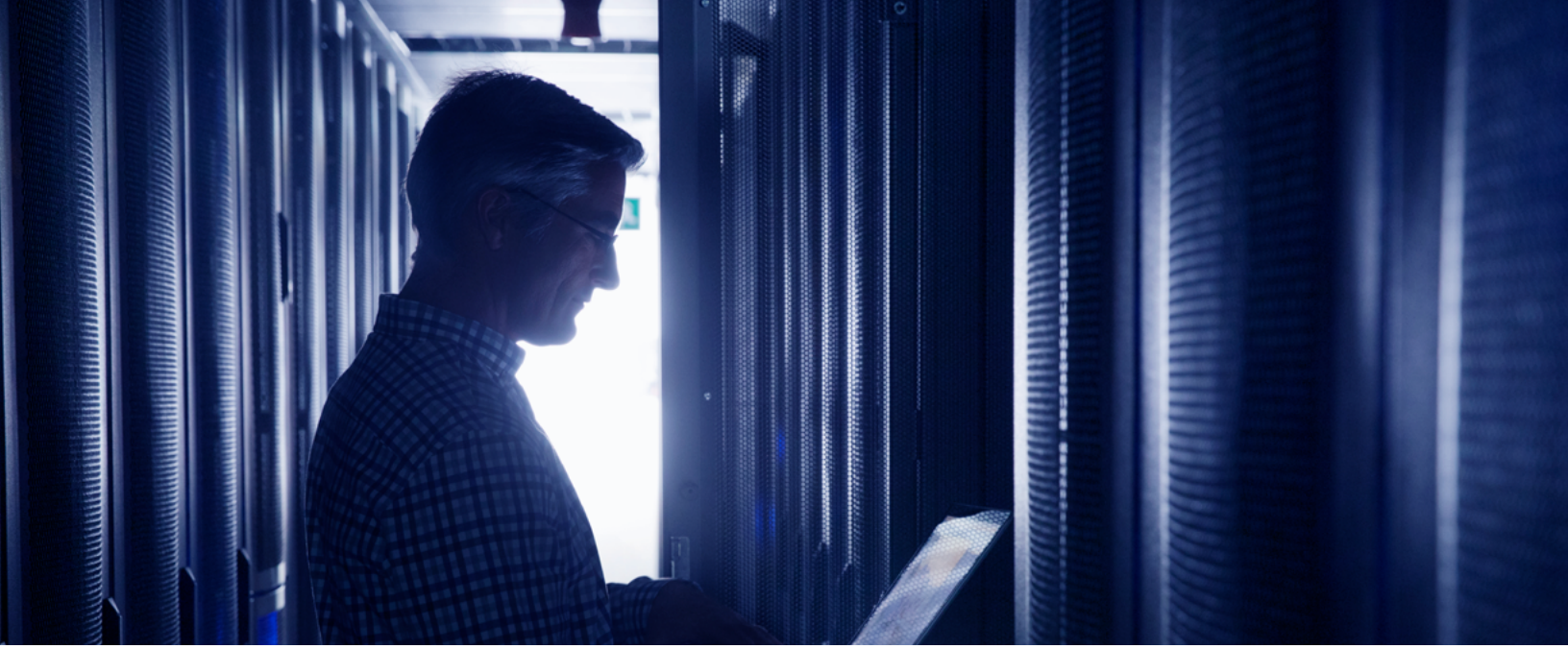
Understanding privacy regulations and their impact on US entities

Amy A. Pines, JD, RPLU, CPLP
Senior Cyber Underwriter

NOT IF, BUT HOW

Munich RE

Understanding privacy regulations and their impact on US entities



Introduction

Within the cyber insurance industry, 2019 marked the start of a period of significant ransomware attacks. An accompanying surge in frequency and severity of claims resulted. Likewise, the depth and complexity of the ransomware attacks graduated from a lockdown of systems with a modest payment demand to double and even triple exfiltration and soaring ransom demands.

