ALERT MEMORANDUM

2018 Cybersecurity and Data Privacy Developments: A Year in Review

January 29, 2019

In 2018, data privacy and cyber breaches made headlines throughout the year. Major companies continued to suffer data breaches, highlighting the risks and potential costs of cyber incidents across industries. At the same time, a growing and overlapping thicket of data security and privacy regulations—within the U.S., European Union, Latin America, and elsewhere—continued to increase compliance costs and regulatory risks. This memo surveys some of the key cybersecurity and data privacy developments of 2018, including the major data breaches and cyberattacks, regulatory and legislative actions, and notable settlements and court decisions.

In addition, we identify some key takeaways from 2018, which include the importance of rapid response and timely disclosure, cyber diligence in M&A transactions, effective management of third-party vendor risk, and protecting privilege. We also highlight key areas to watch in 2019, including GDPR enforcement, efforts to pass a U.S. federal privacy law, responses and potential changes to California's new privacy law, the adoption of comprehensive privacy laws in more U.S. states and non-U.S. jurisdictions, and heightened U.S. litigation and enforcement risk. Data security and privacy will undoubtedly remain a priority for boards and senior management, as well as regulators and enforcement authorities.

For additional insights and updates relating to cybersecurity and data privacy, please visit and subscribe to the Cleary Cybersecurity and Privacy Watch blog.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

NEW YORK

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

Jonathan Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Pamela L. Marcogliese
+1 212 225 2556
pmarcogliese@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

WASHINGTON

Katherine Carroll
+1 202 974 1584
kcarroll@cgsh.com

Alexis Collins
+1 202 974 1519
alcollins@cgsh.com

PARIS

Emmanuel Ronco
+33 1 40 74 69 06
eronco@cgsh.com

Major Cyberattacks

Major cyberattacks and breaches continued to grab headlines in 2018. As in past years, a wide array of industries were targeted by hackers. Companies that collect large amounts of personal identifying information, including payment account information, continue to be some of the most vulnerable. Described below are some of the more notable incidents of 2018.

- **Marriott International** disclosed in November 2018 a breach of approximately 383 million guests' personal information from the database of Starwood Hotels, which Marriott had acquired in 2016. Measured by the number of potentially affected consumers, the Marriott breach was the year's most significant.
- The retail industry also suffered some significant cyber incidents:
  - **Under Amour** disclosed a breach of an estimated 150 million users of its food and nutrition application, MyFitnessPal.
  - **Saks** and **Lord & Taylor** disclosed that their stores had suffered the theft of 5 million cardholders' information.
  - **Adidas** disclosed that contact information and encrypted passwords for millions of customers had potentially been compromised from its website.
- The airline industry was also a frequent target of hackers in 2018:
  - **Cathay Pacific** disclosed a breach of 9.4 million passengers' data.
  - **British Airways** disclosed that personal information, including credit card details, of 380,000 customers was exposed in a data breach incident.
  - **Delta** announced that an online chat vendor may have exposed payment information of "several hundred thousand" customers.
- **Facebook** disclosed two separate incidents:
  - Personal information of approximately 87 million Facebook users was harvested by political consulting firm Cambridge Analytica.
  - In September 2018, Facebook disclosed that hackers exploited a vulnerability to access approximately 30 million user accounts.

Regulatory Actions

2018 also saw a number of significant U.S. enforcement actions relating to cybersecurity and data privacy at both the state and federal level.

- **Uber** agreed to pay $148 million to state enforcement officers of all 50 U.S. states over its 2016 data breach. The breach affected personal records of 57 million users and drivers, and drew attention when Uber admitted to paying the hackers who caused the breach and delaying disclosure of the breach for nearly one year. The FTC also expanded its 2017 settlement with Uber to include additional violations arising from the 2016 breach.
- **Equifax** entered a settlement order with the NY DFS and seven other state banking regulators for its massive data breach in 2017 that exposed sensitive personal information of nearly 148 million customers. Rather than imposing monetary penalties, the order required Equifax's board to review and approve the company's risk assessment, enhance oversight of its information technology operations, and implement software to strengthen their IT security, among other things.
- In the first criminal charges in connection with the Equifax breach, the Department of Justice ("DOJ") and SEC charged a former Equifax executive for insider trading. The DOJ indictment and SEC complaint allege that Equifax's former Chief Information Officer sold Equifax stock after learning of the breach, but prior to its public disclosure.
- **Altaba**, formerly **Yahoo**, entered into a settlement with the SEC for its failure to disclose a cybersecurity breach in 2014. Altaba agreed to pay $35 million to settle allegations that Yahoo violated

federal securities laws by failing to timely disclose the 2014 data breach in its subsequent public securities filings. This was the first time a public company was charged by the SEC for inadequate disclosure related to cybersecurity.[1]

