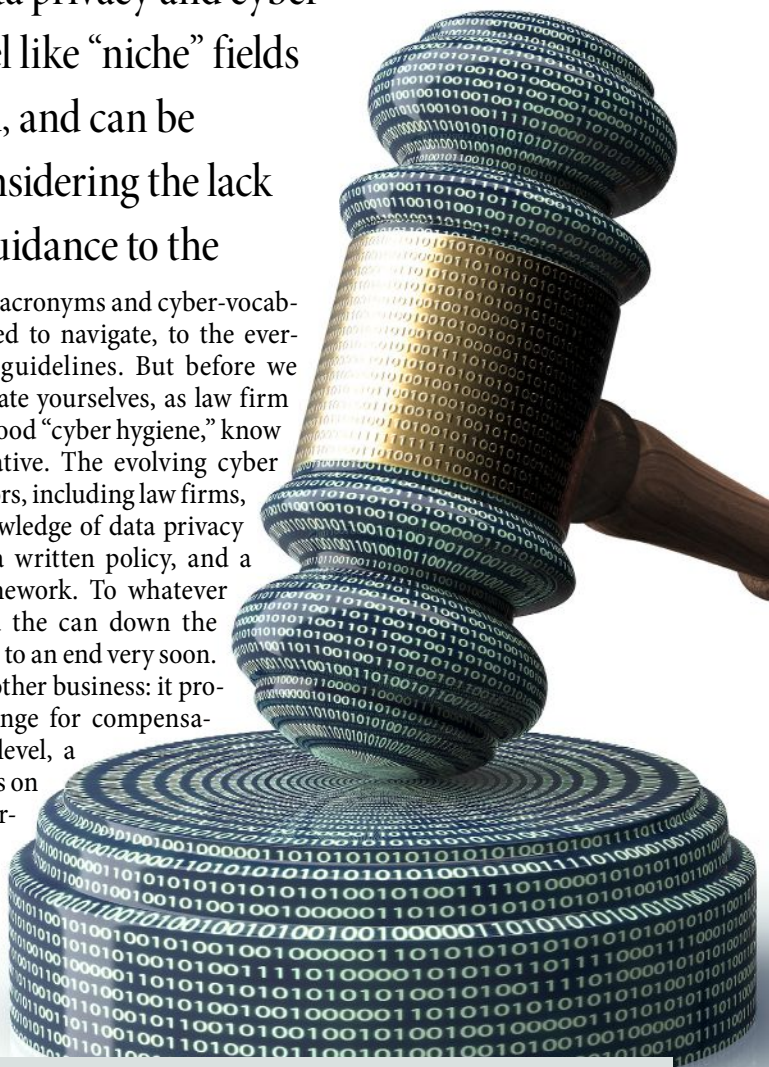
What to Expect When You're *Not* Expecting a Data Breach

Legislative Trends in Data Privacy and Cyber Security

By Brian Gibbons and Lauren Berenbaum

Now, more than ever, it is necessary for law firms to understand the current data landscape, the direction of legislation, and the types of issues being addressed by the federal courts.

The worlds of data privacy and cyber security often feel like "niche" fields in the legal world, and can be intimidating, considering the lack of clear federal guidance to the seemingly endless lists of acronyms and cyber-vocabulary that one is expected to navigate, to the ever-changing state-by-state guidelines. But before we relay the reasons to educate yourselves, as law firm managers, in practicing good "cyber hygiene," know this—there is no alternative. The evolving cyber requirements on all vendors, including law firms, mandates a working knowledge of data privacy terms, the existence of a written policy, and a basic cybersecurity framework. To whatever extent you have "kicked the can down the road," that road is coming to an end very soon.



