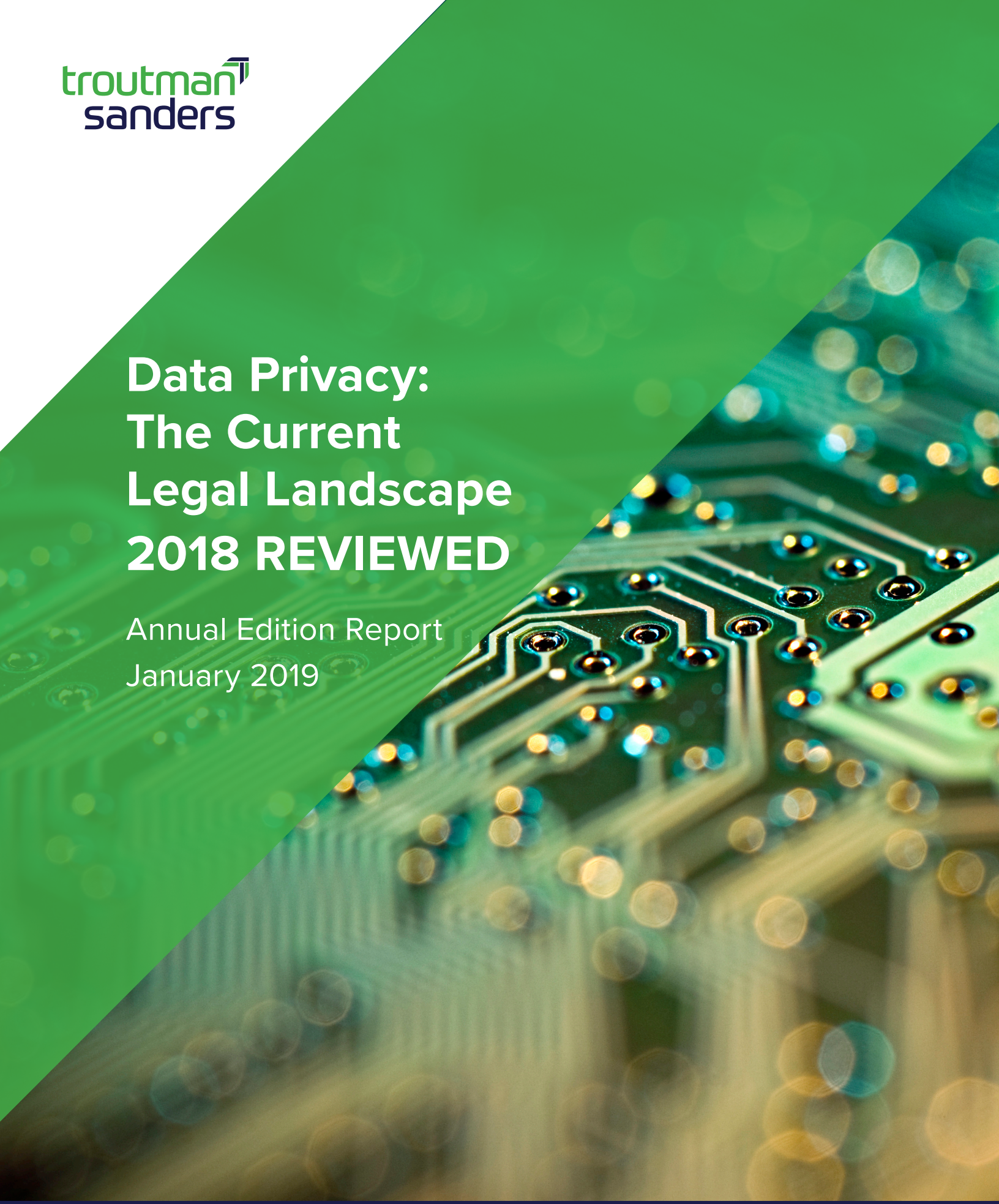
troutman sanders

# Data Privacy: The Current Legal Landscape 2018 REVIEWED

Annual Edition Report

January 2019



# DATA PRIVACY: THE CURRENT LEGAL LANDSCAPE (2018 REVIEWED)

**(Annual Edition Report, January 2019)**

By Mark Mao, Ronald Raether, Sheila Pham, Yanni Lin, Sadia Mirza, Stacy Hovan, Oscar Figueroa, Katharine Malone, Julie Hoffmeister, Molly DiRago, Timothy Butler, Jonathan Yee, and Dan Waltz

**I. Introduction – Why Data-Based Products Are Our Future**

**II. New Legislation, Regulations, and Industry Guidance**

A. The Economic Growth, Regulatory Relief, and Consumer Protection Act

B. Federal Regulations

1. The SEC's "Statement and Guidance on Public Company Cybersecurity Disclosures"
2. The Commerce Department's Likely Promulgation of Export Controls for "Emerging Technologies"
3. Department of Health and Human Service's "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients"

C. Changes and Updates to State Breach Statutes

D. General State Legislation on Data Privacy

1. California's Consumer Privacy Act
2. Vermont's Data Broker and Consumer Protection Legislation
3. Ohio's Senate Bill 18-220
4. California's Senate Bill 18-327
5. Summary of General Cybersecurity Laws Across Different States

E. Local Laws and Initiatives

F. The Fight over Data Privacy Regulations in Broadband

G. The NIST Prepares for a More Connected World

1. The NIST Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations*
2. The NIST Cybersecurity Framework Smart Grid Profile

**III. Evolving Case Law**

A. Data Breach Litigation: Beyond *Spokeo*

1. Consumer Breach Litigation: Moving on to 12(b)(6) Motions
2. Business-to-Business Breach Litigation: Split Circuits

B. Data Misuse Litigation: Where Technicalities Matter

1. Cases Involving Online Tracking and Aggregation
2. Cases Involving Mobile Device Tracking and Aggregation
3. Cases Involving IoT and Emerging Technologies

C. Product Liability Litigation

D. Securities Litigation

**IV. Developments in Regulatory Enforcement**

A. The Federal Trade Commission

B. HIPAA Enforcement

C. State AG Enforcement

D. Other Administrative Enforcement Efforts

**V. Notable International Developments**

A. Developments in the EU Regarding the GDPR and Privacy Class Actions

B. New Privacy Legislation under Consideration in China

C. "Meaningful Consent" Guidance in Canada

**VI. Contacts**

# I. INTRODUCTION – WHY DATA-BASED PRODUCTS ARE OUR FUTURE

Since the European Union ("EU") adopted Article 29 in 1997, a debate has raged over which side of the pond has the better approach to privacy. We have written several articles over the past 21 years discussing the merits of each side. In the last few years, a push to adopt EU-like policies has intensified the debate in the United States and created more public awareness of the issues. Although the conversation on this side of the pond has not been nearly as draconian as the views in Europe, some American "consumer advocates" view data collection as being intrusive and offensive without understanding the key factors driving the debate.