With all of the attention devoted to this threat vector, it is important not to lose sight of other causes of claims that can impact insureds and insurers. One such area is privacy regulation. In 2021, significant legislation was updated, passed, and/or proposed. The potential of claims arising from noncompliance with these regulations cannot be ignored.

Privacy regulation in the United States

Historical background

The early 1970s marked the period of the first attempts at regulating and protecting data privacy in the US.

The *Fair Credit Reporting Act of 1970* was the first law enacted to protect an individual's financial data. It is specific to credit bureaus (rating agencies) and promotes the accuracy, fairness, and privacy of information in the files of the credit bureaus by protecting the information and limiting access to and retention of the data.

In 1974, Congress passed an amendment to Title 5 of the US Code, the *United States Privacy Act*, as amended (the "*Privacy Act*").[1] The *Privacy Act* established a code that governs the collection, maintenance, use, and dissemination of information specific to individuals that is maintained in systems of records by federal government agencies. It also guarantees individuals full access to these records, as it pertains to their personal information.

Thereafter, a number of other significant laws and regulations that directly and indirectly addressed data protection were passed, including, but not limited to, the *Health Insurance Portability and Accountability Act ("HIPAA")*[2] in 1996 (related to the healthcare industry), the *Children's Online Privacy Protection Act ("COPA")*[3], in 1998 (related to personal information of minors), the *Gramm-Leach-Bliley Act ("GLBA")*[4] in 1999 (related to banking and finance), and the *USA Freedom Act of 2015*[5] (enacted to restore portions of the *USA Patriot Act* and specific to the collection of telecommunication metadata of US citizens by American intelligence agencies).

However, no comprehensive federal privacy law has been approved in the US to date. This void has led individual states to enact their own data privacy laws, most notably, California. Other states, such as Illinois, have endeavored to extend protections to individual's biometric data. New York introduced regulations on data specific to the financial services industry. These states have set the foundation for legislation and serve as an example for other states across the country.

Consumer data privacy regulation

California is at the forefront of data privacy and regulation. It has enacted two different acts to this end. The *California Consumer Privacy Act ("CCPA")* was signed into law in 2018. The *CCPA* outlines the standards for data collection, consequences for businesses that do not properly protect use data, and the rights that California consumers can exercise over their data. It applies to businesses (as more specifically defined in the act) that collect data from California residents, regardless of the location of the headquarters of the business itself. California consumers are guaranteed the right to access specified consumer information held by businesses and are also given a right to correct and delete (with exceptions) the information on request. The definition of the personal information in the act is broad: "...information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The *CCPA* also contains an extensive listing of identifiers that it considers to be personal information – including biometric, geolocation, email, browsing history, employee data, and more. There is also an ongoing requirement of risk assessment and cyber security audit. The *CCPA* provides for statutory damages and both a limited private right of action and more general enforcement by the California Attorney General. There is also a grace period – meaning businesses are given 30 days to cure alleged violations before any administrative enforcement by the California Attorney General.

Over 125 cases asserting *CCPA* claims were filed in 2021.[6] Nearly 40% of the *CCPA* cases filed that year either concerned the 2021 T-Mobile data breach or alternatively, another data event involving a financial services company following account hacks on the California Employment Development Department's prepaid debit cards.[7] As such, the largest number of cases filed in 2021 were concentrated in the communications and financial services industries.[8] The remaining cases, however, span a wide range of industries – including technology, healthcare, insurance, and hospitality.[9] To date, no significant judgments or settlements have been entered or reported. However, there are a number of cases pending at present.

