Journal of Banking and Finance Law and Practice
Thomson Reuters

Privacy and Cybersecurity Issues in 2020 – What to Expect

Elizabeth McGinn, Amanda Lawrence and James Chou*

A steady drumbeat of data breaches and growing concern among consumers about how companies are using their personal information will keep regulators, policy-makers and private litigants focused on cybersecurity and privacy in 2020 and beyond. While Congress tentatively explores comprehensive federal privacy legislation, State legislatures across the country are following the European Union's and California's lead, and considering a broad range of initiatives – some incorporating principles similar to the *General Data Protection Regulation* 2016/679 (EU) (*GDPR*) or the *California Consumer Privacy Act of 2018* (*CCPA*), and some that would push well beyond – to protect data. State Attorneys-General are reflecting the concerns of their constituents by ramping up enforcement in these areas. This note examines these initiatives, as well as the major challenges that businesses now face as they attempt to meet regulatory, legislative and consumer expectations for data privacy and protection.

AREAS OF REGULATOR, ATTORNEY-GENERAL AND LEGISLATIVE FOCUS

California Consumer Privacy Act and Similar Privacy Laws

The *CCPA* went into effect at the beginning of 2020 and businesses maintaining information on California residents must now comply with its provisions.[1] In addition to requiring businesses to effectuate new consumer privacy rights – including the right to know, to opt out of sale, to delete and to data portability – the *CCPA* also provides a private right of action for consumers whose personal information (as defined by California data breach law[2]) is compromised due to a failure of a business to implement "reasonable security measures".[3] Although enforcement will not begin until 1 July 2020, the California Attorney-General has indicated that the office has already started to monitor compliance.[4]

Since the *CCPA*'s enactment, similar comprehensive privacy laws have been proposed (and, in some cases, enacted) in other States. For instance, Nevada enacted a privacy law in 2019[5] that, although not nearly as extensive as the *CCPA*, provides opt-out rights for Nevada consumers.

CCPA-like privacy laws are expected to be introduced (or reintroduced) across State legislatures in 2020. For instance, New York introduced the *New York Privacy Act* (*NYPA*) last May, which proposed to establish a fiduciary-like responsibility on businesses that process consumer information and provides a private right of action for violations of the *NYPA*.[6] Given the uncertain prospects for federal standards, business resources are likely to be best utilised by focusing on State and international efforts.

---

* Elizabeth E McGinn: Partner, Buckley LLP. Amanda R Lawrence: Partner, Buckley LLP. James C Chou: Associate, Buckley LLP.

[1] *California Consumer Privacy Act*, Cal Civ Code § 1798.100 et seq (2018).

[2] *California Consumer Privacy Act*, Cal Civ Code § 1798.81.5 (2018).

[3] *California Consumer Privacy Act*, Cal Civ Code § 1798.150(a) (2018).

[4] Alexei Koseff, "California Promises Aggressive Enforcement of New Privacy Law", *San Francisco Chronicle*, 16 December 2019 <https://www.sfchronicle.com/politics/article/California-promises-aggressive-enforcement-of-new-14911017.php>.

[5] *New York Privacy Act*, Nev Rev Stat § 603A.200 et seq (2019).

[6] *New York Privacy Act*, SB 5642 (2019).

Expanding Biometrics

Most States that include biometric data in privacy or data breach laws define biometric data broadly to include any information collected regarding the physical representation, which potentially include such data such as face-prints, particularly when used as an authentication measure.[7]

The Illinois *Biometric Information Privacy Act*[8] (*BIPA*) received renewed attention in 2019 with the Illinois Supreme Court holding in *Rosenbach v Six Flags Entertainment Corp*[9] that a violation of the disclosure provisions of the *BIPA* was a harm to consumers and, therefore, actionable.[10] Since then, a number of class actions have been filed on a theory of a "failure to obtain consent" against retailers such as Home Depot and Loews for the use of facial recognition technology in their retail stores to combat theft.[11]

Other States, such as New York, have proposed similar laws to the Illinois *BIPA*, even as a New York school district becomes one of the first in the United States to implement facial recognition technology.[12] Interestingly, a similar facial recognition program implemented by a school district in the European Union resulted in enforcement by its Data Protection Agency, holding that the *GDPR*, among other things, requires agencies to first conduct an analysis of less intrusive alternatives prior to biometric collection.[13]

Several States have also updated data breach laws to include biometric information, with a few taking effect as of 1 January 2020 or early 2020.