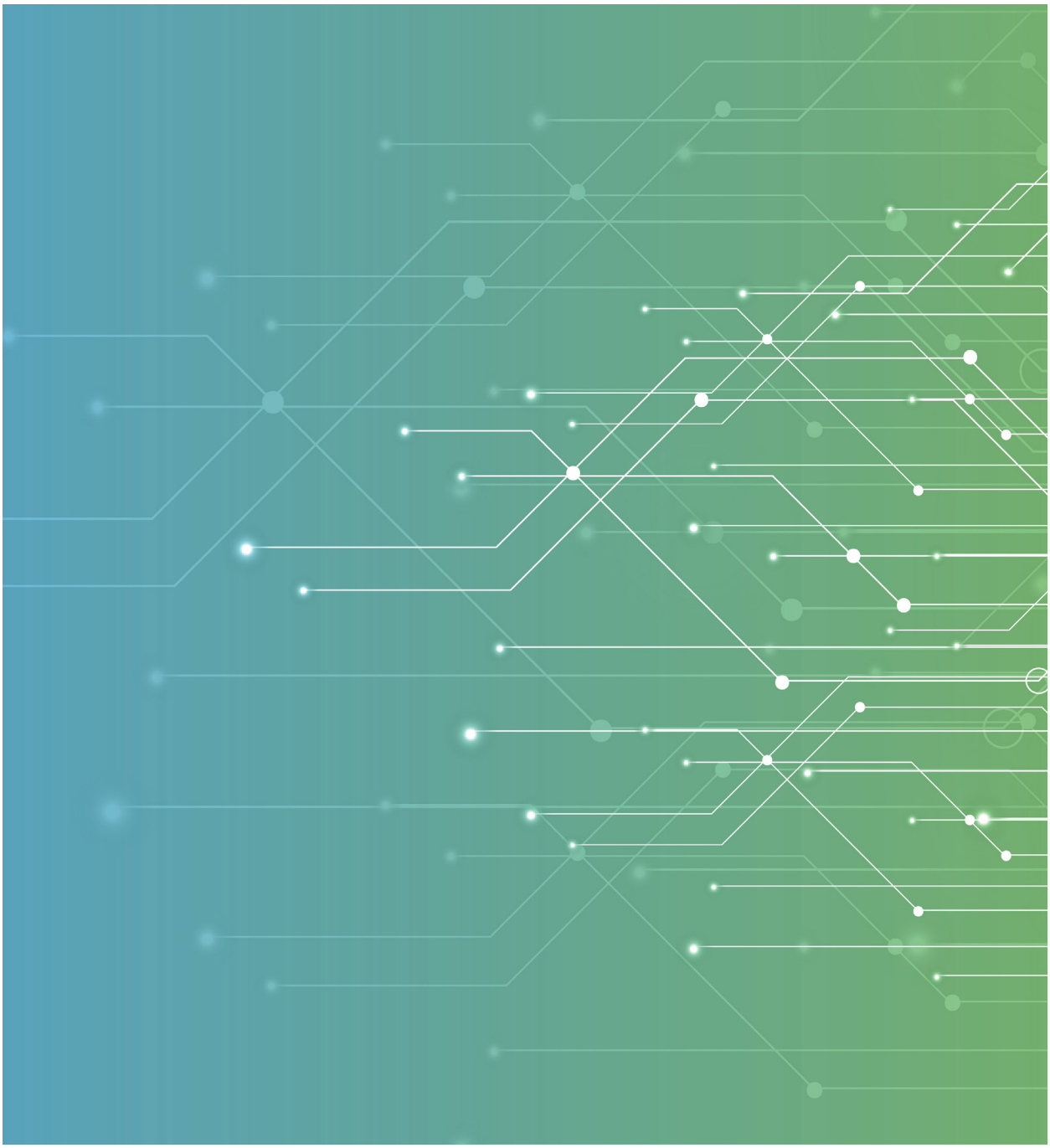
One issue at the center of this long debate is the balance between using the right privacy tools and enabling business and technological innovation. The current criticisms fail to appreciate that the next technological paradigm is completely dependent on both the quality and quantity of data. As connected things ("Internet of Things" or "IoT") explode in popularity, they make new technologies such as augmented reality ("AR") and autonomous vehicles possible. Indeed, data scientists have repeatedly observed that machine learning and artificial intelligence are heavily dependent on the quality of the data, and not just the quantity of data. Where real-time data is available across a wide variety of different product types across everyday life, they enable AR and automation that more reliably improves the human user experience. In realizing these goals, businesses must also adopt privacy compliance regimes that promote good data hygiene and constructive use of data. Such systems must ultimately involve consumer participation.

*Given the lack of clear regulation and guidance, companies will likely continue to collect, use, and share geolocation and other user data.*

The functionality demanded by consumers will require such data. As interconnectivity grows, so do the opportunities to develop better products, and the companies that fail to leverage those opportunities may find themselves falling behind their competitors. Companies developing products on the cutting edge of technology should stay informed of recent enforcement actions, legal cases, and laws to determine how their offerings within the ecosystem may be impacted. Ultimately, the need for in-depth privacy by design and defense will continue to be a differentiator in the market and a key indicator of long term financial success.

Our vision is not just focused on U.S.-centric requirements, but also global requirements. U.S. companies whose data collection practices may impact EU residents now face heavy fines for non-compliance with the European Union's Global Data Protection Regulation ("GDPR"), which went into effect on May 25, 2018. Since then, the effects of the GDPR could not be more pronounced. In its wake, several U.S. states and cities followed with their own versions of legislation and proposals that capture elements of the GDPR. It is just a matter of time until these state initiatives begin to unnecessarily complicate the data use landscape. Although similar to what we have experienced since 2005 with data breach requirements, these state-focused regulations on privacy will likely prove to be even more disruptive.

