

Developments in Cybersecurity & Privacy: A Year in Review

Editor: Robert S. Want, Esq.
February 5, 2020

*This report is a condensed and edited version of
“Cybersecurity: Year in Review,”
published by law firm Cleary Gottlieb,
January 31, 2020.*

*In this edited version, some sections of the report
have been shortened or left out in their entirety.
All footnotes and citation to cases have been omitted.*

To access full report, [click here](#).

Introduction

In the past year, boards and senior management across a range of industries continued to cite cybersecurity as one of the most significant risks facing their companies. At the same time, comprehensive data privacy regulation became a new reality in the United States, and many U.S. companies have implemented major revisions to their privacy policies and data systems to achieve compliance with California’s groundbreaking privacy legislation and other newly enacted state laws.

Major data breaches continued to make headlines during the past year, and state and federal legislators and enforcement authorities remained highly focused on data security and privacy practices. European regulators announced several notable enforcement actions under Europe’s General Data Protection Regulation (“GDPR”), which confirmed that European authorities were willing to use the GDPR’s authorization to levy large fines, even outside the context of major breaches resulting in exposure of customer information.

Cybersecurity: Year in Review highlights what we believe to be the most significant cybersecurity and privacy developments during the past year, and we predict key challenges and areas of focus for the coming year.

Major Cyberattacks

Companies continued to suffer data breaches resulting from cyberattacks by malicious actors and security lapses resulting in exposure of customer data. Although a variety of business sectors remain at heightened risk, recent cyberattacks and data breaches highlight the particular risks faced by the financial, social media, and healthcare sectors.

The financial industry, in particular, suffered several notable security breaches in 2019:

- In May, it was reported that 885 million bank records, including social security numbers, bank account numbers and statements, and mortgage and tax documents that were maintained by First American Corporation were exposed through a design defect in a software application.

- In July, Capital One disclosed that a hacker had gained access to personal and financial information for approximately 106 million customers, at an estimated remediation costs at \$150 million.
- In June, an employee at Canada's Desjardins Group exposed the data of more than 4.2 million bank members by improperly collecting personal information and circulating it to a third party.

In the social media realm, Facebook, still reeling from the Cambridge Analytica scandal in 2018, suffered further data breaches in 2019:

- In March, an internal investigation at Facebook revealed that hundreds of millions of account passwords were stored in plain text on its internal servers, meaning that it was possible for Facebook employees to search and potentially abuse the credentials.
- And Facebook suffered additional data breaches during the past year: in April (540 million user records exposed on public Amazon databases); in September (more than 419 million user records exposed on a public database); in November (approximately 100 third-party developers were improperly granted access to personal user data); and in December (267 million user records, including names, unique user IDs, and phone numbers were exposed in another public database).
- The social media industry reported further data security lapses in October 2019, when it was disclosed that 1.2 billion Facebook, Twitter and LinkedIn profiles were exposed and made publicly accessible on an unsecured server.

The healthcare sector was also the target of several significant cyberattacks:

- In May, Quest Diagnostics disclosed that approximately 11.9 million patients' personal and financial data had been accessed through its external collection agency, American Medical Collection Agency.
- A month later, LabCorp disclosed that 7.7 million of its patient records had been accessed through the same agency, highlighting once again the risks associated with third-party agencies and vendors.
- In June, Dominion National, a dental and vision benefits insurer, disclosed a data breach that exposed the personal records of nearly 3 million patients.

U.S. Enforcement Actions

Not surprisingly in light of the ongoing large-scale data breaches, there were a number of significant U.S. enforcement actions relating to cybersecurity and data privacy in 2019. In some instances, several authorities or regulators have partnered together to announce a joint resolution that includes both financial penalties and remediation requirements. As expected, the Federal Trade Commission ("FTC") has taken a more active role in the privacy space, a trend we expect to continue in 2020.

The past year also saw the initiation of major antitrust investigations of technology companies by U.S. and European authorities that included privacy practices as one area of possibly anti-competitive or abusive behavior, potentially blurring the lines between traditional consumer protection and competition regulation.

- In July, the FTC announced a \$5 billion settlement with Facebook for violations of Section 5(a) of the FTC Act and its prior 2012 FTC settlement order, based on allegations that Facebook provided users with deceptive privacy disclosures and shared users' personal information with third-party applications used by those users' Facebook friends (the Cambridge Analytica scandal).
- Also in July, Equifax agreed to pay \$575 million—potentially rising to \$700 million—in a settlement with the FTC, the Consumer Financial Protection Bureau, the New York Department of Financial Services, and 48 U.S. states over the company's "failure to take reasonable steps to secure its network" in a 2017 breach involving the personal information of 147 million people.