The increased focus on biometrics, including facial recognition technology, will likely continue in the near term as regulatory and social concerns about the sensitivity and use of biometric information persist, particularly as businesses continue leveraging artificial intelligence, cloud and machine-learning technology.

Regulator Examinations Focus on Cybersecurity and Privacy

Over the past year, there have been more requests by State examiners and regulators for documentation regarding the cybersecurity and privacy programs of regulated entities during periodic licensing renewals and examinations. Even State regulators that traditionally have not emphasised privacy and information security have requested written privacy policies such as a Gramm-Leach Bliley internal policy and detailed procedures regarding information security.

---

[7] See, eg, *California Consumer Privacy Act*, Cal Civ Code § 1798.81.5 (effective 1 January 2020) (amending California's data breach law to include "[u]nique biometric data generated from measurements or technical analysis of human body characteristics").

[8] *Biometric Information Privacy Act*, 740 Ill Comp Stat 14/1 et seq (2019).

[9] *Rosenbach v Six Flags Ent Corp*, 129 NE 3d 1197 (Ill 2019).

[10] *Rosenbach v Six Flags Ent Corp*, 129 NE 3d 1207 (Ill 2019).

[11] *Brunson v Home Depot Inc*, 1:19-cv-03970-CC (ND Ga, 12 January 2020).

[12] Michelle T Bradley, "Lockport City School District: January 2020 AEGIS Security System Update" (2020) <https://www.smore.com/utzgy>. Washington has also specifically included facial recognition technology in a proposed biometrics Bill introduced early this year: Daniel R Stoller, "Washington State Privacy Bill Targets Facial Recognition", *Bloomberg Law*, 13 January 2020 <https://news.bloomberglaw.com/privacy-and-data-security/washington-state-privacy-bill-targets-facial-recognition>.

[13] *General Data Protection Regulation* 2016/679 (EU), Art 9; "Facial Recognition: School ID Checks Lead to GDPR Fines", *BBC News*, 27 August 2019 <https://www.bbc.com/news/technology-49489154>.

The New York Department of Financial Services, in particular, has taken steps to ensure that potential applicants are compliant with its cybersecurity regulations, and it is expected that more and more regulators will do so in the coming year. In a major overhaul in the federal contracting space, the Department of Defense (DoD) announced that all federal defense contractors must comply with new cybersecurity certification requirements under the Cybersecurity Maturity Model Certification at one of five levels to continue to provide products or services to the DoD.[14]

Incident Response Planning Will Increasingly Become a Core Cybersecurity Component

While most cybersecurity and privacy frameworks already include incident response as a fundamental component in an information security program, there has been renewed emphasis among State and federal regulatory entities to insist that companies maintain a written incident response plan that is both executable and periodically tested (at least annually), and that covers the compromise of sensitive consumer information.

Last year, the Federal Trade Commission, after considering cybersecurity regulations introduced by the New York Department of Financial Services (NYDFS),[15] proposed new requirements to the Safeguards Rule, which included formalising requirements for incident response planning and mandating a written response plan that outlined: (1) the goals of the plan; (2) the internal processes for incident response; (3) the roles and responsibilities and decision-making authorities during incident response; (4) the plan for internal and external information-sharing; (5) the remediation strategy for identified vulnerabilities in a business' information systems; (6) incident documentation; and (7) procedures for reevaluating and updating the plan.[16]

Businesses, particularly financial institutions and entities maintaining health information, will likely continue to be evaluated, not only on the adequacy of their information security program, but also on the adequacy of their incident response planning and execution. To this end, incident response plans should be routinely reviewed and tested to ensure: (1) they are appropriate with respect to the size and the scope of the business, as well as the sensitivity of the consumer information it maintains; and (2) that the plan meets regulatory guidelines, such as the guidelines established under the *Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information and Consumer Notice*,[17] to the extent applicable.