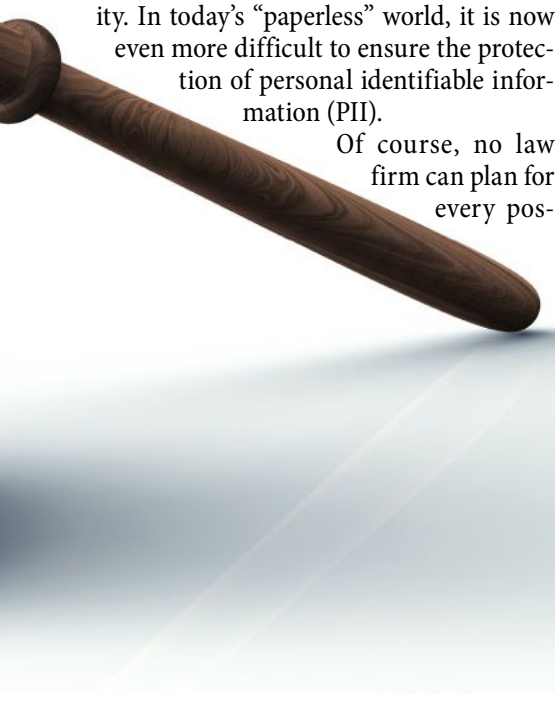
A law firm is like any other business: it provides a service in exchange for compensation. At the most basic level, a law firm's success depends on its ability to cultivate attorney–client relationships and maintain client trust and confidence. Trust is a fundamental principle in the attorney–client relationship as

■ Brian Gibbons is a partner at Wade Clark Mulcahy, based in New York, New Jersey, and Pennsylvania. Brian is the resident partner at the firm's Long Island Office. In addition to being a CIPP-US and CIPM, Brian tries cases and argues appeals in New York State and Federal Court. Lauren Berenbaum, a CIPP-US, is an associate at WCM and practices in Pennsylvania, New York and New Jersey.

clients must feel confident the information shared with their attorney is safeguarded and protected. As data collectors and processors, attorneys and firms are ethically and legally obligated to ensure data protection.

The past year tested client trust as the pandemic exposed glaring gaps and flaws in the current system of data privacy and cybersecurity in the United States and solidified the need for law firms to establish reasonable data collection safeguards. Once we began to socially and physically distance, the world needed to shift to remote work immediately. (In that sense, we are all fortunate that COVID-19 was not COVID-09, because many law firms and other businesses would not have survived the pandemic, given our technological deficiency only ten years earlier.)

This need to maintain business operations increased our reliance on cloud technologies and forced employees to use personal devices and home networks. **Cybersecurity Lessons Learned from the Pandemic** – CSC White Paper. Law firms, like all businesses, were largely unprepared for the rapid sea change, and did not have the infrastructure to support safe work and ensure the security of data. Unfortunately, as law firms collect sensitive client data, law firms became increasingly vulnerable to cyberattacks and malicious cyber activity. In today's "paperless" world, it is now even more difficult to ensure the protection of personal identifiable information (PII).



Of course, no law firm can plan for every possible "worst case" scenario out there. But think about what you would do if you found out your PII was inadvertently emailed to hundreds of people and you subsequently became a victim of identify fraud. Imagine hearing that the law firm you trusted had no protocols in place to prevent or respond to the data breach. Regardless of whether the breach was accidental, this scenario exposes the firm to civil liability and professional conduct violations—not to mention the incurrence of defense costs and unquantifiable reputational harm.

The current data environment is complex and is composed of immense uncertainty as there is no federal law regulating data privacy, the enacted state laws (among the states that even have laws enacted to address data privacy) are not standardized and there is evolving legal precedent. As our reliance on technology continues to grow, the need to implement cybersecurity and data privacy policies is crucial. Now, more than ever, it is necessary for law firms to understand the current data landscape, the direction of legislation, and the types of issues being addressed by the federal courts.

Trends in Privacy Laws and Regulations

The United States has not implemented a comprehensive federal law regulating PII. The lack of guidance is problematic as businesses require predictability and certainty to mitigate liability risks and consumers need transparency and accountability to maintain trust. Americans also maintain a reasonable expectation of privacy, a civil liberty protected by the federal government through the enactment of legislation in specific sectors—the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm–Leach–Bliley Act are just two examples. (HIPAA was passed to, *inter alia*, create national standards for electronic healthcare transactions and provide patients with an opt-in approach to whether their information can be shared with other organizations and individuals. 42 U.S.C. §1320d-2 (2001). In pertinent part, the HIPAA privacy rule focuses on authorizations for use and disclosure, access and accounting of disclosures, de-identification, and authorizations for use and disclosure. *See id.* In 1999, the Gramm–Leach–Bliley Act was enacted to control the way financial institutions deal with the private information of individuals, such as requiring these institutions to share their information-sharing practices with consumers and safeguard sensitive data. 15 U.S.C. §6802.) Since there is no federal law, some states—including, Illinois, California, Virginia, Colorado, New York, Texas, Arizona, and Washington—have enacted data privacy laws focused on guidance and enforcement. In fact, there are currently thirty-eight states that have proposed bills or legislation addressing cybersecurity. State data privacy laws and the General Data Protection Regulation implemented by the European Union provide useful guidance as to what to expect in a federal law.

