ALERT MEMORANDUM

2019 Cybersecurity Developments: A Year in Review

January 31, 2020

Introduction

In 2019, 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 companies have implemented major revisions to their privacy policies and data systems to achieve compliance with California's groundbreaking privacy legislation.

Major data breaches continued to make headlines in 2019, and state and federal legislators, enforcement authorities and regulators 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 are willing to use the GDPR's authorization to levy large fines, even outside the context of major breaches resulting in exposure of customer information.

In this 2019 Year in Review, we highlight the most significant cybersecurity and privacy developments of 2019 and predict key challenges and areas of focus for the coming year.

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

LONDON

James Norris-Jones
+44 20 7614 2336
jnorrisjones@cgsh.com

NEW YORK

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

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

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

PARIS

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

WASHINGTON D.C.

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

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

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 most notable incidents of 2019 included the following:

— The financial industry 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 an software application.

  • In July, Capital One disclosed that a hacker had gained access to personal and financial information for approximately 106 million customers, and 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 wake of two major incidents in 2018, Facebook 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.

  • Facebook suffered further data breaches in April (540 million user records exposed on public Amazon databases), September (more than 419 million user records exposed on a public database), November (approximately 100 third-party developers were improperly granted access to personal user data), and 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 reported 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 and Regulatory Guidance

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,[1] the Federal Trade Commission ("FTC") has taken a more active role in the privacy space, a trend we expect to continue in 2020. We 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 2019, the FTC and Securities and Exchange Commission ("SEC") both announced settlements with Facebook, while the Department of Justice ("DOJ") filed a civil complaint against the company arising from the same circumstances.[2]

  - On July 24, 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 FTC required Facebook to implement remedial measures, including:
    - Establishing a robust privacy and information security program;
    - Appointing a new board subcommittee to serve as an Independent Privacy Committee comprised of independent directors demonstrating certain minimum privacy and data protection capabilities; and
    - An annual certification by Facebook's principal executive officer (CEO Mark Zuckerberg) and a designated compliance officer.
  - That same day, the DOJ filed a complaint against Facebook alleging, among other things, that Facebook violated its 2012 FTC settlement order by providing users with deceptive privacy disclosures and settings; sharing users' personal information with third-party applications used by those users' Facebook friends; and misrepresenting the extent to which users had to opt-in before being subjected to certain facial recognition technology.
  - The next day, the SEC announced a $100 million settlement with Facebook resolving claims that the company's public filings contained misleading statements about the misuse of user data.

— 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 ("CFPB"), 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" based on the company's 2017 breach involving the information of 147 million people. Equifax was required 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.[3]

[1] For further information, see the Cleary Gottlieb "2018 Cybersecurity and Data Privacy Developments: A Year in Review" publication at https://www.clearygottlieb.com/-/media/files/alert-memos-2019/cybersecurity-and-data-privacy-developments--2018-in-review_r1-pdf.pdf.

[2] For further information on this Facebook settlement, see the Cleary Gottlieb "July 2019 Privacy and Cybersecurity Enforcement: Lessons for Management and Directors" publication at https://www.clearycyberwatch.com/2019/08/july-2019-privacy-and-cybersecurity-enforcement-lessons-for-management-and-directors.

[3] For further information on this Equifax settlement, see the Cleary Gottlieb "July 2019 Privacy and Cybersecurity

— In September 2019, 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 2019, the FTC announced a proposed settlement with InfoTrax Systems, L.C., 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 several respects:
    - The FTC alleged a violation of the FTC Act predicated solely upon InfoTrax's failure to maintain reasonable security measures;
    - The settlement order contains extensive prescriptive requirements regarding improvements that InfoTrax must make to its data security practices; and
    - One commissioner filed a concurring statement criticizing the settlement's standard 20-year term as excessively long.[4]

— In July 2019, Cisco Systems reached a $6 million settlement with 19 state Attorneys General to resolve a whistleblower lawsuit under the False Claims Act ("FCA") alleging that the company sold software that was vulnerable to digital attacks. No evidence of any hack or unauthorized access to security systems utilizing Cisco's software was uncovered by the investigation. This was the first successful cybersecurity whistleblower case brought under the FCA.

— The FTC and DOJ announced antitrust investigations into the "Big Four" technology companies (i.e., Facebook, Google, Amazon and Apple) that included aspects of their privacy practices, and multiple state Attorney General investigations similarly targeted a combination of privacy practices and more traditional anti-competitive behaviors.