Geopolitical Tensions May Drive State-Sponsored Cyberattacks

Renewed geopolitical tensions may likely drive state-sponsored cyberattacks on non-military critical infrastructure, such as the United States (US) health, energy and financial sectors.[18] Recently, law-makers on Capitol Hill and in New York urged the financial sector to remain vigilant against cyberattacks.[19] State-sponsored cyberattacks – which include a wide-ranging arsenal of cyber weapons from sophisticated zero-day attacks (or vulnerabilities that have been discovered before a developer is aware of or has an opportunity to release a patch) to conventional malware and spear-phishing methods that utilise already compromised personally identifiable information – can potentially present a nightmare scenario for businesses. Moreover, cyber operations provide state actors with a low-cost, asymmetric and effective way to degrade a country's critical infrastructure.

---

[14] A discussion of the Cybersecurity Maturity Model Certification is available at <https://www.acq.osd.mil/cmmc/>.

[15] NY Comp Codes R & Regs, tit 23 § 500.01 et seq.

[16] 84 Fed Reg 13158, 13160-63, 13169 (4 April 2019).

[17] 12 CFR Pt 30, Appx B, Supp A.

[18] James Rundle, "Threat of Cyberattack By Iran Still Critical, Experts Say", *The Wall Street Journal*, 9 January 2020.

[19] See, eg, New York Department of Financial Services, "Department of Financial Services Issues Alert to Regulated Entities Concerning Heightened Risk of Cyber Attacks" (Press Release, 4 January 2020) <https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202001041>.

The financial sector experienced a wave of suspected state-sponsored distributed denial-of-service attacks on major US banks in 2012 and 2013, causing widespread service disruptions.[20] And on 10 February 2020, the Department of Justice announced an indictment against four members of the Chinese military related to their role in the Equifax data breach.[21] Recently, a state-sponsored actor was reported to have by-passed two-factor authentication to attack government entities and service providers in the energy, finance and insurance sectors.[22]

While a business may not always be able to prevent a zero-day or sophisticated attack from occurring, general and specialised awareness of the cyber threat landscape (through robust cyber threat intelligence, as discussed further below) and robust intrusion detection and incident response capabilities can mitigate the extent of the damage caused by such attacks.

CURRENT AND EMERGING CHALLENGES THAT BUSINESSES SHOULD REMAIN FOCUSED ON

Privacy and Information Security Standards Increasingly Rigorous

Over the past year, there has been the release of additional information security and privacy frameworks that are freely available to businesses. The National Institute of Standards and Technology (NIST), which published the increasingly adopted Cybersecurity Framework and routinely updates its library of information security controls,[23] is now working on a complementary Privacy Framework that seeks to develop a robust model for privacy policies, procedures and standards.[24] The Financial Services Sector Coordinating Council released its Cybersecurity Profile, which adopted the NIST Cybersecurity Framework and incorporated applicable regulatory guidance to the financial services sector.[25]

In addition to an increasing number of frameworks, including State-driven information security standards, there is an expanding number of resources that provide cyber threat intelligence, which is becoming a critical component in any business' cybersecurity program. As such, businesses must be aware of the evolving threats to its authentication and security measures, and ensure that periodic reviews are conducted accordingly. For instance, the FBI reported successful exploitation of text-message-based multi-factor authentication, and urged companies to reevaluate or enhance their authentication practices.[26] Additionally, many browsers, such as Chrome and Safari, will end support for weaker security encryption protocols by early to mid-2020.[27]

Compliance Management with Data Privacy Laws

---

[20] Council on Foreign Relations, "Denial of Service Attacks Against U.S. Banks in 2012–2013" (2012) <https://www.cfr.org/interactive/cyber-operations/denial-service-attacks-against-us-banks-2012-2013>.

[21] FBI, "Chinese Military Hackers Charged in Equifax Breach" (10 February 2020) <https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020>.