Unfortunately, as law firms collect sensitive client data, law firms became increasingly vulnerable to cyberattacks and malicious cyber activity. In today's "paperless" world, it is now even more difficult to ensure the protection of personal identifiable information (PII).

European Union: GDPR

On May 25, 2018, the European Union implemented the General Data Protection Regulation (GDPR), which was designed to standardize how companies and entities process and use personal data. EU GDPR 2016/679. Significantly, the GDPR is designed to simultaneously protect EU citizens from privacy and data breaches and provide consistent guidelines to companies working with PII. The guiding principles behind the GDPR concern transparency, data minimization, and accountability.

The GDPR's applicability is far reaching, applying to organizations established outside of the EU if the organization: (1) offers goods or services (including online sales) to data subjects in the EU; (2) monitors the behavior of data subjects in the EU; or (3) provides services to an entity described above. The General Data Protection Regulation, 3 Records Retention §68:3.75. Law firms that operate internationally, service clients with business beyond the U.S. or transfer data abroad should be aware of the applicable laws and protocols.

BIPA receives great attention because it is the first state law to afford aggrieved individuals with the ability to commence a private right of action sounding in a statutory violation.

As compared to the United States, the GDPR is more geared toward individual privacy rights. This trend toward individual privacy stems from World War II, and even entails the right to be forgotten (RTBF)—described as the right to have private information about oneself removed from Internet searches and other directories under some circumstances. The concept is indicative of the GDPR's focus on individual privacy rights.

Prominent State Data Privacy Laws

California's Consumer Privacy Act of 2018

California's Consumer Privacy Act of 2018 (CCPA) went into effect on January 1, 2020, and applies to, *inter alia*, any for-profit company that conducts business in California and collects personal information from a California resident; and either (a) has annual gross revenue over $25 million; (b) annually buys, sells, receives, or shares for a commercial purpose the personal information of 50,000 or more consumers, households, or devices; or (c) derives 50 percent or more of its annual revenues from selling consumer's personal information. Civ. Code §1798.140(c).

CCPA is prominent because it represents a major step toward expanding consumer privacy rights in the United States. Similar to the GDPR, CCPA is focused on consumer transparency. For example, upon request, a business that collects personal information, including biometric data, about a consumer must disclose (1) the categories of personal information collected about the consumer; (2) the categories of sources from which personal information is collected; (3) the business or commercial purposes for collecting or selling the personal information; (4) the categories of third parties with which the personal information is shared or sold; and (5) the specific pieces of personal information collected about that consumer. Civ. Code §1798.115. CCPA also requires businesses to comply with certain requirements, such as posting clear consumer privacy rights policies on their websites. Civ. Code §1798.130(a)(5).

Illinois' Biometric Information Privacy Act

Illinois' Biometric Information Privacy Act (BIPA) was enacted in 2008 to address the booming biometrics industry and regulate, *inter alia*, the collection, use, handling, retention, and destruction of biometric data. 740 Ill. Comp. Stat. Ann. 14/99; *see also* 740 Ill. Comp. Stat. Ann.14/5(g).

BIPA governs "biometric information"—which includes, in pertinent part "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual"—and "biometric identifiers"—which includes, in pertinent part, "a retina or iris scan, fingerprint, voiceprint or scan of hand or face geometry." 740 Ill. Comp. Stat. Ann. 14/10. Further, BIPA imposes restrictions on an entity's retention of an individual's biometric identifiers and information and how it has to be destroyed after it is no longer retained. BIPA's focus on appeasing consumer concerns by requiring entities to establish clear written policies, obtain consent before use, and provide consumers with proper notice is in line with the guiding principles of the GDPR.