It remains to be seen whether localized efforts in the U.S. will create enough momentum to help push through a serious federal proposal. Data breach laws and cybersecurity requirements, for example, are more fragmented amongst the states as ever. Ironically, the efforts already made by states in lieu of federal regulation might become some of the biggest obstacles against a truly comprehensive federal regulation. Businesses yet to implement sound data governance practices should take immediate action before compliance becomes a business impossibility.



# II. NEW LEGISLATION, REGULATIONS, AND INDUSTRY GUIDANCE

## A. THE ECONOMIC GROWTH, REGULATORY RELIEF, AND CONSUMER PROTECTION ACT

Partly in response to large breaches involving national credit bureaus, Congress passed the Economic Growth, Regulatory Relief, and Consumer Protection Act in May 2018. In addition to several other changes that affected financial institutions, the Act provides that consumer reporting agencies, as defined by section 1681a(p) of the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq*. ("FCRA"), must allow consumers to request free and unlimited national credit freezes and unfreezes for a minimum of one year.[1] In September 2018, the Consumer Financial Protection Bureau ("CFPB") issued updated FCRA model notices and forms to reflect these changes.[2]

Following this Act, it will be interesting to see whether plaintiffs in data breach class actions will be able to plausibly argue that fraudulent accounts continued to be opened in their names after they were provided with a breach notification. The Act may also create individualized issues for plaintiffs seeking class certification.

## B. FEDERAL REGULATIONS

### 1. The SEC'S "Statement And Guidance On Public Company Cybersecurity Disclosures"

On February 21, 2018, the U.S. Securities and Exchange Commission ("SEC") issued its "Commission Statement and Guidance on Public Company Cybersecurity Disclosures."[3] The SEC noted that while its prior guidance led to general disclosures discussing "risk factors," the SEC wanted to "expand and clarify" prior guidance by explaining "the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context."[4]

Although some have criticized the guidance as not going far enough and merely reiterating prior SEC staff views,[5] a close analysis of the new guidance shows that the SEC is becoming increasingly aggressive regarding cybersecurity. The guidance also clarifies several open issues from prior SEC guidance by providing specifics on what disclosures and controls should be made.

**Material Disclosures**

Specifically, with regard to the timing of material disclosures, the SEC indicates that cybersecurity events may need to be disclosed in periodic reports such as Form 10-Ks and Form 10-Qs to avoid misleading statements for the purposes of the Securities Act of 1933 (the "Securities Act") and the Securities Exchange Act of 1934 (the "Exchange Act"). In addition, the SEC suggests that companies may want to consider using Form 8-Ks and Form 6-Ks to issue current reports to disclose cybersecurity events "promptly" to "maintain the accuracy and completeness of effective shelf registration statements."[6]

In terms of the scope of disclosure, the SEC indicates that "[t]he materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to

1 Lisa Weintraub Schifferle, *Free Credit Freezes Coming Soon*, FTC (Jun. 7 2018), https://www.consumer.ftc.gov/blog/2018/06/free-credit-freezes-are-coming-soon-0.

2 *Bureau of Consumer Financial Protection Issues Updated FCRA Model Disclosures*, CFPB (Sept. 12, 2018), https://www.consumerfinance.gov/about-us/newsroom/bureau-consumer-financial-protection-issues-updated-fcra-model-disclosures/.

3 17 CFR parts 229, 249; SEC Release Nos. 33-10459; 34-82746, available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf.

4 *Id.* at 6.

5 Andrea Vittorio, *Companies Get New SEC Direction on Cyber Issues as Hacks Mount*, BLOOMBERG BNA (Feb. 21, 2018), available at: https://www.bna.com/companies-new-sec-n57982089038/.

6 SEC Release Nos. 33-10459; 34-82746, p. 9-10.

any compromised information for the business and scope of company operations." Whether something is material can include whether it may cause "harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities."[7] Although the Commission indicates that it understands that "a company may require time to discern the implications of a cybersecurity incident" and that the company may still need to "cooperate with law enforcement," such ongoing internal or external investigations "would not on its own provide a basis for avoiding disclosure of a material cybersecurity event." If a prior disclosure is incomplete or inaccurate, the SEC suggests that the company may want to consider whether an update or correction should be made.[8]

**Disclosure of Risk Factors**

In the guidance, the SEC also discussed Item 503(c) of Regulation S-K and Item 3.D of Form 20-F, which require companies to disclose factors that may make investments in securities speculative or risky. Notably, the SEC suggests that companies should consider disclosing:

- Prior cybersecurity incidents, including their severity and frequency;
- The probability of the occurrence and the potential magnitude of cybersecurity incidents;
- The adequacy of preventative measures taken, including any limitations;
- Third-party supplier and service provider risks;
- Potential for reputational harm;
- Litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents; and
- Available insurance coverage.

Importantly, the SEC clarified that general discussions of these topics just in terms of "risk factors" may not be sufficient, and instead, "companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of these risks in the appropriate context." In addition, "[p]ast incidents involving suppliers, customers, competitors, and others may be relevant when crafting risk factor disclosure."[9]

In discussing Item 103 of Regulation S-K, which requires companies to disclose information relating to material pending legal proceedings, the SEC notes that companies may need to disclose cybersecurity litigation, "including the name of the court in which the proceedings are pending, the date the proceedings are instituted, the principal parties thereto, a description of the factual basis alleged to underlie the litigation, and the relief sought."[10]

**Management, Controls and Procedures**

With regard to company oversight on cybersecurity, the SEC states that "[a] company must include a description [in its disclosures required by Item 407(h) of Regulation S-K] of how the board administers its risk oversight function."[11]

And in response to recent public outrage concerning insider trading based on undisclosed cybersecurity events, the SEC provides that "[c]ompanies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications to facilitate policies and procedures designed to prohibit directors, officers, and other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents."[12]

7 *Id.* at 10-11.

8 *Id.* at 11-12.

9 *Id.* at 13-14.

10 *Id.* at 16.

11 *Id.* at 18.

12 *Id.* at 18-19.

*Although some have criticized the SEC for not going far enough with promoting better cyber disclosures,[13] the February 2018 guidance is surprisingly aggressive in some of the SEC's recommendation and views.*

Companies may experience substantial difficulty following some of the new suggestions, such as providing increased granularity on existing and ongoing cybersecurity investigations, which are often uncertain and inconclusive.

