure that required cybersecurity personnel are in place;

   5) Prepare to notify the NYDFS within 72 hours of certain cybersecurity events; and

   6) Conduct a risk assessment (effective March 1, 2018).

c. The cybersecurity events that trigger the 72-hour notice requirement include those that:

   1) Require notice to be provided to any other government body, self-regulatory agency, or supervisory body; or

   2) Create a reasonable likelihood of materially harming any part of the normal operation of your company.

d. NYDFS brought its first cybersecurity enforcement action in June 2018, less than one year after the phase-in of the cybersecurity rules had begun.[21]

   1) On June 27, 2018 the NYDFS announced that Equifax agreed to take corrective action for its 2017 data breach, as set forth in a consent order reached with the NYDFS and seven other state banking regulators.

   2) The order required Equifax to improve its cybersecurity practices in several areas and includes very specific requirements and provided a glimpse into what the NYDFS views as sound cybersecurity practices.

   3) The order included the following requirements:

      a) *Information Technology*: The Equifax board must review and approve a written risk assessment that identifies (1) foreseeable threats and vulnerabilities to the confidentiality of personally identifiable information; (2) the likelihood of threats; (3) the potential damage to the company's business operations; and (4) the safeguards and mitigating controls that address each threat and vulnerability.

      b) *Audit*: To improve the oversight of Equifax's audit function, the Equifax Audit Committee must oversee the establishment of a formal and documented internal

[21] Davis Polk Cyber Blog, *NYDFS Brings Its First Cybersecurity Enforcement Action* (June 29, 2018), https://www.dpwcyberblog.com/2018/06/nydfs-brings-its-first-cybersecurity-enforcement-action/.

audit program that is capable of effectively evaluating IT controls and that complies with the internal audit charter.

c) *Board and Management Oversight*: Equifax must improve the oversight of its Information Security Program. For example, the order required the board to approve a consolidated written Information Security Program and Information Security Policy and annually thereafter and review an annual report from management on the adequacy of the company's Information Security Program.

d) *Vendor Management*: Equifax must improve oversight and documentation of critical vendors and ensure that sufficient controls are developed to safeguard information.

e) *Patch Management*: Equifax must improve standards and controls for supporting the patch management function. An effective patch management program must be implemented to reduce the number of unpatched systems and instances of extended patching time frames.

f) *Information Technology Operations*: Equifax must enhance oversight of IT operations as it relates to disaster recovery and business continuity function.

D. European Union General Data Protection Regulation[22]

1. The GDPR repealed and replaced certain existing E.U. data privacy rules and became effective on May 25, 2018.
2. As has been widely cataloged, the GDPR:
    a. Regulates the processing of personal data (i) of establishments in the E.U. and (ii) related to the offering of goods or services to data subjects in the E.U. or the monitoring of behavior of data subjects in the E.U.
    b. Applies to thousands of U.S. companies that use or store the personal data of individuals living in the E.U.
    c. Institutes the strictest data breach notification obligations of any generally applicable cybersecurity law, requiring covered businesses to notify the appropriate authority within 72 hours after learning of the breach.
    d. Imposes administrative fines up to the greater of 20,000,000 Euros or 4% of global annual revenue for failure to comply with substantive requirements.
3. Despite a number of substantial enforcement actions under the GDPR and massive investments across industries in data privacy infrastructure, there is a robust, ongoing discussion about whether the GDPR is "working," both within and beyond the borders of the E.U.
4. Under the GDPR, EU personal data may be transferred from the E.U. to the U.S. only if the U.S. entity provides appropriate safeguards, or only under certain enumerated circumstances.
    a. Since 2016, the E.U.-U.S. Privacy Shield has facilitated certain of these transfers by establishing data privacy safeguards and protections for E.U. data subjects. However, in

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (full text available online at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679).

July 2020, the E.U.-U.S. Privacy Shield was invalidated as an acceptable method of data transfer by the recent *Schrems II*[23] decision.

b. Further, on May 19, 2021, new standard contractual clauses (another E.U.-approved method of data transfer) proposed by the European Commission have been approved and will be issued shortly.

III. Privacy interactions with adjacent subject-matters

A. Bank Secrecy Act and Anti-Money Laundering

1. As Anti-Money Laundering (AML) concerns receive increased attention, businesses and consumers must grapple with privacy considerations that are inherently at tension with the increased transparency of personal information required by AML regulations (e.g., Bank Secrecy Act ("BSA") of 1970).
2. There has been recent interest in establishing BSA/AML laws that balance the need for increased transparency of personal information against privacy and security interests, as reflected in recently passed BSA/AML legislation:
    a. The Anti-Money Laundering Act of 2020 (AMLA) notably introduced a new identifier issued by FinCEN and exclusive to a particular individual or entity, which may be provided by beneficial owners ("BO") in lieu of an unique identifying number from an acceptable identification document.
    b. The Corporate Transparency Act ("CTA") created a national registry of BO information for "reporting companies" in order to counter money laundering. Under the CTA, access to the BO database must be restricted only to necessary and adequately trained users at the requesting agency, and the requesting agency must establish and maintain a secure system to store the BO information and provide a report to the Secretary that describes how it is ensuring the confidentiality of the BO information.