- A Des Moines, Iowa-based broker-dealer and investment adviser agreed to pay $1 million to settle charges related to its failure to maintain appropriate cybersecurity policies and procedures surrounding a cyber intrusion that compromised personal information of thousands of customers. This was the first SEC enforcement action charging violations of the Identity Theft Red Flags Rule.[2]

In addition to bringing several enforcement actions, the SEC also issued several cybersecurity-related guidance documents:

- In February 2018, the SEC issued updated cybersecurity disclosure guidance. The SEC stated that existing disclosure requirements impose an obligation on companies to disclose cyber-related matters based on generally applicable standards of materiality. In particular, companies are expected to provide non-generic disclosures tailored to particular cybersecurity risks and incidents that are material, and may have a duty to correct a prior disclosure if it was untrue, or it omitted a material fact necessary to make the disclosure not misleading, at the time it was made or a duty to update a disclosure that becomes materially inaccurate after it is made.
- In October 2018, the SEC released a Report of Investigation regarding certain cyber-related frauds perpetrated against public companies and related internal accounting controls requirements. The Report focused on the requirement that public companies maintain controls that reasonably safeguard company funds. The Report highlighted certain remedial steps taken by the companies, including enhanced payment authorization controls, vendor payment controls, account reconciliation procedures, outgoing payment notification processes, and training. The Report, however, did not prescribe specific controls but instead stated that "issuers themselves are in the best position to develop internal accounting controls that account for their particular operational needs and risks."
- In December 2018, the SEC's 2019 Examination Priorities highlighted OCIE's key areas of focus, and FINRA drew on its examinations of broker-dealers to identify effective cybersecurity practices in a Report on Selected Cybersecurity Practices.

U.S. Legislative Activity

State legislatures were also active on the cybersecurity and data privacy front in 2018. Some important developments at the state level included:

- As of April 2018, **all 50 states, the District of Columbia and several U.S. territories have data breach notification laws**, with Alabama and South Dakota being the last states to enact their respective laws. Because of the lack of a comprehensive federal regime regarding data breach notifications, companies suffering a breach of personal data generally must comply with multiple state notification requirements. While most states' data breach notification laws have similar structures, nuances in the statutes can create significant differences on questions such as when the clock starts for the required timing of a notice.[3]
- In June 2018, **California passed the California Consumer Privacy Act ("CCPA")**, the most comprehensive data privacy law to date in the United States. Under the CCPA, California consumers have broad rights to know what personal information has been collected about them, the sources for the

[1] For Cleary Gottlieb's previous blog post discussing the SEC enforcement action, see https://www.clearycyberwatch.com/2018/04/yahoos-successor-settles-first-ever-case-involving-sec-charges-failing-disclose-cybersecurity-incident/.

[2] For the SEC Order in this case, see https://www.sec.gov/litigation/admin/2018/34-84288.pdf.

[3] For Cleary Gottlieb's previous blog post discussing the developments in state law regarding data breach notification, see https://www.clearycyberwatch.com/2018/04/50-states-now-data-breach-notification-laws/.

information, the purpose of collecting it, and whether it was disclosed. The CCPA also gives consumers the right to access personal information about themselves held by covered businesses, to require deletion of the information, and to prevent its sale to third parties. The CCPA is scheduled to go into effect in 2020, although significant work remains to be done on regulatory implementation and potential amendments.[4]