BIPA receives great attention because it is the first state law to afford aggrieved individuals with the ability to commence a private right of action sounding in a statutory violation. 740 Ill. Comp. Stat. Ann. 14/20. Pursuant to Section 20 of BIPA, if a private entity negligently, or intentionally or recklessly, violates a provision of BIPA, then the aggrieved individuals are entitled to liquidated damages of $1,000 or $5,000, respectively, or actual damages, whichever is greater. Regardless of whether the private entity negligently or recklessly violates BIPA, aggrieved individuals may recover "reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and other relief, including an injunction, as the State or federal court may deem appropriate." *See id.*

Stop Hacks and Improve Electronic Data Security Act (SHIELD)

New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD) went into effect on March 21, 2020—literally days after the pandemic took hold of the United States. The SHIELD Act presents a prime example of the increased trend towards greater accountability, transparency, and security. *See* 2019 N.Y. Senate Bill No. 5575, N.Y. 242 Leg. Sess. ("Stop Hacks and Improve Electronic Data Security Act") ("SHIELD Act") (amending the General Business Law and the state Technology Law). In particular, it expands the territorial scope of data service requirements to a broader class of people and businesses, broadens New York's data breach notification law to include additional categories of private information, such as biometric data, and expands the definition of "breach of the security system" to include unauthorized "access" of computerized data that compromises the security and integrity of private information. N.Y. Gen. Bus. Law §899-bb. With some exceptions, the SHIELD act affects businesses of all sizes. *See* SHIELD Act, *supra* note 38 (adding "data security protections," pursuant to N.Y. Gen. Bus. L. §899-bb).

The SHIELD act imposes data security requirements, which is representative of where legislation is going. Specifically, the act requires the adoption of reasonable safeguards to ensure private information is kept secure and confidential. In addition, SHIELD requires the implemen-

tation of data security programs, such as risk assessments, employee training, vendor contracts, and data disposal.

Unlike BIPA and CCPA, the SHIELD act does not create a private right of action. Nevertheless, litigation will likely focus on whether a firm's adherence to duties and obligations is reasonable. As litigation ensues in the cyber sector, we expect this standard will be further defined.

Moreover, there are currently several bills before the New York State Assembly and Senate, which purport to create great safeguards regarding internet advertising, disclosure of PII by businesses, and greater scrutiny for business that are data collectors. *See generally* 2021 NY Senate-Assembly Bills A680, S567, A3709, S2886, A405, A400, S1349. For the most part, these bills do not create private rights of action for citizens in the event of noncompliance by a business, which results in a data breach—but legislation in trending in that direction.

Litigation Trends in the United States

The world of data privacy and cybersecurity is complex and confusing—there is limited precedent interpreting state laws, no federal legislation to standardize data protection, and too many acronyms to keep straight. But litigation is still in its infancy. The reality is state and federal courts are only just now beginning to provide guidance on procedural and substantive issues relating to this field, such as with standing and class action certification. There is even less guidance on legal issues relating to liability, and virtually no legal precedent to rely upon with regard to sustainable damages.

Any party commencing litigation in federal court must have Article III standing regardless of the alleged state law violation. To establish standing under Article III, a plaintiff must demonstrate (1) an injury-in-fact; (2) causation; and (3) a likelihood that the injury will be redressed by a favorable decision. If a lawsuit asserting data privacy violations is filed against a law firm, its first line of defense will be to argue the plaintiff lacks standing. As such, based on a survey of federal litigation, we can expect to see the federal court providing guidance on whether standing is established.

By way of example, a few months ago, the Second Circuit issued a ruling that provides Article III standing based on an "increased risk" of identity theft arising from a data breach. *See McMorris v. Carlos Lopez & Assocs., LLC*, ___ F.3d ___ , 2021 WL 1603808 (2d Cir. Apr. 26, 2021). In *McMorris v. Carlos Lopez & Assocs., LLC*, the plaintiff-appellant Devonne McMorris commenced a class action lawsuit against defendant-appellees Carlos Lopez & Associates, LLC (CLA) in response to an email that a CLA employee inadvertently sent to all of CLA's employees. This email contained the sensitive PII—*i.e.*, Social Security numbers, home addresses, dates of birth, phone numbers, dates of hire, and educational degrees—of about 130 former and current CLA workers, including McMorris. After discovering the breach, CLA emailed its current employees, but failed to notify former employees about the inadvertent disclosure or take any other corrective action.