The *California Privacy Rights Act ("CPRA")*, legislation which bolsters the *CCPA* and gives California citizens more data privacy rights, was passed in late 2020 and has an effective date of January 1, 2023 and an enforcement date of July 1, 2023, and a look-back period beginning January 1, 2022 – meaning that data collected from this date forward will be subject to the requirements of the *CPRA*. Additional rights of California consumers include: the right to restrict how their sensitive data is used and disclosed, the right to request that incorrect information be corrected promptly, and the right to opt-out of their data being sold by businesses to advertisers for compensation. It also established a new governmental agency, the *California Privacy Protection Agency ("CPPA")*, tasked with enforcement and supervision of the *CPRA* and *CCPA*. It will oblige subject businesses[10] to improve opt-in and consent processes on their websites, email communications, and other digital channels, and will further require that they have more robust internal practices for responding to data

privacy-related requests from consumers. On one hand, the definition of business is more narrow than that of the *CCPA* to exclude smaller businesses. But on the other hand, the 30-day correction period has been eliminated, the definition of sensitive personal information was expanded, and "contractors" or vendors (businesses that buy and use information) now fall under the purview of the law.

Since the *CPRA* has not reached the enforcement date, there are no enforcement actions to review, but based on the expanded definition of personal information, there is a corresponding expansion of the scope of the right of private action which can, in turn, increase the potential for class action litigation. By way of example, the disclosure of an email along with the password/security question would trigger a breach under the *CPRA*. This is information that is often readily available on the dark web. Coupled with the potential statutory damages of up to $750 per consumer per incident, a potential claim could be incredibly financially consequential.

Both Colorado and Virginia signed into effect consumer data privacy laws in 2021 and a number of other states have pending legislation (including, but not limited to, New York, Massachusetts, Hawaii, Maryland, and North Dakota).

Biometric privacy regulation

The *Illinois Biometric Information Privacy Act ("BIPA")* was the first comprehensive biometric privacy law passed in the US in 2008. It regulates the collection, storage, retention, safeguarding, use, sharing, and destruction of biometric information and biometric identifiers[11] by private companies (with certain exceptions and exclusions). A business must comply with *BIPA* if it collects any biometric information from a resident of Illinois. Compliance means requesting and receiving informed, written consent from each data subject. It also means agreeing not to sell or lease any of the data for profit. There are also specific restrictions on disclosure of the data and security requirements for the companies in possession of the data. But the most unique and potentially significant aspect of *BIPA* is that it includes a private right of action for aggrieved individuals to recover for each violation, with no requirement for actual damage as follows: (1) liquidated damages of $1,000 or actual damages, whichever amount is greater, for negligent violations; or (2) liquidated damages of $5,000 or actual damages, whichever amount is greater, for intentional or reckless violations. Plaintiffs are also entitled to recover reasonable attorney fees and related court costs, including expert witness fees and other litigation expenses.

BIPA litigation is also noteworthy because it is the result of the first stand-alone biometric regulation in the US and, as mentioned earlier, provides the broadest private right of action for plaintiffs. And, due in part to the private right of action, case volume is significant and continues to increase. In 2021, at least 89 court rulings referenced *BIPA* – a 400% increase from 2019.[12]

Perhaps the most well-known case involving *BIPA* is *Rosenbach v. Six Flags Entertainment Corp.*,[13] which held that a consumer need not demonstrate an adverse effect or specific harm to have standing to sue under *BIPA*. Instead, bare procedural violations of the statute are sufficient to establish standing. This ruling was at odds with the way in which many privacy laws are written and enforced around the country – namely, because plaintiffs have to prove that they sustained some form of damage or harm in relation to the illegal disclosure of their personal information. However, this ruling was limited to standing in an Illinois state court. So, there may be a higher threshold to establish standing in federal court. "*See TransUnion, LLC v. Ramirez*, 141 S. Ct. 2190 (2021)", which held that only a plaintiff concretely harmed by a defendant's violation of the *Fair Credit Reporting Act ("FCRA")* has Article III standing to seek damages.[14] While TransUnion was specific to the *FCRA*, it may have implications for *BIPA*.[15] Future case law will settle this issue.