Nonetheless, such disclosures should still be drafted carefully. Up until the last two years, plaintiffs filing securities litigation based on data breaches have had no success. In 2018, however, at least two large securities litigations arising from data breaches have settled to date.[14]

**2. The Commerce Department's Likely Promulgation of Export Controls for "Emerging Technologies"**

On November 19, 2018, the Commerce Department's Bureau of Industry and Security published an advance notice of proposed rulemaking ("ANPRM") in the Federal Register seeking public comment on criteria for identifying and defining "emerging technologies" essential to U.S. national security.[15] Although the request for comments solicited by the ANPRM states that its purpose is to prevent terrorist applications of emerging technologies, the protectionism desired by the current Trump Administration also clearly played a part.

The eventual outcome of the ANPRM will likely have substantial effects on organizations involved in the development and provision of data-based products and services. A number of technologies flagged in the ANPRM have primarily consumer-facing applications going beyond technologies that can clearly be used to the detriment of our national security.

- Position, navigation, and timing technologies;
- Advanced surveillance technologies, such as faceprint and voiceprint;
- Artificial intelligence and machine learning technology, including those involved in computer vision, speech and audio processing, and natural language learning and processing;
- Data analytics technologies, including those used for visualization, contextualization, and automated analysis algorithms;
- Brain-computer interfaces;
- Quantum computing, encryption, and sensing technologies;
- Robotics, particularly mini-drone and molecular robots; and
- Additive manufacturing, such as 3D printing.

The above-referenced list is not exhaustive. We expect a revised list later in 2019, and the public will have another opportunity to make comments. The current China-U.S. trade war will likely play part in the revision and finalization of this list.

Notably, these "emerging technologies" will likely be part of the "critical technologies" subject to a separate Trump Administration initiative to examine foreign investments.[17]

**3. Department of Health and Human Service's "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients"**

[13] Andrea Vittorio, *Companies Get New SEC Direction on Cyber Issues as Hacks Mount*, BLOOMBERG BNA (Feb. 21, 2018), https://www.bna.com/companies-new-sec-n57982089038/.

[14] *See* Hayley Fowler, *Yahoo Gets Green Light On $80M Investor Data Breach Deal*, LAW360 (May 10, 2018), https://www.law360.com/articles/1042356/yahoo-gets-green-light-on-80m-investor-data-breach-deal; Kat Greene, *Wendy's Strikes Deal In Data Breach Shareholder Row*, LAW360 (May 8, 2018), https://www.law360.com/articles/1040982/wendy-s-strikes-deal-in-data-breach-shareholder-row.

[15] 14 CFR Part 744 (Nov. 19, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-11-19/pdf/2018-25221.pdf.

[16] Georgi et al., *Commerce Department Requests Public Comments For Emerging Technologies' Export Controls* (Arent Fox, Nov. 21, 2018), https://www.arentfox.com/perspectives/alerts/commerce-department-requests-public-comments-emerging-technologies-export.

[17] See 31 CFR 801.204(f).

On December 28, the Department of Health and Human Services (HHS) released a set of guidance entitled, "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients."[18] The four volume set, albeit voluntary, provide meaningful examples of what it means to comply with National Institute of Standards and Technologies (NIST) standards, which is what the HHS still states that good cybersecurity practices should map to.

For its third volume for "medium and large health care organizations," the HHS lists ten areas where it provides for suggestions on methodologies and "best practices":

- E-mail protection systems;
- Endpoint protection systems;
- Identity and access management;
- Data protection and loss prevention;
- IT asset management;
- Network management;
- Vulnerability management;
- Security operations center and incident response;
- Medical device security;
- Cybersecurity systems.[20]

Because health organizations tend to react slower to technological change, the models proposed are understandably more static than the newer models pushed for by more recent NIST publications, which plan for a much more connected and dynamic environment. Nonetheless, as with our recommendations regarding the NIST publications, it will be wise for organizations covered by these publications to have documentation showing review, thorough self-assessment, and responsive changes made. A history of documentation alone may save the day, in response to any future regulatory inquiry.

## C. CHANGES AND UPDATES TO STATE BREACH STATUTES

For the first time, all 50 U.S. states have data breach statutes. Below is our compendium of updates for 2018:

**Alabama:** On March 28, 2018, Alabama enacted its data breach notification law, which went into effect on June 1, 2018.[21] Key provisions include:

- Defining "breach of security" or "breach" as the "unauthorized acquisition of data in electronic form containing sensitive personally identifying information."
- Defining "sensitive personally identifying information" as including a resident's first name or first initial and last name in combination with a non-truncated Social Security number or tax identification number, a non-truncated driver's license number or other unique government identification number, a financial account number in combination with any code necessary to access the financial account or conduct a transaction that will credit or debit the financial account, health information, as well as username or email address in combination with a password or security question and answer that would permit access to an online account likely to contain sensitive personally identifying information.
- Requiring that notice be provided no later than 45 days from receipt of notice of a breach or determination that a breach has occurred.

**Arizona:** On April 11, 2018, Arizona revised its data breach notification law, which became effective on August 3, 2018.[22] Key changes include:

- Expanding the definition of "personal information" to also include an individual's username or email

[18] Grande, *Health Cybersecurity Guide Could Redefine Reasonable* (Law360, Jan. 3, 2019), https://www.law360.com/cybersecurity-privacy/articles/1114600/health-cybersecurity-guide-could-redefine-reasonable-?nl_pk=d100b429-aa27-499d-ad44-acee4f8fe74b&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy.

[19] See HHS website at: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html (referencing multiple NIST publications).

[20] *Technical Volume 2: Cybersecurity Practices For Medium And Large Health Care Organizations* (HHS 2018), https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf.

[20] Alabama Data Breach Notification Act of 2018, SB318, 2018 Sess. (AL 2018), http://arc-sos.state.al.us/PAC/SOSACPDF.001/A0012674.PDF.

[22] *New Arizona Law to Protect Data Breach Victims*, ARIZ. ATT'Y GEN., available at: https://www.azag.gov/press-release/new-arizona-law-protect-data-breach-victims (last visited Sept. 17, 2018).

address, in combination with information that allows access to an online account, and to include as specified data elements in combination with first name or first initial and last name, and either: unique private key used to authenticate or sign an electronic record, health insurance identification number, medical or mental health information, passport number, taxpayer identification number or other number issued by the IRS, or biometric data used to authenticate an individual when accessing an account.