In addition to these enforcement actions, U.S. federal authorities also issued new cybersecurity guidance:

— Over the course of 2019, the FTC has been working to strengthen the injunctive relief imposed in orders in data security cases.[5]

  - In April 2019, the FTC issued a statement explaining that it was examining the obligations in its orders in data security cases and mandating "new requirements" while "anticipat[ing] further refinements."[6] Thereafter, the FTC ultimately issued seven data security orders with specific data security practices and obligations that differed markedly from past orders.
  - In a recent blog post, Andrew Smith, the director of the FTC's Bureau of Consumer Protection, explained the origin of these efforts and summarized the orders' refinements. Smith acknowledged that FTC data security orders historically "contained fairly standard language," [7] which the Eleventh Circuit stuck down in 2018 as "unenforceably vague" when vacating an FTC cease-and-desist order against

Enforcement: Lessons for Management and Directors" publication at https://www.clearycyberwatch.com/2019/08/july-2019-privacy-and-cybersecurity-enforcement-lessons-for-management-and-directors.

[4] For Cleary Gottlieb's previous blog post discussing the FTC settlement, see https://www.clearycyberwatch.com/2019/11/latest-ftc-data-privacy-settlement-may-signal-more-direct-approach-to-regulating-data-security.

[5] For Cleary Gottlieb's previous blog post discussing the FTC's actions, see https://www.clearycyberwatch.com/2020/01/ftc-summarizes-a-year-of-change-in-its-data-security-orders.

[6] For the FTC's April 2019 statement, see https://www.ftc.gov/system/files/documents/cases/2019-03-19_idressupclixsense_statement_final.pdf.

[7] For the FTC's blog post, see https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance.

LabMD, Inc.[8] After considering the information learned during the December 2018 hearing and the *LabMD* decision, the FTC focused on three areas for change: (1) proscribing "more specific" requirements for data security programs that are tailored to the problems alleged in the complaint; (2) increasing "third-party assessor accountability" and enhancing FTC oversight of assessors; and (3) elevating "data security considerations to the C-Suite and Board level" in the form of senior officer compliance certifications.

— In April 2019, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a Risk Alert addressing privacy-related obligations under Regulation S-P, the primary SEC rule regarding privacy notices and safeguard policies for all registered broker-dealers and investment advisers. The Risk Alert set out the most frequent Regulation S-P deficiencies that OCIE had identified during examinations over the past two years.[9]

— A month later, the OCIE released another cybersecurity-related Risk Alert, this time, highlighting the risks associated with broker-dealers and investment advisors storing customers records and information in the cloud and on other types of network storage solutions.[10]

— In early January of 2020, the SEC issued the OCIE's 2020 Examination Priorities, which highlighted that the OCIE will continue to prioritize information security in its examination programs.[11]

GDPR Enforcement Actions and Guidance

Developments in the General Data Protection Regulation

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 [12]:

— 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 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 for a cybersecurity incident affecting the Starwood guest reservation

[8] *LabMD, Inc. v. Fed. Trade Comm'n*, No. 16-16270, 2018 WL 2714747, at *1 (11th Cir. 2018).
[9] For Cleary Gottlieb's previous blog post discussing the SEC's Regulation S-P Risk Alert, see https://www.clearycyberwatch.com/2019/05/sec-privacy-risk-alert-may-foreshadow-upcoming-reg-s-p-enforcement-against-broker-dealers-investment-advisers.
[10] This alert and the SEC's Regulation S-P Risk Alert are the latest in a series of recent privacy and cybersecurity guidance documents issued by the SEC, including the SEC's February 2018 Commission Statement and Guidance on Public Company Cybersecurity Disclosures and October 2018 Report of Investigation on cyber-related frauds and public company accounting controls.
[11] For Cleary Gottlieb's previous blog post discussing the SEC OCIE's 2020 Examination Priorities, see https://www.clearycyberwatch.com/2020/01/from-the-expected-to-the-surprises-highlights-of-sec-ocies-2020-priorities.
[12] For further information, see the Cleary Gottlieb "Selected Issues for Boards of Directors in 2020" publication (Cybersecurity: What Keeps Us Up at Night) at https://www.clearycyberwatch.com/2020/01/cybersecurity-what-keeps-us-up-at-night.

database starting as early as 2014—notably, before Marriott acquired Starwood in 2016—but not discovered until 2018. Records relating to about 30 million individuals in the European Economic Area ("EEA") were affected—7 million of which were related to individuals in the United Kingdom. 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 allegedly not properly disclosing to users how personal data is collected and used across its personalized ads services.[13]