[22] Catalin Cimpanu, "Chinese Hacker Group Caught Bypassing 2FA", *ZDNet*, 23 December 2019 <https://www.zdnet.com/article/chinese-hacker-group-caught-bypassing-2fa/>.

[23] The Cybersecurity Framework is accessible at <https://www.nist.gov/cyberframework>.

[24] The Privacy Framework is accessible at <https://www.nist.gov/privacy-framework>.

[25] The FSSCC Cybersecurity Profile is accessible at <https://fsscc.org/Financial-Sector-Cybersecurity-Profile>.

[26] FBI Cyber Division, "Cyber Criminals Use Social Engineering and Technical Attacks to Circumvent Multi-Factor Authentication" (20190917-001, 17 September 2019) <https://info.publicintelligence.net/FBI-CircumventingMultiFactorAuthentication.pdf>.

[27] Bruce Morton, "Major Browsers Coordinated on Deprecating TLS 1.0 and 1.1" (Entrust Datacard, 5 November 2018) <https://www.entrustdatacard.com/blog/2018/november/deprecating-tls>.

The *GDPR* is now entering its second year, and a number of enforcement actions are already on record;[28] the *CCPA* is also now in effect, and other State privacy and cybersecurity laws and regulations are potentially in the pipeline. Though each of the privacy statutes and regulations introduce similar or overlapping privacy principles, such as the right to opt-out of third-party disclosures of consumer information, each maintains nuances on requirements and exceptions.[29] The varying statutory frameworks and regulations makes compliance management increasingly complex as businesses must navigate through a host of varying State, federal (to the extent it is a covered entity) and international laws.

The increasing complexity of privacy laws has resulted in renewed focus on data governance and data management practices. In order to comply with many of the existing privacy laws, including the *GDPR*, businesses must have total visibility of their information processes, including where and how sensitive consumer information is processed, stored, transmitted and disclosed across its information systems.

Data governance and management is often an overlooked component of an information security and data privacy program. Well-designed safeguards protecting sensitive business and consumer information are less effective if the business is unaware of how information moves through its networks, internally and externally, on a day-to-day basis.

Vendor Management to Remain a Major Challenge

In 2019, several companies faced challenges with third and fourth-party service providers, including incidents related to the compromise of sensitive consumer or financial information and incidents related to the availability of consumer information (which cybersecurity laws are beginning to address[30]). Third and fourth-party risk remains a particularly challenging area of information security and privacy compliance, and is expected to remain so as businesses continue to outsource data processing, modelling and other technology services.

While the overall proportion of data breaches caused by a third-party has fluctuated from year-to-year, several studies have placed third or fourth-party breaches at more than half of all data breaches for a typical given year.[31] Additionally a major study concluded that third parties were a significant cost-amplifying factor in data breach response.[32]

Generally, cybersecurity, privacy and data breach laws put the majority of the compliance responsibility squarely on the data owners (and not providers).[33] Consequently, any compromise of a third or fourth-party service provider may adversely affect a business, particularly those that did not conduct adequate due diligence and periodic review for compliance with contractual and information security program requirements.

---

[28] "Major GDPR Fine Tracker – An ongoing, Always-Up-to-Date List of Enforcement Actions" (Alpin, 17 December 2019) <https://alpin.io/blog/gdpr-fines-list/> (tracking 27 major (over €100,000) enforcement actions totaling over €428,545,407 in fines).

[29] Compare Nev Rev Stat § 603A.330(2)(b) (excluding financial institutions subject to the *Gramm–Leach–Bliley Act*) with Cal Civ Code § 1798.145(e) (only excluding "personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act" or the *California Financial Information Privacy Act*).

[30] See, eg, NY Comp Codes R & Regs, tit 23 § 500.02(a) ("Each Covered Entity shall maintain a cybersecurity program designed to protect the … availability of the Covered Entity's Information Systems").

[31] See, eg, Chuck Brooks, "A Passport to Data-Centric Protection and Privacy" (IBM, 8 January 2020) ("More alarming is that 59 percent of companies experienced a data breach caused by a third party and that, according to an IBM-sponsored study by Solitaire Interglobal Ltd, 78 percent of customers surveyed would not automatically return to a business after a data breach" (internal footnotes omitted)).