- Establishing that notification must occur within 45 days of determination of security breach.
- Adding that if breach requires notification of more than 1,000 individuals, to also notify the three largest nationwide consumer reporting agencies and the Attorney General, unless an independent third-party forensic auditor or law enforcement agency determines, after a reasonable investigation, that a security breach has not resulted in or is not reasonably likely to result in substantial economic loss to affected individuals.
- Granting power to the Attorney General to enforce a violation of the statute not to exceed lesser of $10,000 per affected individual or the total amount of economic loss sustained by affected individuals. A knowing and willful violation of the statute is an unlawful practice.

**Colorado:** On May 29, 2018, Colorado revised its data breach statute, which became effective on September 1, 2018.[23] Key changes include:

- Expanding the definition of "personal information" to also include the following data points in combination with first name or first initial and last name: student, military, or passport identification number; medical information; health insurance identification number; or biometric data. "Personal information" was also expanded to include a Colorado resident's username or email address in combination with information that would permit access to an online account or a Colorado resident's account number or credit card number in combination with any information that would permit access to that account.
- Establishing that notification to affected residents must be made within 30 days of the date of determination that a security breach occurred.
- Establishing that the Attorney General must be notified if a covered entity believes that more than 500 Colorado residents have been affected by a breach. This must also be done within 30 days after determination of a breach.
- Establishing new requirements for the content of notifications to affected individuals.

**Connecticut:** On June 4, 2018, Connecticut revised its data breach statute, which will be effective on October 1, 2018.[24] Key changes include:

[23] Protections for Consumer Data Privacy, HB18-1128, 2018 Sess. (Colo. 2018), https://leg.colorado.gov/bills/hb18-1128.

[24] An Act Concerning Fees for Security Freezes on Credit Reports, Notification of A Consumer's Decision to Place or Remove A Security Freeze on A Credit Report and The Duration of Certain Identity Theft Prevention Services Required After A Date Breach, S. 472, 2018 Sess. (CT 2018), https://www.cga.ct.gov/2018/TOB/s/2018SB-00472-R00-SB.htm.

- Eliminating the fee consumers previously had to pay to credit agencies to place and remove credit freezes.
- Requiring credit rating agencies to place credit freezes as soon as practicable but no later than five business days after receipt of such request.
- Requiring credit rating agencies to remove security freezes as soon as practicable but no later than three business days after receipt of such request.
- Requiring credit monitoring be provided to affected consumers for not less than twenty-four months, when Social Security numbers are affected.

**Iowa:** On April 10, 2018, Iowa revised its data breach notification law, which went into effect on July 1, 2018.[25] Key changes include:

- Modifying the definition of "encryption" to mean only those certain algorithmic processes that meet accepted industry standards.
- Clarifying that the law does not apply to businesses that are subject to and comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").
- Requiring notification of a security breach to the Attorney General within five business days after giving notice of the breach of security to any consumer.

**Louisiana:** On May 20, 2018, Louisiana revised its data breach notification law, which went into effect on August 1, 2018.[26] Key changes include:

- Expanding the definition of "personal information" to also include first name or first initial and last name of an individual resident of Louisiana in combination with a passport number, state identification card number, or biometric data.
- Adding requirements for owners and licensees of computerized data to "implement and maintain reasonable security procedures and practices" and "take all reasonable steps to destroy or arrange for the destruction of records within its custody or control" when such data is "no longer to be retained by the person or business."
- Requiring notification no later than 60 days after discovery of the incident.
- Providing a lower threshold for substitute notification (if the cost of providing notification would exceed $100,000 or the affected class of persons notified exceeds 100,000).

**Nebraska:** On February 28, 2018, Nebraska revised its Financial Data Protection and Consumer Notification of Data Security Breach Act, which became effective on July 19, 2018.[27] Key changes include:

- Adding the requirement that any individual or commercial entity that conducts business in Nebraska and owns, licenses, or maintains computerized data that includes personal information about a resident of Nebraska to implement and maintain reasonable security procedures. These security procedures must also include proper disposal of personal information.
- Adding the requirement whereby if an individual or commercial entity discloses computerized data that includes personal information about a Nebraska resident to a nonaffiliated third-party service provider, it shall require by contract that the service provider implement and maintain reasonable security procedures and practices. This requirement does not apply to any contract entered before the effective date of the Act.
- Adding that any individual or commercial entity that complies with the Gramm-Leach-Bliley Act ("GLBA") or HIPAA, or with a state or federal law that provides greater protection to personal information than provided by this Act, then the individual or commercial entity will be in compliance with the foregoing requirements.
- Adding that any violation of the foregoing requirements would be considered an unlawful unfair or deceptive act or practice, but any violation does not give rise to a private right of action.

[25] Senate File 2177 (IA 2018), https://www.legis.iowa.gov/docs/publications/LGE/87/Attachments/SF2177_GovLetter.pdf.

[26] Database Security Breach Notification Law, S. 361, 2018 Sess. (LA 2018), https://www.legis.la.gov/legis/ViewDocument.aspx?d=1101149.

[27] Financial Data Protection & Consumer Notification of Data Security Breach Act of 2006, LB757, 2018 Sess. (NE 2018), https://ndbf.nebraska.gov/sites/ndbf.nebraska.gov/files/legal/87-801%20to%2087-808%20Financial%20Data.pdf.

**Oregon:** On March 16, 2018, Oregon revised its data breach notification law, which took effect on June 2, 2018.[28] Key changes include:

- Expanding the scope of the duty to notify to include a person that received notice of a breach of security from another person that maintains or otherwise possesses personal information on the person's behalf.
- Expanding the definition of "personal information" to include "any other information or combination of information that a person reasonably knows or should know would permit access to the consumer's financial account."
- Requiring notice of the breach to be given not later than 45 days after discovery or receiving notification of the breach.
- Requiring that if credit monitoring services and identity theft prevention and mitigation services are offered, it must be offered without charge to the consumer and may not be conditioned on a consumer providing a credit or debit card number or the consumer's acceptance of any other service the person offers to provide for a fee.