— In October 2019, the Berlin Commissioner for Data Protection and Freedom of Information issued a €14.5 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.[14]

— In December 2019, the FDPA imposed a €500,000 fine on Futura Internationale for GDPR violations in connection with cold-calling campaigns. Futura Internationale was sanctioned for failing to provide adequate information about or effectively implement current and prospective clients' opt-out requests, among other things.[15]

Over the course of 2019, European authorities have provided further guidance on the application and interpretation of the GDPR:

— *Administrative Arrangements for Sharing Data.* On February 12, 2019, the European Data Protection Board ("EDPB") issued its first opinion on "administrative arrangements" between European Union ("EU") financial supervisory authorities and securities agencies and their non-EU counterparts. Such "administrative arrangements" permit personal data to be transferred from public authorities in Europe to those of third countries.[16] In assessing the adequacy of an administrative arrangement, the EDPB highlighted the following factors, among others: whether the administrative arrangement accurately reflects the GDPR's key data protection definitions and concepts; whether the financial supervisory authorities retain personal data only for as long as is necessary for the relevant purpose; whether the administrative arrangement is predicated on the idea that the relevant financial supervisory authorities have specific responsibilities and regulatory mandates; that adequate notice is provided to data subjects; and

[13] For Cleary Gottlieb's previous blog post discussing the FDPA's fine against Google, see https://www.clearygottlieb.com/news-and-insights/publication-listing/the-evolving-privacy-landscape-at-a-glance-compliance-considerations-for-a-new-decade.

[14] For Cleary Gottlieb's previous blog post discussing the Berlin Commissioner for Data Protection and Freedom of Information's fine against die Deutsche Wohnen SE, see https://www.clearygottlieb.com/news-and-insights/publication-listing/the-evolving-privacy-landscape-at-a-glance-compliance-considerations-for-a-new-decade.

[15] For Cleary Gottlieb's previous blog post discussing the FDPA's fine against Futura Internationale, see https://www.clearycyberwatch.com/2019/12/french-regulator-fines-futura-internationale-e500000-for-infringements-of-the-gdpr-in-connection-with-telephone-advertising-campaigns.

[16] Under the GDPR, personal data cannot be transferred from the EEA to a third country unless the European Commission has decided that the data protection laws of such third country are "adequate," or unless "appropriate safeguards" are in place to ensure that the treatment of personal data in the hands of the recipient reflects the GDPR's high standards.

that transfers may only take place within the framework of such mandates.[17]

— *Territorial Scope.* On November 14, 2019, the EDPB adopted the final version of the guidelines on the GDPR's territorial scope. As compared to the draft version of the guidelines,[18] the final version clarified a number of open questions, including that the presence of an employee in the EU, or the inadvertent or incidental offering of goods or services to non-EU individuals in the EU, will not suffice to mandate application of the GDPR. Thus, the fact that some of an organization's data processing activities fall within the GDPR's scope will not mean that all of the organization's processing activities will do so.

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. More and more states are moving towards imposing affirmative cybersecurity and data protection obligations that go beyond data breach notification requirements, 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 states such as Nevada, Maine, Massachusetts, Maryland, New Jersey, Oregon, Washington, and Texas, New York enacted the Stop Hacks and 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.

CCPA

Under the CCPA, California consumers have broad rights to know what personal information has been collected about them, the sources for 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. For our analyses of the CCPA's requirements and key interpretive issues, see our alerts here and here.[19]

In October, California passed several amendments to the CCPA and the California Attorney General issued long-awaited proposed implementing regulations. The amendments provided temporary relief on application of certain core CCPA requirements to employee information and information collected in certain business-to-business ("B2B") contexts.

The statute went into effect on January 1, 2020; by July 2020, the Attorney General is required to issue final regulations and enforcement actions can begin starting July 1. One of many questions that remains unclear and contested is whether the Attorney General can and will bring actions based on any non-compliance during the period from January 1 to July 1, 2020. 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 (e.g., the Gramm-Leach-Bliley Act

[17] For Cleary Gottlieb's previous blog post on the EDPB's guidance on administrative arrangements under the GDPR, see https://www.clearycyberwatch.com/2019/03/edpb-issues-first-opinion-on-administrative-arrangements-under-the-gdpr-for-cross-border-data-flows-between-eu-and-non-eu-securities-agencies.