[32] IBM and Ponemon Institute, "Cost of a Data Breach Report 2019" (2020) 39.

[33] See, eg, Wash Rev Code § 19.255.010(1) ("Any person or business that conducts business in this state and that *owns or licenses data* that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state" (emphasis added)).

Insider Threats

Insiders (employees, contractors or other individuals with authorised access) continue to contribute to a substantial proportion of data incidents. In 2019, several high-profile data breaches in the financial services sector were due, in part, to insider abuse. And as businesses increasingly leverage third-party cloud access, technology services, data science solutions, processing and other services, each potentially requiring access to or the storing of private consumer information as part of legitimate activities, the risk of an insider breach increases.

Over the past several years, large companies have become increasingly sophisticated at implementing policies, procedures and standards aimed at managing insider threat (as required by certain regulated entities). Some examples include the prohibition of removable storage devices, email scanning for sensitive information and mobile device management. Regulators, such as the NYDFS, are requiring businesses to implement safeguards to monitor the use of authorised users that have access to sensitive consumer information,[34] and businesses that experience data breaches due to poor insider risk mitigation may face additional regulatory scrutiny.

Aggregators and Data Brokers

In 2017, the Consumer Financial Protection Bureau published guidelines for financial institutions regarding financial data sharing and data aggregators, which, among other things, emphasised the consumer's right to access such services, but also imposed a duty on financial institutions to prevent abuse by third-party aggregators accessing consumer information.[35] Now, in 2020, it is expected that third-party aggregators will remain a challenge with respect to information security and consumer protection, with financial institutions struggling to maintain control over screen-scraping and the sharing of consumer account credentials.

Third-party aggregator services will need to expand their capabilities and services, requesting more and more consistent access to consumer information held by financial institutions. Additionally, regulators will likely continue to rely upon financial institutions and other regulated entities to protect consumer information and consumer choices. To this end, financial institutions are developing alternative approaches to prevent screen-scraping, such as the use of security tokens and the monitoring of third-party access, which: (1) provide consumers with more control over third-party aggregator access to personal and financial information; and (2) improve the security and confidentiality of consumer and financial information.

Secure Development Operations

Many industry frameworks, as well as the NYDFS, have also turned to pre-emptive policies, procedures and standards designed to prevent vulnerabilities from appearing in the first place.[36] Similar to the idea of privacy-by-design, development operations and development security operations (DevSecOps) emphasise the need to build security into the development environment and consider information security as part of the overall development effort. In 2019, the DoD introduced a DevSecOps framework for the defense industry as a formal approach to implementing security operations in application development.[37] Recently, the Payment Card Industry Standards Council has also released its Payment

---

[34] NY Comp Codes R & Regs, tit 23 § 500.14(a).

[35] Consumer Financial Protection Bureau, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Authorization" (18 October 2017) <https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf>.

[36] See, eg, NY Comp Codes R & Regs, tit 23 § 500.03(i) (requiring businesses, as part of its cybersecurity program, to consider "systems and application development and quality assurance").

[37] Chief Information Officer, "DoD Enterprise DevSecOps Reference Design" (Department of Defense, 12 August 2019).

Card Industry Software Security Standards and Secure Software Lifecycle to promote secure payment software and secure software development practices.[38]

Although DevSecOps is not a new concept, it has traditionally not garnered much attention; however, it is anticipated that security-by-design-like concepts will become more widely developed in light of growing cybersecurity laws and regulations.[39]

CONCLUSION

The strong emphasis on privacy and cybersecurity compliance will remain a key area of focus for regulators, legislatures and the general public. Businesses will be expected to maintain reasonable security measures and comply with privacy regimes, both of which remain highly active and dynamic fields.

[38] The Payment Card Industry Software Security Standards and the Secure Software Life Cycle Standards are accessible at: <https://www.pcisecuritystandards.org/document_library>.

[39] See, eg, NY Comp Codes R & Regs, tit 23 § 500.08(a).