**South Dakota:** On March 21, 2018, South Dakota signed into law its Data Breach and Security Law, which took effect on July 1, 2018.[29] Key provisions include:

- Defining "personal information" to be a person's first name or first initial and last name in combination with any one or more of the following: Social Security number; driver's license number or other unique ID number created or collected by a government body; account, credit card, or debit card in combination with any required code that would permit access; health information; ID number assigned by employer in combination with code that would permit access; or biometric data.
- Requiring notification to be made within 60 days unless there is a law enforcement hold or an investigation has been performed and the assessment is that the breach will not likely result in harm to the affected person (notice of this result must be provided to the Attorney General).
- Allowing that, subject to certain requirements, notification may be provided by written notice, electronic notice, or substitute notice.
- Providing that any information holder that is regulated by federal law or regulation, including HIPAA or the GLBA, and maintains breach procedures pursuant to such laws is deemed to be in compliance with this chapter if the information holder notifies South Dakota residents in accordance with the provisions of the applicable federal law or regulation.

## D. GENERAL STATE LEGISLATION ON DATA PRIVACY

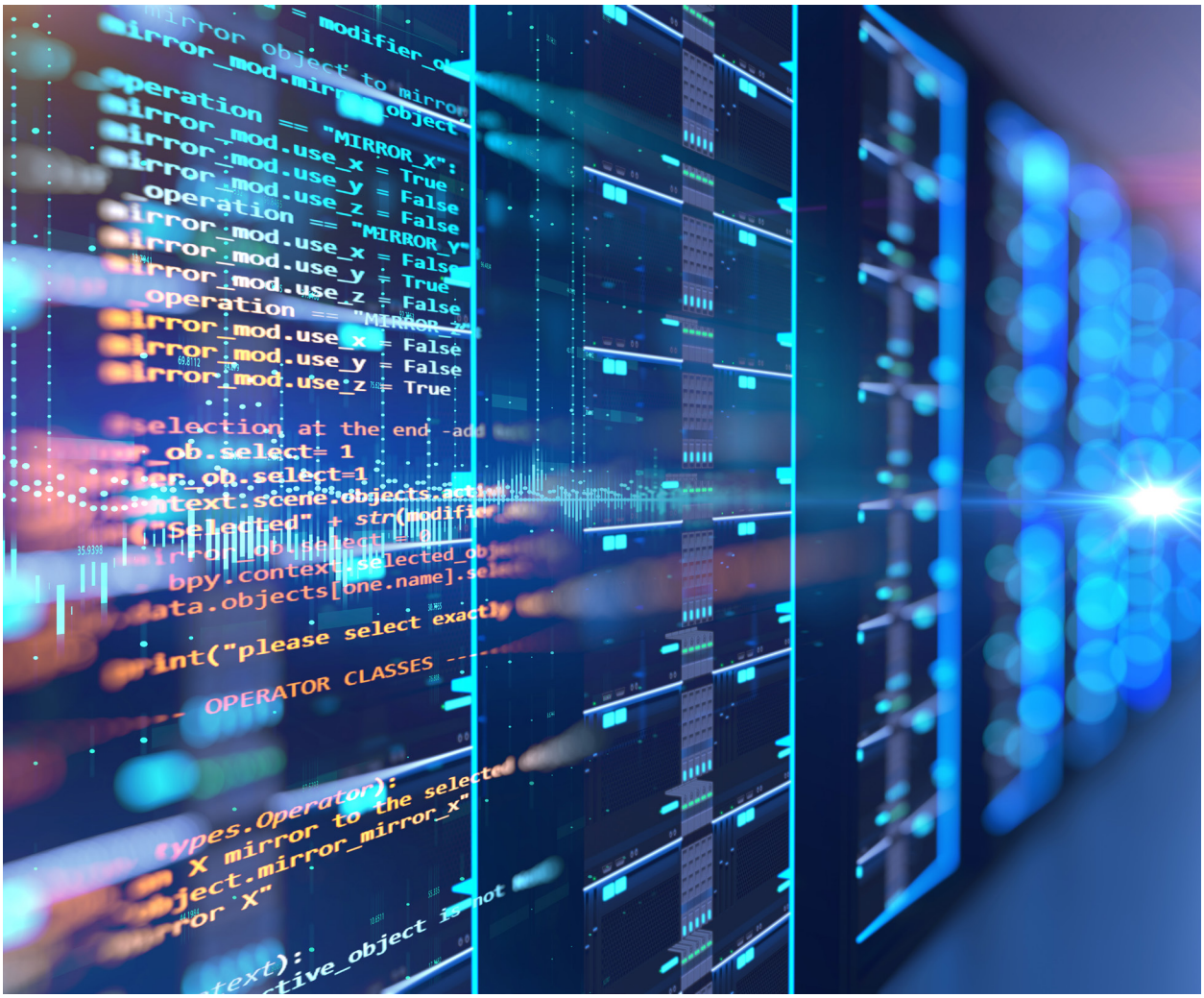
Several important pieces of state legislation on cybersecurity and data use were passed in 2018. Most notably, California passed the most comprehensive data use legislation in the nation, and Ohio became the first state to pass legislation that specifically defines "reasonable" cybersecurity safeguards.

### 1. California's Consumer Privacy Act

*In June 2018, California legislators passed Assembly Bill 375, later amended by Senate Bill 1121 (commonly known as the "California Consumer Privacy Act" or "CCPA") that would grant Californians "increased control" over their data.*

[28] Relating to Actions After A Breach of Security That Involves Personal Information; And Prescribing an Effective Date, S. 1551, 2018 Sess. (OR 2018), https://olis.leg.state.or.us/liz/2018R1/Downloads/MeasureDocument/SB1551/Enrolled.

[29] An Act to Provide for The Notification Related to A Breach of Certain Data and To Provide A Penalty Therefor, S. 62, 2018 Sess. (SD 2018), http://sdlegislature.gov/Legislative_Session/Bills/Bill.aspx?File=SB62ENR.htm&Session=2018&Version=Enrolled&Bill=62.



The CCPA will have substantial effects on businesses that have appreciable interactions with California in how they store, share, disclose, and engage with consumer data. The CCPA will be effective as of January 1, 2020.

To comply with the CCPA, businesses will need to create internal processes to properly and timely respond to consumer requests for information, requests for deletion, and requests to opt out of having their information sold. Businesses will also need to update their privacy policies and websites to provide the required methods for consumers to exercise their newly acquired rights and provide the more stringent required disclosures. Vendor management and controls will also need to be updated to ensure compliance with the limitations provided for by the CCPA. Businesses heavily reliant upon analyzing data will need to heighten technological capabilities to ensure that personal information is de-identified.