The settlement required Equifax to take remedial steps including: conducting annual assessments of internal and external security risks; obtaining annual certifications from the board of directors or relevant subcommittee attesting to compliance with the settlement order; and ensuring that service providers that access personal information stored by Equifax have adequate safeguards to protect such data.

- In September, Google and YouTube agreed to pay \$170 million to the FTC and New York State to settle allegations that the companies illegally collected personal data from children without the consent of their parents. It was by far the largest amount ever obtained by the FTC in a matter brought under the Children's Online Privacy Protection Act, enacted in 1998.
- In November, the FTC announced a proposed settlement with InfoTrax Systems, a third-party service provider, regarding multiple data security failures allegedly resulting in the unauthorized access of end-users' personal information. The proposed settlement is noteworthy in that the FTC alleged a violation of the FTC Act predicated solely upon InfoTrax's failure to maintain reasonable security measures, and the settlement order contains extensive prescriptive requirements regarding improvements that InfoTrax must make to its data security practices.

Over the course of 2019, the FTC has been working to strengthen the injunctive relief imposed in orders in data security cases, such as that imposed in the InfoTrax settlement.

GDPR Enforcement Actions

European regulators are becoming increasingly aggressive in enforcing the General Data Protection Regulation ("GDPR"). In particular, the U.K. Information Commissioner's Office ("ICO") announced headline-grabbing enforcement actions in 2019 related to alleged cybersecurity breaches and data protection violations, reflecting the potentially massive fines that companies are subject to under the GDPR.

While not quite reaching the maximum fine permitted by the GDPR (up to the higher of €20 million or 4% of a company's global turnover), the ICO announced its intention to fine British Airways £183.4 million (\$242.2 million) for a cybersecurity incident resulting in the misappropriation of the personal data of approximately 500,000 British Airways customers. The ICO has not disclosed how it determined the size of this fine, but it amounts to approximately 1.5% of British Airways global turnover. The ICO noted that its investigation revealed that British Airways had "poor security arrangements" in relation to its customers' information.

In July 2019, the ICO published its intention to fine Marriott £99.2 million (\$131 million) for a cybersecurity incident affecting the Starwood guest reservation database starting as early as 2014, but not discovered until 2018. Records relating to about 30 million individuals in the European Economic Area were affected. Like the fine in British Airways, the ICO did not disclose how it calculated the fine, but it appears to amount to approximately 0.6% of Marriott's revenues in 2018.

Separately, European regulators have also engaged in GDPR enforcement related to privacy violations that did not arise out of cybersecurity incidents, unlike that of British Airways and Marriott:

- In January 2019, the French Data Protection Authority ("FDPA") announced a €50 million fine against Google for alleged GDPR violations for not properly disclosing to users how personal data is collected and used across its personalized ads services.
- In October, the Berlin Commissioner for Data Protection & Freedom of Information issued a €14.5 million (\$19.1 million) fine against a German real estate company, die Deutsche Wohnen SE, for its failure to maintain a GDPR-compliant data retention policy and consequently storing tenants' personal information longer than necessary for the purposes for which the data was initially collected. This shows that a seemingly minor offense—over retention of data—can also bring serious penalties.
- In December 2019, the FDPA imposed a €500,000 fine (\$660,000) on Futura Internationale for GDPR violations in connection with cold-calling campaigns. Futura was sanctioned for failing to provide adequate information about or effectively implement current and prospective clients' opt-out requests, among other things.

U.S. State and Federal Legislative Developments

California continues to blaze the trail on U.S. privacy regulation, with its adoption in 2019 of amendments to the Consumer Privacy Act (the "CCPA") and the release of the California Attorney General's implementing regulations. Companies with California customers devoted significant resources to preparing for the CCPA to come into force on January 1, 2020.

Influenced by the E.U.'s GDPR and the CCPA, more and more states are moving towards imposing affirmative cybersecurity and data protection obligations that go beyond data breach notification requirements. The result is that the United States, in the absence of overriding federal legislation, is making the U.S. patchwork of regulation in this area increasingly challenging to manage efficiently.

In addition to significant new privacy and cybersecurity laws in a number of states—including Nevada, Maine, Massachusetts, Maryland, New Jersey, Oregon, Washington, and Texas—New York enacted the Stop Hacks & Improve Electronic Data Security Act (the "SHIELD Act"), which for the first time imposes data security obligations on out-of-state companies that do business with New York residents.