Equally compelling are the settlements recorded to date under *BIPA*. In 2021, a California federal court judge gave final approval of a settlement in a class action lawsuit against Facebook. Under the terms of the settlement, Facebook agreed to pay $650 million to 1.6 million Illinois residents for violations of *BIPA* (specifically related to the use of unauthorized facial tagging). Also in 2021, a federal court in Illinois granted preliminary approval of a $92 million settlement reached in the TikTok multi-district litigation, the Six Flags litigation referenced above received preliminary approval of a $36 million settlement, an Illinois state court judge approved a $25 million class action settlement between ADP and its employees, and Walmart reached a $10 million settlement with current and former employees – all based on *BIPA* violations.

Similar legislation goes back to 2009 when Texas enacted the *Capture or Use Biometric Identifier Act* (the *"Texas Act"*), which is most greatly distinguished from *BIPA* by the fact it has no private right of action. Instead, it is within the discretion of the Attorney General of Texas to pursue any violations.

In 2017, Washington became the third state to enact a specific biometric privacy legislation, the *Washington Biometric Privacy Act*. It does not require notice or consent, and in some circumstances, contains a broad security exception exempting entities collecting biometric information for "security purposes." Like the *Texas Act*, it provides no private right of action.

More recently, in 2021, both New York and Colorado passed biometric-specific laws, but each is less stringent than *BIPA*. A number of other states, such as Arkansas, have more broad privacy statues that regulate biometric data by including it in the statutory definition of personal information.

Maine, Maryland, Massachusetts, Missouri, Kentucky, New York, and West Virginia all have some form of a proposed biometric regulation bill pending. In February 2022, California introduced a bill to expand the protections of the *California Privacy Rights Act* to also include biometric information.

Also in February 2022, the Illinois Supreme Court made a much anticipated decision in the matter of *McDonald v. Symphony Bronzeville Park, LLC*.[16] The Court held that the *Illinois Workers' Compensation Act ("IWCA")* does not preempt claims under *BIPA*. This decision eliminated a technique frequently used by employers to defend against *BIPA* claims (essentially asserting that the *IWCA* was an exclusive remedy for work-related "injuries"). The Court held that a *BIPA* violation and the resultant claim for liquidated damages are clearly distinguished from the actual physical injuries that are covered by the *IWCA*. A claim against an employer for an alleged violation of *BIPA* would not be covered by *IWCA* and cannot be preempted by *IWCA*.

There are also several pending cases that will have an impact on the course of future *BIPA* litigation. For example, *Cothron v. White Castle*,[17] in which the Court will make a determination on claim accrual – specifically, whether a claim accrues each time an entity collects or discloses biometric information or only the first time. The determination of the accrual issue will also set the tolling period for the statute of limitations. The decision will have a significant impact on potential damages under *BIPA*.

Also of interest, two class action lawsuits were filed early in 2022 related to *BIPA* violations in companies offering dashcam telematics. These cases are both pending, but are a warning signal to any company operating in the same space to ensure compliance with *BIPA* – including obtaining informed consent prior to collection – and demonstrate the far reach of *BIPA*.

Financial services industry regulation

The New York State Department of Financial Services (the "NYDFS") promulgated a regulation establishing cybersecurity requirements for financial services companies. The *NYDFS Cybersecurity Regulations ("NYDFS Regs")* were effective on March 1, 2017. The *NYDFS Regs* are "designed to promote the protection of consumer information as well as the information technology systems of regulated entities."[18] They apply to any individual or entity that is operating under a license, charter, or similar authorization by the NYDFS. Such entities include banks, insurance companies, and other financial services companies. *NYDFS Regs* §500.11 addresses third-party service providers. This is one of the first examples of a system of state-wide cybersecurity standards specific to a particular industry. Under the terms of the regulation, covered entities must develop a comprehensive written cybersecurity policy that aligns with industry best practices and ISO 27001 standards. The policy must address specific areas, including information security, data governance, and classification, a business continuity and disaster recovery plan, systems operations and availability concerns, network security, consumer data privacy, risk assessment, and related topics. It must include a proposed plan of response to a potential cyber event and further requires data breach notification within 72 hours. Further requirements include: designation of a chief information security officer to maintain policies and procedures, conducting annual penetration testing and biannual vulnerability assessments, maintaining an audit trail of material financial transactions, limiting and reviewing access privileges, utilizing multi-factor authentication for any person accessing the internal or external network, and generally maintaining the confidentiality of non-public information. Finally, pursuant to §500.11, covered entities must certify that third-party vendors with which they do business have adequate cybersecurity programs in effect – essentially requiring that vendors who do business with covered entities will be compliant with the same cybersecurity standards.