For technology companies, the CCPA may create additional obstacles when building an ecosystem of different organizations, each bringing a unique aspect to the product or service. For example, consider the companies involved in creating certain mobile application experiences for consumers who provide the various application programing interfaces ("APIs") and software development kits ("SDKs") that enable the consumer experience. Practically, all parties involved in an ecosystem will likely be affected by the conduct of the others, which is a shift from the traditional American digital paradigms. Partners and vendors will need to be carefully vetted prior to engagement by business teams and legal counsel.

*Each involved party will need to understand the data that the others are collecting, sharing, and selling, and will need to obtain representations and warranties in their agreements to protect themselves from a consumer class action or regulatory enforcement.*

Additionally, many contractual provisions such as licensing of data and indemnity will become greater points of contention in business-to-business deals and should be carefully discussed and reviewed with legal counsel.

Although many commentators refer to the CCPA as "California's Mini-GDPR," there are material differences between the CCPA and Europe's GDPR. Despite these differences, however, compliance with one can make compliance with the other dramatically easier. A comparison of the two statutes helps to illustrate these points:

| | CCPA | GDPR |
|---|---|---|
| **Application** | Sole proprietorship, partnership, LLC, corporation, association, or other legal entity organized or operated for profit or financial benefit that:<br>- Collects consumers' personal information or does so on behalf of others;<br>- Alone or jointly with others determines the purposes and means of the processing of consumers' personal information; and<br>- Does business in California; and<br>- That satisfies one of the following:<br>o Annual gross revenues in excess of $25,000,000;<br>o Alone, or in combination, annually buys, receives for business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or<br>o Derives 50% or more of annual revenue from selling consumers' personal information.<br><br>This includes any entity that controls or is controlled by a business meeting the above definition, and that shares common branding with such business.<br>*1798.140(c)*[30] | Any of the following processing of personal data:<br>- In context of activities of establishment of controller or processor in the Union, regardless of where the processing takes place;<br>- Of data subjects who are in the Union by a controller or processor not established in the Union, where processing activities are related to:<br>o Offering of goods and services to data subjects in the Union; or<br>o Monitoring of their behavior as far as behavior takes place in the Union.<br>- By a controller not established in the Union but in a place where Member State Law applies by virtue of public international law.<br>*Art. 3*[31] |

[30] All citations in this column will be to the California Civil Code, unless otherwise stated.

[31] All citations in this column will refer to the Articles of the General Data Protection Regulation, unless otherwise stated.

| | CCPA | GDPR |
|---|---|---|
| **Covered Information** | "Personal information" is anything that identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.<br><br>It includes but is not limited to:<br>- Identifiers such as real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name, SSN, driver's license number, passport number, or other similar identifiers;<br>- Any categories of personal information described in section 1798.80 (name, signature, SSN, physical characteristics or description, address, telephone number, passport number, driver's license or state ID card number, insurance policy number, employment, employment history, bank account number, CC number, debit card number, or any other financial information, medical information, or health insurance information);<br>- Characteristics of protected classifications under California or federal law;<br>- Commercial information (records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies);<br>- Biometric information;<br>- Internet or other electronic network activity;<br>- Geolocation data;<br>- Audio, electronic, visual, thermal, olfactory, or similar information;<br>- Professional or employment-related information;<br>- Educational information not publicly available;<br>- Inferences drawn from any of the above.<br><br>"Personal information" does not include "publicly available information."<br>- "publicly available information" means information that is lawfully made available from federal, state, or local government records.<br>- "publicly available information" does not mean: 1) biometric information collected by a business about a consumer without the consumer's knowledge; 2) information that is used for a purpose incompatible with the purpose for which it is maintained and made available or for which it is publicly maintained; and 3) consumer information that is deidentified or aggregate consumer information.<br>*1798.140(o)(1)-(2)* | "Personal data" is any information relating to an identified or identifiable natural person ('data subject'), which is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.<br>*Art. 4(1)*<br><br>Special categories of personal data are generally prohibited from processing with several exceptions. These special categories include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. It also includes genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.<br>*Art. 9* |

| | CCPA | GDPR |
|---|---|---|
| **Right to Access Information** | Consumers have the right to request categories of information collected, from whom it was collected, the specific business purposes for which it was collected, and with whom it is shared.<br>*1798.100, 1798.110*<br><br>Consumers also have right to request categories of information sold and to whom it was sold, and also the categories of personal information that the business disclosed about the consumer for a business purpose. "Sellers" appear to also be "collectors."<br>*1798.115*<br><br>These requests require a verifiable request from the consumer. Certain exceptions to the above apply for truly "one-time" uses.<br>*1798.100(d), 1798.110(b), 1798.115(b)*<br><br>The disclosures must be provided to the consumer free of charge within 45 days of a verifiable request, and cover the preceding 12-month period, and be delivered through the consumer's account with the business or by email or electronically in a readily useable format that allows the consumer to transmit the information from one entity to another without hindrance.<br>*1798.130(2)* | Data subjects have the right to obtain from the data controller:<br>- Confirmation as to whether or not personal data concerning him or her are being processed;<br>- Where personal data are being processed, then also the following:<br>o Purposes of the processing;<br>o Categories of personal data concerned;<br>o Recipients or categories of recipient to whom personal data have been or will be disclosed, particularly recipients in third countries or international organizations;<br>o Where possible, envisaged period for which personal data will be stored, or if not possible, the criteria used to determine that period;<br>o Right to request from controller rectification or erasure or personal data or restriction of processing or to object to such processing;<br>o Right to lodge complaint with supervisory authority;<br>o Existence of automated decision-making and meaningful information about logic involved and significance and consequences for data subject.<br>*Art. 15*<br><br>The controller shall provide information on action taken on this request to the data subject without undue delay and in any event within one month of the request. Extensions may be permitted.<br>*Art. 12* |
| **Right to Deletion** | A consumer has the right to direct a collector of personal information about the consumer to delete such information it has collected from the consumer.<br>*1798.105* | Data subject shall have right to obtain erasure of personal data without undue delay if: retention not necessary for original purpose of collection; consent withdrawn and no other legal basis for processing; objection to processing and no overriding legitimate grounds; compliance with legal obligation; or collected in relation to offer of information society services.<br>*Art. 17*<br><br>The controller shall provide information on action taken on this request to the data subject without undue delay and in any event within one month of the request. Extensions may be permitted.<br>*Art. 12* |