The plaintiffs asserted state law claims of negligence, negligence per se, as well as statutory consumer protection violations on behalf of classes in California, Florida, Texas, Maine, New Jersey, and New York. The plaintiffs also claimed CLA "breached its duty to protect and safeguard [their] personal information and to take reasonable steps to contain the damage caused where such information was compromised." Due to the PII disclosure, plaintiffs asserted they faced an imminent risk of identity theft and becoming victims of "unknown but certainly impending future crimes." In response to the complaint, CLA moved to dismiss for, *inter alia*, lack of Article III standing. The United States District Court for the Southern District of New York agreed with CLA and dismissed McMorris' claims for lack of subject-matter jurisdiction as McMorris failed to allege an injury-in-fact sufficient to confer Article III standing.

McMorris appealed to the Second Circuit, asserting that the increased risk of identity theft confers Article III standing. The Second Circuit focused on whether the plaintiffs sufficiently alleged concrete, particularized, and actual or imminent injury. The court considered three non-exhaustive factors: (1) whether the data at issue was comprised as a result of a targeted attack intended to obtain the plaintiffs' data; (2) whether the plaintiffs could show some misuse of their compromised data, even if the plaintiffs have not yet experienced theft or fraud; and (3) whether the type of disclosed data subjects plaintiffs to a perpetual risk of identity theft or fraud.

While the Second Circuit recognized the information CLA divulged renders plaintiffs more exposed to future identity theft or fraud, plaintiffs failed to establish "imminent injury." In addition, the Second Circuit determined that the plaintiffs had no standing because they failed to show their PII was subject to a targeted data breach, or that any entity misused their PII.

The SHIELD act imposes data security requirements, which is representative of where legislation is going. Specifically, the act requires the adoption of reasonable safeguards to ensure private information is kept secure and confidential.

This decision is significant. Although the court agreed with the district court's holding that McMorris failed to establish an injury in fact, the court held that Article III injury-in-fact standing only requires proof of a substantial risk of future identity theft or fraud. A substantial risk may be sufficient to establish Article III standing, even if the plaintiff has not been a victim of identity theft or fraud. The Second Circuit's thorough decision gives insight to future litigants regarding the required legal standard in this jurisdiction.

While the federal circuits remain split as to whether an increased risk of identity theft following a data breach, without proof of actual harm, is sufficient to confer Article III standing, this decision opens the door for lawsuits and seemingly requires defendants to engage in litigation even if no liability is ultimately

found. Essentially, while it is important to be aware of current litigation trends, firms must understand the potential exposure they face by enacted and pending legislation.

Guidance from the Bar

In 2018, the American Bar Association (ABA) issued a formal opinion explaining lawyers' ethical responsibility to use reasonable efforts when using the internet to send or discuss confidential client information. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Securing Communication of Protected Client Information"). "As custodians of highly sensitive information" the ABA explained that data breaches and cyber threats are "a major professional responsibility and liability threat facing the legal profession." ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018) ("Lawyers' Obligations After an Electronic Data Breach or Cyberattack"). Significantly, the ABA stressed, depending on the context of the cyber incident, an attorney's compliance with state data breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not automatically establish compliance with ethics obligations. *See id.* The ABA formal opinions discussing attorney ethical obligations in the context of data privacy and cybersecurity stress the importance of making *reasonable* efforts to prevent and respond to data incidents.

Depending on the context of the cyber incident, an attorney's compliance with state data breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not automatically establish compliance with ethics obligations.

Federal Law Predictions

The COVID-19 pandemic exposed the inadequate cybersecurity and data privacy laws in the U.S. Now, with the new administration in office and the lifting of COVID-19 restrictions, the federal government is shifting its focus to data privacy. As a result, for the following reasons, comprehensive federal legislation and further guidance is on the horizon.