- In September**, California also adopted the first state law regarding the security of Internet of Things ("IoT") devices**. Starting on January 1, 2020, any manufacturer of a device that connects "directly or indirectly" to the internet must equip it with "reasonable" security features that are designed to prevent unauthorized access, modification, or information disclosure.
- **Colorado** and **Ohio** also adopted data protection laws in 2018. Ohio took a novel approach by providing a safe harbor from breach claims for companies that adopt a cybersecurity program, provided that the program conforms with the NIST cybersecurity framework or another industry-recognized cybersecurity framework.
- **Vermont** became the first state to adopt a law directed at regulation of data brokers.
- The proliferation of state laws, combined with increasingly negative public sentiment about some data sharing practices, led to increased support by the end of the year for some form of federal privacy legislation. Industry groups, including leading tech firms, have publicly advocated for a federal law that preempts the patchwork of state law requirements. In Congressional testimony, the FTC Chair and Commissioners unanimously endorsed adoption of a comprehensive federal privacy bill, although they were divided on whether it should preempt state law. A bipartisan coalition of state AGs has opposed federal preemption of state notification and privacy laws, arguing that state agencies play an important role in protecting consumer rights. By the end of 2018, Congress appeared poised to take up the issue. Multiple bills were introduced in the closing months of 2018, including the Consumer Data Protection Act, which appears modeled on the GDPR and provides for prison sentences for misrepresentations by executives, and the Data Care Act, introduced in December by a group of 15 senators.

Updated NIST Framework

In April 2018, the U.S. Commerce Department's National Institute of Standards and Technology ("NIST") released an updated version of its voluntary Cybersecurity Framework. The Framework is the result of public-private collaboration and represents the most significant set of (non-binding) cybersecurity standards in the United States. The 2018 version of the Framework includes updates on authentication and identity, self-assessing cybersecurity risk, managing cybersecurity within the supply chain and vulnerability disclosure.

U.S. Court Decisions

U.S. courts grappled with the issues raised by data breach litigation brought by consumers and others. Proof of injury and **Article III standing** issues continue to be front and center in data breach cases.

- In March 2018, **the Supreme Court** declined review of the standing issue in the data breach context,[5] despite the ongoing disagreement between the Circuit courts.[6]
- **The Ninth Circuit** held in March 2018[7] that it was sufficient for consumers to allege a **substantial risk** of identity theft or fraud resulting from a data breach,

[4] For Cleary Gottlieb's previous blog post discussing the CCPA, see https://www.clearycyberwatch.com/2018/07/californias-groundbreaking-privacy-law-new-front-line-u-s-privacy-debate/.

[5] *Attias v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017), *cert. denied Carefirst v. Attias*, No. 17-641 (2017).

[6] For Cleary Gottlieb's previous blog post discussing the implications of the Supreme Court's decision, see https://www.clearycyberwatch.com/2018/03/supreme-court-declines-review-standing-data-breach-context-despite-ongoing-circuit-split/.

[7] *In re Zappos.com, Inc.*, No. 16-16860, 2018 WL 1189643 (9th Cir. Mar. 8, 2018).

even in the absence of allegations that the risk actually materialized.[8]

- **The Seventh Circuit** joined the Ninth Circuit in *Dieffenbach v. Barnes & Noble, Inc.*,[9] deciding that allegations of data theft combined with a **substantial risk** of future harm are sufficient to establish Article III standing, even in the absence of allegations that the risk actually materialized.[10]
- **The Fourth Circuit** took a stricter approach in *Hutton v. National Board of Examiners in Optometry, Inc.*,[11] holding that alleged costs for mitigating measures to safeguard against future identity theft was a sufficient injury to establish standing while declining to adopt the lower "substantial risk" standard.[12]

2018 also saw some of the first court decisions that focused on the merits of data breach claims at the pleading stage, rather than solely standing issues. Many of the decisions turned on the particular applicable state law, further underscoring the disparate set of obligations and liabilities companies may have across the 50 U.S. states.

- In *In re Supervalu, Inc. Cust. Data Sec. Breach Litig.*,[13] the plaintiff established Article III standing, yet the court nevertheless held that the plaintiff had failed to state a claim under Illinois state law including because he did not plead out-of-pocket losses and negligence claims were barred by the "economic loss" doctrine.
- The Northern District of California held in *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*[14] that, as a matter of California law, the plaintiffs did *not* need to plead out-of-pocket losses and the economic loss rule did *not* bar the negligence claims. The court also found that plaintiffs stated claims under California consumer protection laws by alleging they would not have paid for Yahoo! premium services had they known that its e-mail server was not secure.
- In *Bellwether Community Credit Union v. Chipotle*,[15] the court found that the plaintiffs had failed to sufficiently plead claims for negligence and violations of unfair competition laws in Maine, Florida, Massachusetts, Vermont and Arkansas. The judge did, however, allow allegations under California's Unfair Competition Law and New Hampshire's Consumer Protection Act.