California Consumer Privacy Act

Under the CCPA, California consumers have broad rights to know what personal information has been collected about them, the sources of the 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 statute went into effect on January 1, 2020, and the Attorney General is required to issue final regulations before enforcement actions begin on July 1. Key compliance challenges for many companies have included determining whether their data sharing practices constitute a “sale” of data under the statute, resolving how to give consumers a “notice at collection” for data collected offline, and understanding the scope and impact of certain exemptions, such as the Gramm-Leach-Bliley Act exemption.

Key steps for firms subject to the CCPA in achieving compliance include:

- Updating websites, mobile applications and other locations where consumers’ personal information is collected in order to provide the consumer with a meaningful understanding of the information collected about them, as well as the purposes for which the information will be used. If information is sold (as defined broadly under the CCPA), covered businesses must provide the consumer with a “Do Not Sell My Personal Information” link at the point of collection.
- Updating privacy policies to apply to both online and offline (brick-and-mortar) practices. Privacy policies must detail the categories of information that are collected, the sources of the information, how such information may be used and with whom, as well as the consumers’ rights under the CCPA and how to exercise those rights, including the right to opt out of sale of data and the right to access and delete data. If no notice of the right to opt out of sale is provided, companies must expressly state that they do not and will not sell personal information.
- Updating contracts with vendors that receive personal information to ensure that vendors qualify under certain exceptions to the law (such that sharing information with them does not constitute a “sale”) and collaborate with respect to consumers’ access or deletion requests.
- Training employees who are responsible for handling consumer inquiries about the business’ privacy practices, the requirements of the CCPA, and how to direct consumers to exercise their rights.

Finally, there is an increasing focus on the new California ballot initiative proposed by the activist whose ballot proposal forced the California legislature to adopt the CCPA. The new initiative, slated for the ballot in November 2020 and already garnering wide public support in California, would impose additional restrictions on sensitive health and financial information, and provide stiff penalties for misuse of children’s data.

New York's SHIELD Act

In July, New York enacted the SHIELD Act (Stop Hacks & Improve Electronic Data Security Act), which expanded the state's data breach notification obligations and, for the first time, imposed affirmative cybersecurity obligations on covered entities beyond the financial institutions already covered by the New York Department of Financial Services cybersecurity regulations and affirmative obligations to companies located outside New York.

The principal changes under the SHIELD Act include:

- Expanding the law's jurisdiction to entities that maintain private information of New York residents, regardless of whether or not such entities actually conduct business within the State.
- Broadening the scope of "private information" triggering notification obligations in the event of a breach, including username/password for any online account and biometric data.
- Expanding the definition of "breach" to include unauthorized "access" to private information, in addition to unauthorized acquisition of such information.
- Increasing civil penalties for violations of notification obligations.
- For the first time, affirmatively requiring covered businesses to develop, implement, and maintain "reasonable" data security safeguards, which include, among other things, conducting risk assessments and addressing identified risks.

The first four provisions went into effect in October 2019, while the fifth (requiring companies to adopt and maintain a cybersecurity compliance program) becomes effective on March 21, 2020.

Other U.S. States and the Need for Federal Privacy Legislation

Apart from legislative developments in California and New York, a number of other U.S. states have proposed or enacted privacy and cybersecurity laws. In May 2019, Nevada passed an internet privacy law requiring affected businesses, among other things, to offer consumers the right to opt-out of the sale of their personal data. In June, Maine enacted an internet privacy law that prohibits internet access providers from using, disclosing, selling or permitting access to customers' personal information without express consent.

Meanwhile, a number of other states, including Massachusetts, New Jersey, Maryland, Oregon, Texas and Washington, enacted new laws related to data breach notifications, while Arizona, Connecticut, Florida, Pennsylvania, and others proposed or passed legislation strengthening data privacy protections.

Unless Congress enacts a comprehensive federal privacy scheme that harmonizes the cybersecurity and data privacy landscape, the burdens that businesses face in seeking to comply with this increasingly complex patchwork of state cybersecurity and privacy laws—and the attendant risk of compliance failures—will continue to grow.

Legislative Developments Outside the United States and Europe

China and India each had notable legislative action over the past year. In May 2019, the Cyberspace Administration of China issued draft Measures on Administration of Data Security that, when issued in final form, will constitute binding regulations on network operators who collect, store, transmit, process and use data within Chinese territory.

India is expected to pass a GDPR-inspired data privacy law at some point in 2020 that would require express consent for most uses of an individual's personal data, and allow for individuals to request that their personal information be deleted.