By way of example of an enforcement action, in 2021, the NYDFS issued a $3 million fine to National Securities Corporation for violations against the *NYDFS Regs*.[19] National Securities Corporation was the victim of four different cybersecurity incidents between 2018 and 2020. The incidents involved unauthorized access to employee email accounts – one of which resulted in an unauthorized transfer of funds from customers. Not only did National Securities fail to report two of the incidents within the 72-hour notice time frame, the company also provided a certificate of compliance that contained false representations – including the implementation of security controls such as multi-factor authentication – that were deemed to have been directly related to the breaches at hand.

Similarly, a $1.8 million settlement was reached between the NYDFS and First Unum Life Insurance Company of America and Paul Revere Life Insurance Company after customer data was compromised twice by phishing attacks in 2018 and 2019.[20] Not only was the data compromised, upon investigation, the NYDFS determined that each company falsely certified to compliance with the requirements of the *NYDFS Regs*, despite knowing they had not implemented basic controls such as multi-factor authentication.

But regulation of the US banking system is not limited to state-based legislation. By way of example, in November 2021, a joint press release was issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency announcing a rule to "improve the sharing of information about cyber incidents that may affect the US banking system."[21] The rule requires a banking organization to notify its primary federal regulator of any significant security incident as soon as possible and no later than 36 hours after the banking organization determines that a cyber incident has occurred.[22] Notification is required for incidents that have materially affected – or are reasonably likely to materially affect – the viability of a banking organization's operations, its ability to deliver banking products and services, or the stability of the financial sector.[23] There is also a related provision applicable to bank service providers with notification requirements for customers of a banking organization in the event of the service provider's breach. The rules went into effect in April 2022, with full compliance required by May 1, 2022.

The 36-hour notification requirement provided for in the rule is the shortest time frame of any law to date, including that provided for in the *NYDFS Regs*. The rule is illustrative of the complexities that arise in achieving regulatory compliance when multiple regulations apply with different standards for compliance. It also exemplifies the widely held sentiment that greater information sharing and coordination and collaboration amongst the government, law enforcement, and the private sector is necessary to avoid or mitigate cyber-attacks.

International regulations

General Data Protection Regulation

The *General Data Protection Regulation ("GDPR")* is the framework set by the European Union (EU) for the protection and privacy of data. *GDPR* created a single privacy law across the EU and it quickly became the global standard for privacy regulation. It sets mandatory rules for how organizations and companies process data (processing includes collecting, storing, sharing, destroying, etc). It became effective in 2018, but was most recently updated in 2021 to effectuate changes intended to further enhance the effectiveness of the law, including the removal of the privacy shield.[24] Now, US companies are obliged to adopt the standard *GDPR* terms related to the use of the customer data of European citizens. Violations of the *GDPR* can result in stiff penalties – up to 4% of a company's worldwide annual revenue.

To date, over 800 fines have been issued, with a resultant value of more than €1 billion. Two of the largest include a €746 million fine brought by a French privacy rights group against Amazon for violations related to an advertising targeting system that was carried out without proper consent. A second example is a €225 million fine against WhatsApp issued by the Irish Data Protection Commission under the *GDPR* for violations of the transparency obligations under the law (specific to non-users of the app, whose data was captured by WhatsApp).

Violations of the *GDPR* can result in stiff penalties – up to **4%** of a company's worldwide annual revenue.