[18] For Cleary's previous blog post on the EDPB's draft guidelines on the GDPR's territorial scope, see https://www.clearycyberwatch.com/2019/01/edpb-publishes-draft-guidelines-territorial-scope-gdpr.

[19] For Cleary Gottlieb's previous blog posts discussing the CCPA amendments, see https://www.clearygottlieb.com/-/media/files/alert-memos-2019/california-consumer-privacy-act-amendments-offer-relief.pdf, and https://www.clearygottlieb.com/news-and-insights/publication-listing/the-evolving-privacy-landscape-at-a-glance-compliance-considerations-for-a-new-decade.

exemption and the temporary employee and B2B exemptions).

Firms subject to the CCPA[20] faced challenges in 2019 working towards compliance with substantial new obligations on a short time frame, with significant interpretive uncertainty in some areas. Key steps for achieving January 1, 2020 compliance included:

— Updating websites, mobile applications and other locations where consumers' personal information is collected in order to provide the consumer with meaningful understanding of the information collected about them at or before collection, 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 your vendors qualify under certain exceptions under 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 your business' privacy practices, the requirements of the CCPA and how to direct consumers to exercise their rights.
— Implementing methods for complying with consumers' exercise of the rights granted by the CCPA, including:

- Designating an official contact for questions about your company's privacy policies;
- Offering two or more designated methods for receiving consumer requests under the CCPA;
- Establishing, documenting and complying with a method for verifying that the person making a request for access or deletion is indeed the subject consumer;
- Ensuring your business can identify an individual consumer's data to provide that individual with access to that data, delete it from your records or remove such data from data sets that are sold to third parties.

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, which expanded 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

[20] In general, the CCPA's provisions apply to any entity doing business in California that meets one of the following thresholds: (i) it has annual gross revenues in excess of $25 million; (ii) it annually buys, receives for its commercial purposes, sells, or shares for commercial purposes personal information relating to 50,000 or more consumers, households, or devices; or (iii) it derives 50% or more of its annual revenue from selling consumer personal information. *See* Cal. Civ. Code § 1798.140.

regulations and to companies located outside New York.[21]

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; and

— 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 on October 23, 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 2019. In May, 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, among other things, prohibits internet access providers from using, disclosing, selling or permitting access to customers' personal information without express consent to that use, disclosure, sale or access. Meanwhile, 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 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.[22] 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[23] also went into effect in 2019. The Cayman Islands Data Protection Law went into effect on September 30, 2019, and incorporated many of the same principles as the GDPR. Bahrain's Personal Data Protection Law, which went into effect

[21] For Cleary Gottlieb's previous blog post on the New York SHIELD Act, see https://www.clearygottlieb.com/-/media/files/alert-memos-2019/new-york-passes-expansive-new-cybersecurity-law.pdf.

[22] For Cleary Gottlieb's previous blog post discussing recent Chinese and Indian legislative action in the data privacy field, see https://www.clearygottlieb.com/news-and-insights/publication-listing/the-evolving-privacy-landscape-at-a-glance-compliance-considerations-for-a-new-decade.

[23] For Cleary Gottlieb's previous blog post discussing recent Bahrain legislative action in the data privacy field, see https://www.clearygottlieb.com/news-and-insights/publication-listing/key-data-protection-considerations-bod-2019.

on August 1, 2019, 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 (the *Lei Geral de Proteção de Dados Pessoais*) that mirrors many of the GDPR's concepts will go into effect in 2020.[24]

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

Privilege-Related Decisions

Corporations should continue to remain vigilant about protecting 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.[25]

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*,[26] 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*,[27] 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, LLC* in 2018,[28] 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*,[29] 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.

[24] For Cleary Gottlieb's previous blog post discussing recent Brazil legislative action in the data privacy field, see https://www.clearygottlieb.com/news-and-insights/publication-listing/key-data-protection-considerations-bod-2019.

[25] For further information, see the Cleary Gottlieb "2018 Cybersecurity and Data Privacy Developments: A Year in Review" publication at https://www.clearygottlieb.com/-/media/files/alert-memos-2019/cybersecurity-and-data-privacy-developments--2018-in-review_r1-pdf.pdf.

[26] 329 F.R.D. 656, 666-67 (D. Or. 2019).

[27] No. 8:19-MD-2879-PWG (D. Md. Aug. 30, 2019), ECF No. 418.

[28] In 2018, the Sixth Circuit in *In re United Shore Financial Services, LLC*, No. 17-2290, 2018 WL 2883893 (6th Cir. Jan. 3, 2018) 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 defense based on the investigative conclusions.