In the **regulatory context**, the Eleventh Circuit vacated a cease-and-desist order from the FTC against LabMD, Inc. as unenforceable because it found that the order commanded an overhaul of the company's data security program without providing a reasonably definite standard by which a court could determine compliance.

In the **shareholder litigation context**, in December, the District Court for the Northern District of California dismissed a putative securities fraud class action against **PayPal** Holdings, its subsidiary TIO Networks Corp., and several executives for a breach that resulted in the potential compromise of personally identifiable information for 1.6 million customers. Notably, the court found that plaintiffs had sufficiently alleged the existence of a false statement because the company had disclosed only a security "vulnerability," when an actual breach had occurred. The court, however, ultimately dismissed the complaint because plaintiffs failed to adequately plead scienter, i.e. that defendants knew not

[8] For Cleary Gottlieb's previous blog post discussing the Ninth Circuit decision, see https://www.clearycyberwatch.com/2018/03/ninth-circuit-reverses-dismissal-lack-standing-data-breach-case/.
[9] *See In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-08617, 2017 WL 2633398 (N.D. Ill. June 13, 2017), vacated sub nom. *Dieffenbach v. Barnes & Noble, Inc.*, No. 17-2408, 2018 WL 1737128 (7th Cir. Apr. 11, 2018).
[10] For Cleary Gottlieb's previous blog post discussing the Seventh Circuit decision, see https://www.clearycyberwatch.com/2018/04/seventh-circuit-expands-jurisprudence-data-breach-cases/.
[11] No. 17-2408, 2018 WL 1737128 (7th Cir. Apr. 11, 2018).
[12] For Cleary Gottlieb's previous blog post discussing the Fourth Circuit decision, see https://www.clearycyberwatch.com/2018/07/fourth-circuit-eight-circuit-address-injury-data-breach-cases/.
[13] No. 14-02586 (D. Minn. Mar. 7, 2018).
[14] No. 16-MD-02752, (N.D. Cal. Aug. 30, 2017).
[15] 17-cv-01102 (N.H. Oct. 25, 2018).

only of an actual security breach, but also the magnitude of the breach and the type of data accessed.[16]

U.S. Litigation Settlements

Several record-breaking litigation settlements were reached in 2018, with settlement amounts increasing from prior years. Some of the most notable settlements included:

- A court approved Anthem's settlement to pay **$115 million** for a consumer class action over its 2015 breach affecting almost 80 million users. Under the settlement, Anthem agreed to spend a specified minimum amount per year on information security and to revise its cybersecurity practices based on recommendations by the plaintiffs' cybersecurity expert, update its data retention policies, and conduct annual reviews of its information technology security and settlement compliance.[17]
- Yahoo agreed to pay **$85 million** and provide two years of free credit monitoring to a class of approximately 200 million users affected by its breaches in 2013 and 2014, which were disclosed in 2016.
- Yahoo separately agreed to pay shareholders **$80 million** to settle claims that it misled investors by failing to disclose the breaches in its public filings, while still touting the strength of its cybersecurity practices.

GDPR and Related International Developments

Cybersecurity and data privacy developments were just as fast-paced outside of the United States.

GDPR and Related Guidance:

- The European Union's General Data Protection Regulation ("GDPR") became fully applicable in May 2018 and represents the biggest change to EU data protection law in more than twenty years.[18] It grabbed headlines as a result of its extra-territorial reach, the various new obligations it imposes upon organizations, and the enhanced enforcement powers given to member state data protection supervisory authorities. In particular, supervisory authorities may levy fines of up to €20 million or 4% of annual global revenue (whichever is higher).[19]
- The European Data Protection Board[20] ("EDPB") has endorsed and published various guidelines in connection with the application and interpretation of the GDPR, including in relation to the concepts of "transparency" and "profiling," as well as the territorial scope of the GDPR.
  - *Transparency* - The EDPB's guidelines set out important information about how to achieve compliance with the GDPR's overarching obligation to be transparent about processing activities. The guidelines should be consulted in connection with any communications made to data subjects about the way in which their personal data will be used; in particular, to ensure