B. Artificial Intelligence

1. Request for Information on Use of Artificial Intelligence
    a. On March 31, 2021, five federal agencies issued a request for information ("RFI") on financial institutions' use of artificial intelligence, recognizing the benefits and risks of AI to both consumers and businesses.[24]
    b. The agencies stated that the purpose is to understand the practices and challenges in developing, adopting, and managing AI, as well as areas where clarification by the agencies would be helpful.

---

[23] Regulation C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems ("Schrems II"), available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=9793916.

[24] Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning, 86 Fed. Reg. 16837 (filed Mar. 30, 2021), available at https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence

c. The RFI highlights several areas of risks of AI, some which overlap with data privacy and security concerns: explainability, overfitting, cybersecurity risks, dynamic updating, oversight of third parties, and fair lending.

d. The agencies must receive any comments by next week, June 1, 2021.

2. European Union's Proposed Rules on Artificial Intelligence

a. Last month, the European Commission released its proposed rules on artificial intelligence.[25] The main provisions consist of:

1) Binding rules for AI systems that apply to providers, users, importers, and distributors of AI systems in the EU, regardless of where they are based;

2) A list of certain prohibited AI systems;

3) Extensive compliance obligations for providers and users of "high-risk" AI systems; and

4) Fines of up to the higher of EUR 30 million or 6% annual turnover.

b. The Commission proposed a risk-based approach. The proposed rules do not include any specific requirements for non-enumerated AI systems and those that do not qualify as "high-risk."

c. Enforcement of the AI regulations are left to the member states.

d. The proposed regulations do not replicate the GDPR's "one stop shop" system, which may lead to consistency concerns across the 27 member states.

C. Health and Safety

1. The goals of advancing community health have long conflicted with goals of protecting personal health data. The COVID-19 pandemic, however, has created new challenges for individuals and businesses that involve balancing public safety and personal health concerns.

a. Some examples of issues resulting from the COVID-19 pandemic include whether employers may implement a mandatory vaccine policy or collect employee's vaccine status[26] and relatedly, whether businesses and governments may require "vaccine passports" that show proof of vaccination status.[27]

2. In efforts to respond to these challenges, the Department of Health and Human Services Office for Civil Rights (OCR) has relaxed HIPAA enforcement for companies acting good faith, and has issued new guidance to companies to ensure HIPAA compliance.[28]

---

[25] Proposal for a Regulation 2021/0106 of the European Parliament and of the Council of 21 April 2021, (full text available online at https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence).

[26] *See* Jennifer Bryant, *Return to the office 'a perfect storm' of privacy issues for businesses*, IAPP (April 27, 2021), available at https://iapp.org/news/a/return-to-office-a-perfect-storm-of-privacy-issues-for-businesses/.

[27] *See* Linda Chiem, *As CDC Eases Travel Guidance, Are 'Vaccine Passports' Next?*, Law360 (April 21, 2021), available at https://www.law360.com/articles/1371784.

[28] *See U.S. Cybersecurity and Data Privacy Outline and Review – 2021*, Gibson Dunn (Jan. 28, 2021), available at https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2021/.

IV. U.S. Privacy Law in an International Context

A. Broadly speaking, the world of privacy regulation can be viewed as having three poles: the United States, the European Union, and China.

B. In the United States, data is viewed as an alienable commodity. It can be bought and sold like any other good, and, once sold, it belongs to the buyer.

C. The European Union views data privacy as an inalienable human right. According to this view, personal data inherently belongs to users and they have the right to retrieve or delete it even after selling it. Central to this view of the world is the misuse of personal data by 20th-century European dictatorships to commit atrocities. The view of data privacy as a fundamental right is best understood in light of that relatively recent history.

D. In China, the government does not conceive of data privacy as an individual right, and considerations of personal privacy are regarded as subordinate to state interest.

E. These three approaches to data privacy are mutually incompatible—moving closer to one pole requires moving away from the other two. Needless to say, this mutual incompatibility presents a challenge for companies operating internationally.

F. Other countries can be viewed as falling on a spectrum between these poles.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your usual Davis Polk contact.

Jon Leibowitz	+1 202 962 7050	jon.leibowitz@davispolk.com
Matthew A. Kelly	+1 212 450 4903	matthew.kelly@davispolk.com
Mikaela Dealissia	+1 212 450 3534	mikaela.dealissia@davispolk.com