First, the Biden Administration appreciates the risks posed by the lack of federal legislation and supports the establishment of clear standards for data privacy protection, which is evident by Biden's recent enactment of two Executive Orders. Jedidiah Bracy, **What could a Biden administration mean for privacy, cybersecurity**, November 9, 2020. On May 12, 2021, Biden **issued an Executive Order on Improving the Nation's Cybersecurity**, which directs the private sector to "adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace." In doing so, the Executive Order provides a guide to the private sector for modernization of cybersecurity practices. Kristin Bryan, ***What Businesses Can Learn From Biden Cybersecurity Order***, May 28, 2021. Recently, on June 9, 2021, Biden issued an Executive Order designed to improve the nation's cybersecurity. Biden's Executive Orders appear to reflect the need for the government to work with stakeholders and the private sector. This is significant as stakeholders are urging Congress to establish federal privacy legislation.

Second, under the Biden Administration, we may see federal enforcement and government agencies, such as the SEC and FTC, taking a more active role in enforcement efforts. By way of illustration, on June 15, 2021 Lina Kahn ("Khan") was appointed as the new chair of the FTC. Jon Swartz, ***New FTC chair Lina Khan is Big Tech's biggest nightmare,*** June 22, 2021. This appointment is significant as it is predicted Khan, who once "likened widespread data collection to environmental pollution," will work to establish the FTC as "one of the country's chief privacy enforcers." Issie Lapowsky, ***More bad news for Big Tech: Lina Khan's a privacy hawk, too***, June 21, 2021. It is also possible the FTC will use its rulemaking powers to implement data privacy guidance and legislation. If the FTC implements privacy regulation, it may seek to provide consumer transparency and establish business accountability while seeking to maintain a balance between competition and consumer protection. FTC Rulemaking: A Solution for Federal Privacy Regulation?, International Association of Privacy Professionals, June 23, 2021. In addition, on June 15, 2021, the **SEC announced** that it settled charges against a real estate settlement services company for disclosure controls and procedural violations related to a cybersecurity vulnerability that exposed over 800 million images, including images containing the social security numbers and financial information of individuals. Most recently, on June 17, 2021, Senator Kirsten Gillibrand **reintroduced legislation**, the Data Protection Agency Act of 2021, which is designed to create a Data Protection Agency, "an independent federal agency that would protect Americans' data, safeguard their privacy, and ensure data practices are fair and transparent." Significantly, under this proposal, the DPA will have authority and resources to enforce data protection rules through, *inter alia*, civil penalties and injunctive relief. *See id.* If enacted, this will require firms to be cognizant of another set of rules and regulations.

Third, there is a trend of increased support among members of Congress for the enactment of a federal privacy law that directly addresses data privacy protections and cybersecurity. Arguably the most comprehensive federal bill proposed to date, this past September, legislators introduced the "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act" (also known as the "Safe Data Act") bill to the Senate. S. 4626, 116th Cong. 2d (2020) ("Safe Data Act"). Significantly, the purpose of the Safe Data Act is "[t]o establish data privacy and data security protections for consumers in the United States." See id. The Safe Data Act is broad and comprehensive as it combines three prior legislative proposals—the U.S. Consumer Data Protection Act, Filter Bubble Transparency Act, and Deceptive Expe-

riences to Online Users Reduction Act. Müge Fazlioglu, ***Consolidating US privacy legislation: The SAFE DATA Act***, September 21, 2020.

Significantly, the Safe Data Act focuses on establishing baseline protections by providing consumers with more choice and control over their data, directing businesses to be more transparent about their data policies and practices and establishing uniform data protections across the country to be enforced by state attorneys and the Federal Trade Commission (FTC). In addition, the Safe Data Act provides the FTC with authority, *inter alia*, to develop new rules to expand categories of sensitive data and maintain a data broker registry. It also seeks to restore the FTC's authority to obtain monetary remedies for consumers.