[16] Sgarlata v. PayPal Holdings Inc., No. 17-cv-06956-EMC, 2018 WL 6592771 (N.D. Cal. Dec. 13, 2018)
[17] For Cleary Gottlieb's previous blog post discussing the settlement and Anthem's subsequent settlement with U.S. health officials, see https://www.clearycyberwatch.com/2018/10/u-s-department-health-human-services-settles-anthem-record-16m-alleged-hipaa-violations/.
[18] A general overview of the GDPR is provided in our Alert Memorandum (https://www.clearygottlieb.com/~/media/organize-archive/cgsh/files/publication-pdfs/alert-memos/alert-memo-pdf-version-201650.pdf).
[19] For details of the guidance issued in connection with GDPR's new administrative fine regime, please see the Cleary blog post at https://www.clearycyberwatch.com/2017/12/administrative-fines-gdpr/
[20] The EDPB is an independent body established by the GDPR composed of representatives of the national data protection authorities and the European Data Protection Supervisor, which can adopt general guidance on the GDPR and is also empowered to make binding decisions to ensure a consistent application of the GDPR.

compliance with the information giving requirements set out in Articles 13 and 14 (and the standards prescribed by Article 12). The guidelines emphasize the importance of accessibility of information, for the purpose of empowering data subjects through information.

- *Profiling* – The GDPR places general safeguards around profiling and automated decision-making, including that data subjects have the right *not* to be subject to automated decision making (including profiling) to the extent that such decisions produce legal effects which could affect them in a significant way. The profiling guidelines unpack the various concepts which form part of such rules under the GDPR, including providing clarity over the differences between "profiling" on the one hand and "solely automated decision making" on the other.[21]
- *Territorial Scope* – Most recently, the EDPB published its highly anticipated draft guidelines on the territorial scope of the GDPR. Under the GDPR, the applicability of EU data protection principles has been expanded to include processing of personal data in the context of an EU establishment (even where the processing does not take place in the EU) and processing activities conducted by an organization outside of the EU which relate to the offering of goods or services or the monitoring of behavior of data subjects in the EU (respectively, the so called "establishment" and "targeting" criteria). The EDPB's guidelines provide information in connection with the various elements of the applicability tests, including unpacking the concepts of "establishment" and "targeting".[22]

Enforcement Action:

- In 2018, data protection supervisory authorities continued to take enforcement actions for breach of the previous European data protection regime. For example, the UK ICO levied the maximum fine of £500,000 against Equifax for its 2017 data breach (i.e., which occurred prior to the GDPR taking full effect). Similarly, the ICO also fined Uber £385,000 for failing to protect customers' personal information relating to a 2016 cyberattack[23] (along with the Dutch and French supervisory authorities who also imposed fines in connection with this security event).[24] The ICO also issued a notice of intent to levy the maximum fine possible (£500,000) on Cambridge Analytica.[25] It is likely that we will continue to see enforcement actions under the previous regime in 2019, with enforcement actions under the GDPR becoming increasingly more commonplace.
- Enforcement action under the GDPR commenced in 2018 (including the ICO's order against AggregateIQ, requiring AggregateIQ to delete the personal data of UK data subjects from its systems, and the CNIL's formal notices against two marketing platform providers for failing to obtain valid consent for the use of location data for profiling and targeted advertising). Few monetary penalties have been imposed to date, with one of the first being the fine imposed by the German data protection authority against Knuddels GmbH & Co KG following a security breach which resulted in the

[21] For details about the profiling guidelines, as well as information on guidelines relating to the role of the data protection officer and data protection impact assessments, please see a previous Cleary blog post at https://www.clearycyberwatch.com/2017/11/preparing-gdpr-guidance-article-29-working-party/

[22] For Cleary's blog post summarizing the guidelines, please see https://www.clearycyberwatch.com/2019/01/edpb-publishes-draft-guidelines-territorial-scope-gdpr/

[23] Uber, Information Commissioner's Office (November 26, 2018) https://ico.org.uk/action-weve-taken/enforcement/uber/.

[24] Dutch DPA: fine for data breach Uber, Autoriteit Persoonsgegevens (November 27, 2018) https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fine-data-breach-uber.