GDPR is, perhaps, the most well-known international privacy regulation. But international regulation and enforcement is not limited to the *GDPR*. The *GDPR* brought data protection into consideration for countries around the world and served as a model for many of them. To date, legislation to protect data and privacy has been enacted in more than 120 different countries.[25]

Canada's Personal Information Protection and Electronic Documents Act

Canada has two federal privacy laws: the *Privacy Act* (enacted in 1983), that regulates how the federal government handles personal information, and The *Personal Information Protection and Electronic Documents Act ("PIPEDA")*, enacted in 2000, that regulates how private businesses handle personal information. The *Privacy Act* is specific to Canadian citizens' right to access and correct personal information that the government holds. *PIPEDA* applies to the collection, use, and disclosure of personal information in the private sector.[26] Compared to the *GDPR*, and even to the *CCPA*, *PIPEDA* is relatively limited in scope. It does not apply in a number of instances, such as: when the *Privacy Act* applies, to provincial and territorial governments that have their own privacy laws, to not-for-profit entities, when personal information is processed for literary, artistic, or journalistic purposes, etc. Pursuant to *PIPEDA*, companies need to adhere to 10 general information principles to protect personal information: accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access, and challenging compliance. Compliance with *PIPEDA* is evaluated against the standard of "reasonableness," allowing companies to collect, use, and disclose personal information for purposes that a "reasonable person would consider appropriate in the

circumstances."[27] This requirement applies even if the individual consented to the collection use or disclosure of their personal information. *PIPEDA* does not specify extraterritorial application, however, Canadian federal courts stipulated to jurisdiction to make an extraterritorial order with world-wide effects against a foreign resident.[28]

Of note, in addition to the federal laws in Canada, there are several other federal laws specific to certain industries, such as banking, as well as provincial sector-specific laws that include data privacy provisions, generally and specific to certain industries.

Also of note, in November 2000, a new bill was introduced that would substantially overhaul *PIPEDA* and replace it with new legislation. Due to procedural issues, the bill did not pass, but a second introduction of the bill titled *Digital Charter Implementation Act* is expected in early 2022.

China's data security law and personal information protection law

In the fall of 2021, two new laws were passed by the Standing Committee of the National People's Congress of the People's Republic of China PRC. The *Data Security Law ("DSL")* was passed on June 10, 2021 and came into effect on September 1, 2021. The *Personal Information Protection Law ("PIPL")* came into effect on November 1, 2021. The *DSL* and *PIPL* work together with the *Cybersecurity Law*, China's first set of cybersecurity regulations, to establish a more comprehensive framework for governing cybersecurity and data privacy protection in China. These two new laws potentially impact all business operating in China – including multinational corporations – and corporations operating outside of China that collect or handle data subject to the regulations. The consequences of non-compliance with the laws is significant, including fines of up to 5% of a company's revenue for the past year and/or revocation of the company's license to do business in China and/or personal liability for company executives.

Underwriting implications

In light of all of the regulatory additions and revisions, both in the US and within the global landscape, there is undoubtedly a heightened risk of cyber claim activity for any commercial insured due to non-compliance with applicable regulations.

With this in mind, it is crucial that cyber liability underwriters conduct the appropriate due diligence in their underwriting process to assess the extent to which their insured is subject to the various regulations and, consequentially, whether an insured is aware of, compliant with, and monitoring such regulations, so as to mitigate the risk of a potential claim.

With respect to biometric data and *BIPA*, specifically, but all other regulations and data, generally, insureds must have a clear understanding of what data they collect, where it comes from, and to whom it belongs. They also need to understand where and how it is both stored, processed, sold, and destroyed. The type and source of data will, in large part, determine to which privacy laws a business is subject. Data mapping is essential, but knowing and understanding the data is just step one. After, insureds must evaluate which specific laws apply to them, and with multi-state or national corporations, it is likely not just a single law. Once an insured determines which laws apply, it must take steps to achieve compliance with each individual law, as not all requirements and standards are the same. Compliance can include anything from IT testing to appointing CISOs to obtaining consent and providing notice in the event of a breach, to name a few.