Meanwhile, data protection laws in the Cayman Islands and Bahrain also went into effect during the past year. The Cayman Islands Data Protection Law incorporated many of the same principles as the GDPR. Bahrain's Personal Data Protection Law regulates the collection, processing and storage of individuals' personal data, and sets up a new authority—the Personal Data Protection Authority—charged with investigating violations of the law. Similarly, a new Brazilian data protection law, which mirrors many of the GDPR's concepts, will go into effect in 2020.

U.S. Court Decisions Affecting Data Breach and Privacy Litigation

Privilege-Related Decisions. Corporations should continue to remain vigilant about protecting attorney-client privilege when facing a data breach. It is important that the company's attorneys be involved from the outset in all communications with internal personnel and external advisers involved in investigating and remediating the breach in order to provide advice about the legal ramifications of the attack.

With counsel involved for the purpose of providing legal advice, such communications may be covered by the attorney-client privilege, thereby protecting them from disclosure in any subsequent investigation or litigation. In 2019, there were two notable court decisions that emphasized the need for caution by litigants wishing to raise a defense relying on privileged investigations and reports, including third party reports, or otherwise disclosing the conclusions of such investigations and reports:

- In *Premera Blue Cross Customer Data Security Breach Litigation*, the District Court of Oregon held that a company's early audit and investigation into the cause of a breach—begun prior to engaging counsel—was therefore a necessary business function regardless of litigation, and thus, even documents created subsequent to the hiring of counsel were not privileged. However, the court also held that actions taken in response to the breach were likely guided by advice of counsel and concerns about potential liability and would therefore be privileged.
- In *In re Marriott International Inc. Customer Data Security Breach Litigation*, the District Court of Maryland held that Marriott was required to publicly file its investigation report (which was compiled by a third party) because it had relied on the report's conclusions in its motion to dismiss. Marriott argued that disclosure would allow hackers to “hone their strategies”; but to support its holding, the court noted that the described database was no longer in use. This holding, coupled with the Sixth Circuit's holding in *In re United Shore Financial Services* in 2018, reinforces the importance of having forensic investigators that are retained by companies either prior to or subsequent to a data breach be supervised by counsel, and of maintaining forensic conclusions as confidential, in order to maximize privilege over a data breach investigation.

Data Breach Standing Decisions. In *Spokeo v. Robins*, the Supreme Court held that a plaintiff must allege both a violation of a federal statute and some cognizable real-world harm to establish standing in a privacy case.

In March 2019, the Supreme Court remanded a class action in *Frank v. Gaos*, based on allegations that Google harmed user privacy rights by disclosing search terms to third parties in violation of state law and the federal Stored Communications Act. The Supreme Court directed the lower court to reassess whether the consumers had standing in light of *Spokeo*. Since *Spokeo*, however, the Supreme Court has been silent as to what would constitute a sufficient injury, leaving unresolved a split among the federal circuits as to whether allegations based solely on the risk of future harm are sufficient to establish standing.

As a result, in the event of a data breach where plaintiffs cannot prove their data was used, or in the event of a data exposure where plaintiffs cannot prove their data was accessed, there remains an open question among courts as to when allegations of future harm are too “speculative” to constitute an injury sufficient to meet standing.

Post-Data Breach Securities Class Action Suits. Securities class action suits are now routinely filed by shareholders after the announcement of a data breach. The past year saw numerous such actions filed against the likes of Capital One, FedEx, and Zendesk, among others. Certain notable decisions were reached in the following cases:

- In *Sgarlata v. PayPal Holdings Inc.*, the Northern District of California dismissed the action, holding that plaintiffs had failed to adequately allege that PayPal knew not only of an actual security breach, but also the magnitude of the breach and the type of data accessed.
- In *In re Intel Corporation Securities Litigation*, the Northern District of California dismissed an action based on product security vulnerabilities. The court held that Intel’s statements about chip security and chip performance (for instance, that certain chips were “optimized particularly for data protection” and “have the ability to protect against identity breaches”) constituted nonactionable puffery, and thus were not misleading or false within the meaning of applicable securities law.
- In *In re Equifax Securities Litigation*, the Northern District of Georgia found that plaintiffs had sufficiently alleged that Equifax had misstated the adequacy of its commitment to data security and its compliance with data protection laws. At the same time, the court held that Equifax’s risk factors were not misleading, and Equifax did not have a duty to correct prior misstatements once it became aware of the data breach.
- In *In re Facebook, Inc. Securities Litigation*, the Northern District of California dismissed a shareholder action based on the revelation that Cambridge Analytica had acquired private Facebook user data, and that Facebook had allegedly attempted to suppress evidence of the breach contrary to its policy. The court held that plaintiffs had failed to demonstrate that Facebook ignored red flags concerning Facebook’s data security at the time its officers made statements about its vulnerabilities.