[25] For further information, please see the Cleary blog post at https://www.clearycyberwatch.com/2018/07/uk-data-protection-regulator-set-levy-maximum-fine-facebook-cambridge-analytica-case/

theft (and subsequent publication) of information relating to approximately 330,000 users. Knuddels was fined €20,000, which appeared to take into account the efficiency with which the data controller mitigated the damage and informed data subjects.[26] In January 2019 however, the French supervisory authority (the "CNIL") issued its first GDPR-based fine (and the first big-ticket fine under the GDPR to date). The fine of €50 million was levied against Google LLC for its personalized advertising practices. The alleged violations relate to a lack of transparency, accessibility and proper information for data subjects, as well as reliance on invalid consent. Google LLC announced that it will be appealing this decision before the French Supreme Administrative Court (the "*Conseil d'Etat*").

Data Transfers:

- *Adequacy* - In July 2018, the EU and Japan agreed to recognize each other's data protection systems as equivalent, allowing businesses to transfer personal data between the EEA and Japan without further safeguards. The European Commission has so far recognized 12 other countries as adequate, but this is the first time that the EU has agreed to a reciprocal adequacy arrangement.
- *Privacy Shield*. In June 2018, the European Parliament called for suspension of the Privacy Shield on the basis that it did not believe that the United States was compliant with its obligations. The European Commission conducted its second annual review of the scheme in October 2018 and found, to the contrary, that the United States *does* ensure an adequate level of protection for personal data transferred under the Privacy Shield, noting that the Department of Commerce has strengthened the certification process and the FTC has taken a more proactive approach to enforcement.[27] Consequently, the Privacy Shield remains a viable mechanism for the transfer of personal data the United States, for the time being (subject to continued scrutiny from European institutions).
- *Standard Contractual Clauses*. In April 2018, following a complaint to the Irish High Court by the Irish Data Protection Commission in connection with the data processing activities of Facebook (which include the transferring of personal data of EU data subjects to the United States), the Irish High Court referred a number of questions to the Court of Justice for the European Union ("CJEU"), including questions in connection with the adequacy of Standard Contractual Clauses ("SCCs") and the Privacy Shield. This reference was challenged by Facebook, and the Irish Supreme Court has agreed to hear Facebook's appeal. In the event that the CJEU is required to give its opinion on the adequacy of SCCs and the Privacy Shield, these mechanisms may be invalidated, which would cause chaos for international data flows.

Regulatory Review of GDPR's Impact:

- The French CNIL's first review and assessment of its activities 6 months after the entry into application of the GDPR shows an increased awareness of individuals, with respect to their rights to data protection, and of companies, with respect to their GDPR obligations. The CNIL highlights *inter alia* that the number of complaints for alleged GDPR breaches has increased by 34 % and that it has already received 1000 data breach notifications.[28]

International Developments:

2018 also saw several other countries implement national data protection laws, often with parallels to the GDPR.

- **Brazil's** new data protection law (*Lei Geral de Proteção de Dados Pessoais*) was recently passed

[26] For further information, see our blog post at https://www.clearycyberwatch.com/2018/12/first-german-fine-issued-gdpr/

[27] For further information, please see the Cleary Gottlieb "Selected Issues for Boards of Directors in 2018" publication (Cybersecurity and Privacy), at https://www.clearygottlieb.com/news-and-insights/publication-listing/selected-issues-for-boards-of-directors-2018-landing-page

[28] https://www.cnil.fr/fr/rgpd-quel-bilan-6-mois-apres-son-entree-en-application

and is scheduled to go into effect in 2020. Among other things, it includes significant new data protection rules and transfer limitations similar to the GDPR. It also includes data breach notification requirements, and significant penalties of up to 2% of turnover in Brazil, up to approximately USD $12 million per violation. The Brazilian National Monetary Council also issued new cybersecurity requirements for financial institutions, including third-party service providers in or outside Brazil.[29]

- **Canada's** new mandatory breach-notification requirements in the Personal Information Protection and Electronic Documents Act ("PIPEDA") went into effect on November 1, 2018. PIPEDA requires affected entities to report to the Canadian Office of the Privacy Commissioner, notify the affected individuals as soon as feasible, and imposes recordkeeping obligations requiring companies to keep records of *every* breach involving personal information under their control for two years.
- A government committee in **India** released a draft Personal Data Protection Bill in 2018, which is currently making its way through the legislative process. The bill is modeled after the GDPR, but also introduces data localization requirements.
- **China** adopted multiple new standards and draft or final regulations related to cybersecurity, including the national standard on protection of personal information, which became effective in May 2018. Further regulations are expected in 2019, including rules regarding cross-border transfer for personal information and other data.