The bill is currently with the Senate Committee on Commerce, Science and Transportation, which held a hearing on September 23, 2020 titled "**Revisiting the Need for Federal Data Privacy Legislation**." Significantly, the purpose of the hearing was to "examine the current state of consumer data privacy and legislative efforts to provide baseline data protections for all Americans" and "examine lessons learned from the implementation of state privacy laws in the U.S. and the E.U. General Data Protection Regulation. Hearings, Revisiting the Need for Federal Privacy Legislation, September 23, 2020.

The committee must evaluate and explore issues such as whether the Safe Data Act should preempt state laws or whether individuals should be granted a private right of action to seek redress. Cameron F. Kerry, et al., **Bridging the gaps: A path forward to federal privacy legislation**, Jun 3, 2020. These two issues are arguably the most contested and polarizing issues and it will be interesting to see how the committee discussions play out. The state laws complicate the preemption debate and expose significant implications to establishing a federal law as they do not all provide a private right of action and contain different purposes, definitions and standards. Therefore, to understand where the U.S. is headed, it is important to appreciate the significance of the GDPR and state laws as they provide the framework for federal legislations in addition to a potential for firms to face liability.

What Does This All Mean for Law Firms?

We like to think that, as attorneys, we are educated professionals, seeking to enhance the jurisprudence in our respective fields. And while this is partly true, in a more realistic sense, we are vendors, in the client service industry. And like any business that collects, or merely engages with PII, law firms must be cognizant of the various laws regulating data collection and possession and appreciate the potential for the enactment of a federal law addressing data privacy and protection. Responding to a cyber incident is costly—particularly if the firm has not implemented any cybersecurity and data privacy policies. For example, a firm is likely to incur costs associated with notifying law enforcement and clients about the breach. In addition, there may be unknown and unquantifiable costs associated with the unauthorized access to sensitive client and nonclient data, as well as costs associated with retaining consultants for necessary repairs, loss of billable time, and web and email access. Not to mention the monetary damages flowing from a cyber incident or the potential violations of the Professional Rules of Conduct.

Will taking these safeguards, as a law firm, prevent a breach from ever occurring? Of course not. Breaches will happen, but when they do, the law firms and other businesses with a proper safeguard in place will be less exposed to an eventual claimant. Think of a business owner that is legally responsible for the sidewalk in front of his or her store—will shoveling snow and removing ice prevent any possibility of a slip-and-fall? No, it will not. Accidents happen, as do breaches. But having a protocol for when it snows serves to demonstrate reasonable safeguards by the property owner. Having a *written* policy for data collection and cyber-incident response, similarly, constitutes reasonable safeguards on the part of a business owner.

With the increased use of cloud technologies and reliance on remote work along with the developing legal precedent and legislation, the risk of facing liability and violating a state privacy law or consumer protection act, GDPR provision, or even the Rules of Professional Conduct is at an all-time high. Unfortunately, there is no foolproof plan to cover every potential issue. However, to limit any potential liability and exposure, there are some "best practices" firms (and even their clients) should follow that focus on transparency, oversight, and accountability. Working to enact the following practices will help law firms to defend against any liability and ensure reasonable efforts are taken to secure and safeguard PII.

- First, firms should determine their legal obligations to develop proper compliance and employee-training programs.
- Second, firms should develop written policies that, *inter alia*, identify the type of data collected, explain how the data is used and stored, and delineate retention and destruction protocols. Further, to the extent legally permissible, these policies should grant clients the right to request the deletion of their information and be readily and easily accessible to clients.
- Third, before obtaining any PII, firms should provide clear notice of their privacy policies to educate consumers and ensure corporate accountability. In addition, firms should obtain written consent from clients.
- Fourth, firms should establish and publish protocols explaining how an individual may request information about the type of data collected or how to request the deletion of his or her information.
- Fifth, firms should detail their data protection procedures in all their contracts, including those with customers, employees and vendors.
- Finally, firms should review their applicable insurance policies to confirm whether they are adequately covered for any data protection and security risks, as any legal actions may create defense and indemnity issues.

The implementation of these safeguards will not prevent all breaches or cyber incidents—but they will certainly curtail the "panic" that sets in once a breach does take place. Whether we are law firm owners, business owners, vendors, clients, or insurers, we all have one thing in common—we do not like surprises, especially in the cybersecurity sense. Being prepared and having these safeguards in place mitigates against surprises—for lawyers and our clients.