Insureds must also maintain awareness of investigations and resulting fines and penalties that are levied under particular laws to better understand how they evolve in light of their enforcement. By way of example, *CPRA* can be analyzed on paper, but once it is actually enforced, a great deal more about the act will likely be understood.

Insureds should also remain aware of any changes in the regulations, such as the 2021 *GDPR* revisions, that added additional obligations for US-based companies. Changes in legal interpretations of the various regulations could change the scope, intent, and/or standards for compliance, so vigilant awareness is necessary.

Insureds must also exercise caution when engaging in marketing activities that use prospective/customers' personal information.

From an underwriting standpoint, insureds should have a strong awareness of the urgency and gravity of regulatory compliance. The above-mentioned steps can be arduous, and targets are constantly being added and changed. There is an ongoing requirement of risk assessment and cyber security audit in the face of the regulations. Compliance demands vigilance. Fines and penalties will likely increase in number and potentially in amount over time.

Best practices for insureds

There are a number of steps that insureds can take to mitigate the risk of breach and/or regulatory non-compliance.

Know your data – It would be impossible to underscore the gravity of this best practice. Knowing your data includes knowing the source, type, and use of data and whether permission was sought/obtained for collection and/or storage, and/or sale. Also of importance is knowing where the data is

stored, how the data is used, and with whom data is shared/to whom data is sold. And finally, insureds should have in place appropriate data retention policies.

Determine applicable regulatory requirements – Be it through an internal team, outside counsel, or a niche vendor, insureds must assess which regulatory requirements apply and what steps must be taken to achieve compliance: obtaining consents, updating privacy notices, storing and protecting data appropriately, etc.

Implement and maintain an appropriate cyber security posture – The *CCPA* requires companies to have "reasonable" cyber security measures in place, the *NYDFS Regs* require cyber security policies that align with ISO 27001 standards. While there is no common standard or set of guidelines throughout each of the regulations, it is generally reasonable to believe that a more robust program will decrease the likelihood of a potential attack and will be looked upon favorably by regulatory bodies.

Be aware of third-party vendor exposure – Whether specific standards are set forth for third party vendors/processors such as in the *NYDFS Regs* and *GDPR*, or not, the cyber security posture of an insured's third-party vendors directly impacts each and every insured. Thorough due diligence and vetting should occur prior to engaging a third-party vendor and throughout the course of the contractual period to prevent against vulnerabilities and to ensure regulatory compliance.

Secure suitable cyber insurance – A prudent strategy is two-pronged, involving risk mitigation and risk minimization. Cyber liability insurance can be a worthwhile investment and stop-gap, should the unavoidable occur. Insureds should consider, inter alia, appropriate scope of coverage, terms and conditions, limits and sublimits, and retention. For insurers, reinsurance is an option that also can mitigate risk and reduce financial consequences from both first and third-party losses.

Conclusion

Companies should review, evaluate, and comply with regulations not only in multiple states, but potentially multiple countries, making engaging in daily business activities that much more complicated and adding to the ever-growing and evolving list of cyber threat vectors that impact our industry.

The task of compliance may seem herculean, especially with all of the focus and dedication of resources to ransom attacks. Ignoring regulatory requirements, however, could lead to increased vulnerability of attack and just as bad, resultant fines and penalties.