Illinois Biometric Law Litigation. In 2008, Illinois became the first state to implement a comprehensive biometric privacy regime—called the Biometric Information Privacy Act (“BIPA”). While other states have followed suit (e.g., Texas and Washington), Illinois is the only state that provides a private right of action for violations of that law.

In 2019, Illinois state courts decided two cases concerning BIPA:

- In January 2019, the Illinois Supreme Court in *Rosenbach v. Six Flags Entertainment Corp.* held that plaintiffs may bring an action for mere technical violations of BIPA’s disclosure and consent requirements, without additional allegations of actual or threatened injury or damage.

- In April, an appellate court in Illinois held in *Liu v. Four Seasons Hotel Ltd.* that an employee’s allegations of BIPA violations do not constitute allegations of “a wage or hour violation”—which would be subject to arbitration under the applicable employment agreement—even where collection of biometric data is being used to monitor hours worked.

Pennsylvania Rules Employers Have Duty to Guard Employees’ Personal Data. In November 2018, in *Dittman v. UPMC d/b/a The University of Pittsburgh Medical Center*, the Supreme Court of Pennsylvania held that an employer had a legal duty to safeguard its employees’ sensitive personal information, where the employer required that information as a condition of employment and stored that data on an internet-accessible computer.

Dittman is notable because it is the first time a state’s highest court has broadly held that a company owes a duty to protect employees’ personal data that it collects and stores. If the reasoning of *Dittman* is adopted by courts in other states, employers could face increased risk of financial liability following a data breach that compromises personal information of employees.

Takeaways and Predictions for 2020

Last year’s data breaches and other cybersecurity developments reinforce the importance of several issues in mitigating cyber risk:

- To prevent cyber breaches, companies should ensure that they have adequate detection and monitoring policies and take precaution to protect their cybersecurity systems. Facebook’s March 2019 data breach and First American’s exposure of data were both caused by design defects in the companies’ systems, and the FTC’s settlement with InfoTrax was predicated solely upon the company’s failure to maintain reasonable security measures. In addition, an increasing number of jurisdictions—including now New York—are imposing affirmative obligations for companies to maintain adequate cybersecurity compliance programs.

- Companies should take steps in anticipation of post-data breach litigation, including maximizing attorney-client privilege protection, as a flurry of claims are now routinely filed after data breach announcements.

- Given the increasing number of new privacy and cybersecurity laws enacted by states, companies must remain aware of the different (and sometimes conflicting) obligations they face under various state regimes.

Based on developments in 2019, companies can expect authorities in both the United States and internationally to continue their focus on cybersecurity:

- In addition to monetary penalties, enforcement authorities (sometimes acting jointly) will increasingly impose a broad range of undertakings on companies for violations of privacy and cybersecurity laws, including implementation of privacy and cybersecurity risk assessments, third-party monitoring, specified director and officer responsibilities and changes to board composition. This shift is evident from enforcement actions such as Facebook's FTC and Securities & Exchange Commission settlements and Equifax's multi-regulator settlement.
- In 2019, states continued to strengthen their statutory and regulatory cybersecurity regimes, and in doing so, provided new leverage to state attorneys general, who are in turn increasingly empowered by the continuing lack of federal legislation in this area. We expect states to continue to follow California's lead in adopting more comprehensive, GDPR-style privacy laws and remaining active in the enforcement space.
- Meanwhile European regulators are likely to continue to remain aggressive in enforcing the GDPR, especially given the additional regulatory guidance issued this year with respect to the GDPR's territorial reach.
- In 2019, U.S. regulators announced antitrust investigations into the "Big Four" technology companies—Google, Apple, Facebook, and Amazon—with a focus on the potential role of the companies' privacy practices in allegations of anti-competitive behavior. We expect this focus to continue in 2020.
- We expect increased focus on corporate use of facial recognition and biometrics, and new bodies of regulation to address it.
- Apart from standard data breaches and cyberattacks, we expect even more growth in ransomware attacks on companies (use of malicious software to deny access to a computer system or data until a ransom is paid).

The past year was a busy period in cybersecurity and privacy developments. We expect these issues to continue to be a chief concern for in-house counsel, management and boards of directors for the next year and beyond.