Takeaways and Looking Ahead to 2019

The breaches disclosed and other developments in 2018 reinforce the importance of several issues in mitigating cyber risk:

- **Timely investigation and disclosure continues to be critical (but challenging)**. A number of companies were criticized for the amount of time taken to identify the affected data and make disclosures after learning of the breach. In contrast, Under Amour made a disclosure four days after learning of their breach, which may have mitigated any reputational harm. Prompt disclosure has to be carefully managed given the risks of disclosing inaccurate or incomplete information, so this continues to present challenges. The updated Uber FTC settlement also underscores that companies must be scrupulous in meeting their disclosure obligations even if they believe the threat has been neutralized.
- **Cyber diligence in M&A transactions is essential**. Marriott apparently inherited a compromised database in its merger with Starwood. Cyber diligence in mergers and acquisitions, including a target's information security systems and any past breaches, has become standard practice. Understanding best practices for diligence and contractual protections is more important than ever.
- **Third-party vendors remain an area of high risk**. The breach of Delta customer information took place at one of its vendors, which allegedly did not inform Delta of the breach for several months following the incident. Conducting cyber diligence of vendors and considering when agreements should require prompt notifications and include other protections is a critical aspect of managing cybersecurity risk given the potential exposure.
- **Companies must be vigilant about protecting privilege.** In *In re United Shore Fin. Servs., LLC*,[30] the Sixth Circuit required a company to turn over materials relating to a privileged forensic data breach investigation because, the court concluded, the company had implicitly waived privilege when it asserted an affirmative

[29] See https://www.clearycyberwatch.com/2018/05/brazil-issues-new-cybersecurity-regulation-regulated-financial-institutions/

[30] No. 17-2290, 2018 WL 2883893 (6th Cir. Jan. 3, 2018).

defense based on the investigative conclusions. In order to maximize privilege over a data breach investigation, companies should ensure that forensic investigators are retained and supervised by outside counsel and that any forensic conclusions are maintained confidentially, and should guard against implicit waiver when defending litigation.

- **Companies must position themselves to adapt quickly.** Legal requirements are multiplying and regulatory expectations are evolving rapidly. Companies must be forward-thinking and strategic about their approach to data privacy to avoid constant and costly change and identify cost-effective ways to minimize fragmentation due to multiple legal regimes. Particularly with California's new privacy law soon becoming effective alongside the GDPR, new requirements pending in other important jurisdictions, and regulatory focus on privacy and data security, global companies in particular must be strategic and agile to stay on top of (and ideally ahead of) changing requirements.

In 2019, legislative, regulatory, and enforcement activity related to data privacy and cybersecurity is likely to continue at a fast pace, while data will continue to become even more central to much of the economy. Areas to watch in 2019 include:

- The FTC seeking to take a more active role in the privacy space, including efforts to use its enforcement actions to impose particularized data security requirements.
- Continued proliferation of data privacy and cybersecurity requirements around the world, including the potential for federal privacy legislation in the United States.
- A shifting landscape in private industry's approach to potential privacy legislation, with growing recognition of the benefits of federal legislation.
- Intense negotiations between privacy advocates and industry over the implementation of California's CCPA.
- Increasing U.S. litigation risk following a data breach, particularly with the potential ability of plaintiffs to forum shop for hospitable jurisdictions following a nationwide breach, and continued enforcement risk with respect to compliance with breach notification requirements.
- More GDPR enforcement activity as the first year since the GDPR became effective comes to an end, including potentially actions relying on the GDPR's extra-territorial reach.
- Shifting norms and expectations of regulators and other enforcement authorities with respect to customer consent and uses of customer data.

In sum, while cybersecurity and data privacy issues filled the 2018 headlines and demanded the attention of boards and senior management, we expect 2019 to be just as eventful.

...

CLEARY GOTTLIEB