But the news is not all bad. Some regulations can potentially help businesses. As state attorneys general investigate and enforce compliance under these acts, they could collaborate to a greater degree and even share resources with victims to facilitate a swifter and more effective resolution in the event of a cybercrime. And some provisions of the regulations can lead to a more secure organization and more secure data, in general (e.g., use of multi-factor authentication, data minimization, better processing, and storing more sensitive information), which could in turn, lead to a decrease in cybercrime. Finally, insurers can use the topic as a point for further education and awareness and, ultimately, partnership with insureds.[29]

[1] 5 U.S.C. § 552(a) (1974).
[2] Health Insurance Portability and Accountability Act of 1996, Pul. L. No. 104-191, Stat. 1936.
[3] 15 U.S.C.t § 6502.
[4] 15 U.S.C. § 6801-6809.
[5] H.R. 2048, Pul. L. 114-23.
[6] Rafael M. Langer-Osuna, Marisol C. Mork and Kristin L. Bryan, *2021 Year In Review: CCPA Litigation*, published in The National Law Review, Volume XII, Number 14, January 14, 2022, www.natlawreview.com.
[7] *Id*.
[8] *Id*.
[9] *Id*.
[10] Any company that engages in the data collection, analysis and storage of any person located in California is subject to the CPRA if they meet the following criteria: for-profit companies that do business in California, greater than $25 million in annual revenue, buy, sell, or share personal information of over 100,000 consumers or households, or derive at least 50% of annual revenue from selling or sharing of consumer personal information.
[11] "Biometric information" means any information based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of "biometric identifier." "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, scan of the hand or face geometry, palm veins, odor, or scent and ear features. Examples of exclusions to this definition include writing samples, photographs, tattoo descriptions, and information captured in a healthcare setting or under HIPAA, etc. 740 ILCS 14/10.
[12] Kristen L. Bryan, Christina Lamoureux, and Dan Lonergan, *2021 Year In Review: Biometric and AI Litigation*, The National Law Review, Vol. XII, No. 84, Jan. 5, 2022.
[13] *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186.
[14] For additional insight into the decision, see 135 Harv. L. Rev 333, Nov. 10, 2021, https://harvardlawreview.org/2021/11/transunion-v-ramirez/.
[15] Robert Cattanach, Kent Schmidt and Melonie Jordan, No Concrete Harm, No Standing" – Supreme Court's *TransUnion v. Ramirez Decision Clarifies Federal Court Standing Requirements for CCPA and BIPA Class Actions*, (June 20, 2021), https://dorsey.com/newsresources/publications/client-alerts/2021/06/supreme-court-transunion-v-ramirez-decision.
[16] *McDonald v. Symphony Bronzeville Park, LLC,* 2022 IL 126511 (2022).
[17] *Cothron v. White Castle,* 467 F.Supp.3d 60-4 (2020), on appeal.
[18] 23 NYCRR §500, *et seq.*
[19] New York State Department of Financial Services. (April 14, 2020). *DFS Superintendent Lacewell Announces Cybersecurity Settlement With Licensed Insurance Company* (Press release). https://www.dfs.ny.gov/reports_and-Publications/press_releases/pr202104141.
[20] New York State Department of Financial Services. (May 13, 2021). *DFS Superintendent Lacewell Announces Cybersecurity Settlement With First Unum and Paul Revere Life Insurance Companies* (Press release). https://www.dfs.ny.gov/reports_and_ublications/press_releases/pr202105131.
[21] Agencies Approve Final Rule Requiring Computer-Security Incident Notification, November 18, 2021, https://www.federalreserve.gov/newsevents/pressrleases/bcreg20211118a.htm.
[22] *Id.*
[23] *Id.*
[24] The so-called privacy shield was intended to make it easier for data to be transferred from European companies and institutions to their U.S. counterparts.
[25] Amanda Coos, *Data Protection Legislation Around the World in 2021*, Jan. 8, 2021, www.endpointprotector.com/blog/data-protection-legislation-around-the-world/.
[26] "Personal information" is broadly defined as any "information about an identifiable individual" whether public or private, with limited exceptions. Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, Part I, Definitions.
[27] *Id.* at Part I, Purpose.
[28] *A.T. v. Globe24h.com,* 2017 FC 114.
[29] This paper is for informational purposes only and is not intended to be legal, underwriting, financial or any other type of professional advice and the recipient should consult with his/her own counsel or other advisors to determine its applicability to the recipient's particular circumstance.

Printed May 2022