[29] 136 S. Ct. 1540 (2016).

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*.[30] However, since *Spokeo*, 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.[31]

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. 2019 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.*,[32] 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*,[33] 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*,[34] 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*,[35] 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

[30] No. 17-961, 2019 WL 1264582 (Mar. 20, 2019) (per curiam). The Northern District of California has yet to rule on the issue presented in *Spokeo*. For Cleary Gottlieb's previous blog post discussing the *Frank v. Gaos* decision, see https://www.clearycyberwatch.com/2019/04/supreme-court-vacates-approval-of-class-action-settlement-and-remands-to-determine-article-iii-standing-in-data-privacy-case.

[31] The Second, Fourth, and Eighth Circuits have determined that such allegations are insufficient. By contrast, the D.C., Third, Sixth, Seventh, Ninth, and Eleventh Circuits have determined that allegations about a substantial risk of future harm are sufficient.

[32] No. 17-CV-06956-EMC, 2019 WL 4479562 (N.D. Cal. Sept. 18, 2019). For Cleary Gottlieb's previous blog post discussing the *Sgarlata v. PayPal Holdings, Inc.* case, see https://www.clearycyberwatch.com/2019/01/california-district-court-dismisses-securities-class-action-plaintiffs-failed-plead-paypal-knew-magnitude-security-breach.

[33] No. 18-CV-00507-YGR, 2019 WL 1427660 (N.D. Cal. Mar. 29, 2019).

[34] 357 F. Supp. 3d 1189 (N.D. Ga. 2019).

[35] No. 18-CV-01725-EJD, 2019 WL 4674347 (N.D. Cal. Sept. 25, 2019).

security at the time its officers made statements about its vulnerabilities.

Illinois Biometric Law Litigation

In 2008, Illinois was 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:

— On January 25, 2019, the Illinois Supreme Court in *Rosenbach v. Six Flags Entertainment Corp.*,[36] 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.

— On April 9, 2019, an appellate court in Illinois held in *Liu v. Four Seasons Hotel, Ltd.*[37] 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

On November 21, 2018, in *Dittman v. UPMC d/b/a The University of Pittsburgh Medical Center*,[38] 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 any 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.

2019 Takeaways and Predictions for 2020

According to the Association of Corporate Counsel's Chief Legal Officers 2019 Survey, cybersecurity issues remain top of mind, with 68% of CLOs ranking data breaches and protection of corporate data as "extremely important" or "very important."[39] 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 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 Systems was predicated solely upon the company's failure to maintain reasonable security measures. In addition, an increasing number of jurisdictions—including now New

[36] 129 N.E.3d 1197 (Ill. 2019). For Cleary Gottlieb's previous blog post discussing the *Rosenbach v. Six Flags Entertainment Corp.* case, see https://www.clearycyberwatch.com/2019/02/illinois-supreme-court-rules-plaintiffs-not-required-allege-actual-injury-sue-biometric-information-privacy-act.

[37] No. 18-2645, 2019 WL 1560416 (App. Ct. Ill. Ap. 9. 2019). For Cleary Gottlieb's previous blog post discussing the *Liu v. Four Seasons Hotel, Ltd.* case, see https://www.clearycyberwatch.com/2019/05/illinois-appellate-court-holds-employee-biometric-privacy-claims-are-independent-of-wage-and-hour-disputes.

[38] 196 A.3d 1036 (Pa. 2018). For Cleary Gottlieb's previous blog post discussing the *Dittman* case, see https://www.clearycyberwatch.com/2019/01/pennsylvanias-highest-court-rules-employers-duty-guard-employees-personal-data.

[39] In addition, 65% of CLOs ranked information privacy as "extremely important" or "very important." For the Association of Corporate Counsel's Chief Legal Officers 2019 Survey, see https://www.acc.com/sites/default/files/resources/upload/2019-ACC-Chief-Legal-Officers-Survey.pdf.

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 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 both enforcement actions such as Facebook's FTC and SEC settlements and Equifax's multi-regulator settlement, and the FTC's April 2019 public statements on this topic.

— 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, 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.[40]

— 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).

2019 was a busy year 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.

…

CLEARY GOTTLIEB

[40] Indeed, just before publication of this memorandum, Facebook announced a $550 million settlement to end a class action lawsuit alleging violations of Illinois's biometric privacy law in connection with its use of facial recognition software in photographs.