| | CCPA | GDPR |
|---|---|---|
| **Right to Rectification** | N/A | Data subject shall have right to rectification of inaccurate personal data or to make complete otherwise incomplete personal data.<br>*Art. 16*<br><br>The controller shall provide information on action taken on this request to the data subject without undue delay and in any event within one month of the request. Extensions may be permitted.<br>*Art. 12* |
| **Right to Restrict Processing** | N/A | Data subject shall have right to restrict processing if: accuracy of data contested; processing unlawful and data subject objects to erasure; personal data not needed by controller but must be retained for legal claims; data subject objected.<br>*Art. 18*<br><br>The controller shall provide information on action taken on this request to the data subject without undue delay and in any event within one month of the request. Extensions may be permitted.<br>*Art. 12* |
| **Right to Data Portability** | Consumers shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.<br><br>Upon a verifiable request, business shall promptly disclose and deliver within 45 days, free of charge, the personal information required. Information may be delivered by mail or electronically, and if provided electronically, then it shall be in a portable and readily useable format to allow transmission to another entity without hindrance. A business must provide this information at any time, but not more than twice in a 12-month period.<br>*1798.100; 1798.130* | Data subject shall have right to receive personal data concerning him or her in machine-readable format where processing based on consent or contract and processing carried out by automated means.<br>*Art. 20*<br><br>The controller shall provide information on action taken on this request to the data subject without undue delay and in any event within one month of the request. Extensions may be permitted.<br>*Art. 12* |
| **Right to Object** | N/A | Data subject shall have right to object to processing, including profiling, where legal basis for processing is public interest or legitimate interest.<br><br>Data subject shall have right to object at any time to processing of personal data for direct marketing purposes.<br>*Art. 21*<br><br>The controller shall provide information on action taken on this request to the data subject without undue delay and in any event within one month of the request. Extensions may be permitted.<br>*Art. 12* |

| | CCPA | GDPR |
|---|---|---|
| **Right to Opt Out** | A consumer has the right to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This is the right to opt out.<br>*1798.120(a)* | N/A |
| **Opt Out Notice** | A business that sells consumers' personal information to third parties shall provide notice to consumers that this information may be sold and that consumers have the right to opt out of the sale of their personal information.<br><br>A clear and conspicuous link must be provided on the business' website homepage to allow consumer to opt out.<br><br>This right must also be included in the privacy policy or in any description of California-specific privacy rights.<br>*1798.120(b); 1798.135(a)*<br><br>Consumers ages 13-16, or consumer's parent or guardian of consumers who are less than 13 years of age, must affirmatively authorize sale of consumer's personal information. ("Right to Opt In")<br>*1798.120(c)* | N/A |
| **Exceptions to Opt Out Notice** | N/A | N/A |
| **Privacy Policy** | Privacy policy must disclose:<br>- Description of consumer's rights pursuant to sections 110, 115, and 125 and one or more designated methods for submitting requests.<br>- List of the categories of personal information business has collected about consumers in the preceding 12 months.<br>- Two separate lists: 1) list of the categories of personal information business has sold about consumers in preceding 12 months, or if business has not sold such information, it shall disclose that fact; 2) list of categories of information it has disclosed about consumers for a business purpose in preceding 12 months, or if business has not disclosed such information, it shall disclose that fact.<br><br>Privacy Policy must be updated at least once every 12 months and must be provided just in time to consumers.<br>*1798.130(a)(5)* | Privacy policy must disclose:<br>- Identity and contact details of controller and representative, if applicable;<br>- Contact details of DPO, if applicable;<br>- Purposes and legal basis for processing;<br>- Legitimate interests pursued, if that is basis for processing;<br>- Recipients or categories of recipients of personal data, if any;<br>- Fact that controller intends to transfer personal data to third country or international organization and any adequacy decisions or reference to safeguards and how to obtain copy;<br>- Retention/storage period or criteria used to determine;<br>- Existence of rights to: access, rectification, erasure, restriction of processing, objection to processing, data portability, withdraw consent, lodge complaint with supervisory authority;<br>- Whether provision of personal data is statutory or contractual requirement and whether data subject is obliged to provide personal data and of possible consequences of failure to provide such data;<br>- Existence of automated decision-making, logic involved, and significance and consequences of such processing;<br>- Categories of personal data concerned; and<br>- Originating source of personal data, if not from data subject directly, and if applicable, whether it came from publicly accessible sources.<br>*Art. 13-14* |

| | CCPA | GDPR |
|---|---|---|
| **Delivery of Privacy Notices** | Privacy Policy information to be included in online privacy policy and in any California-specific description of consumers' privacy rights, or if business does not maintain those policies, then post it on its internet website.<br>*1798.130(a)(5)*<br><br>Consumers must be informed at or before the point of collection as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.<br>*1798.100(b)* | Notice to the data subject must be provided in a concise, transparent, easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information must be provided in writing or by other means, including electronically, where appropriate.<br>*Art. 12* |
| **Reuse and Redisclosure** | Where a third party buys personal information from a business, the third party cannot sell such information unless the consumer received explicit notice and is provided an opportunity to exercise the right to opt out.<br>*1798.115(d)* | Consent is required for each purpose for which data is processed, and new consent would be required for each new purpose for which data is shared.<br>*Art. 6* |
| **Prohibition Against Discrimination** | Requirement that business not discriminate against consumers for exercising their rights under the title, including by:<br><br>(1) Denying goods or services;<br>(2) Charging different prices or imposing penalties;<br>(3) Providing a different quality of service;<br>(4) Suggesting the above;<br><br>...unless the above is related to differences resulting from "the value provided to the consumer by the consumer's data."<br><br>Business may offer financial incentives to consumers, however, to obtain their personal information. But the practices for this entire subsection may not be "unjust, unreasonable, coercive, or usurious."<br>*1798.125* | Data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, with certain exceptions.<br>*Art. 22* |

Lawyers from American ad-tech backgrounds should take note of the following definitions under the CCPA:

- "Selling" information means "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration." *1798.140(t)(1).*
- "Deidentified" information means "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information (also)": (1) has implemented technical and business safeguards that prohibit reidentification; (2) has implemented business processes that prevent inadvertent release; and (3) makes no attempt to reidentify. *1798.140(h).*

Consumers whose information is accessed as a result of a business's failure to implement and maintain reasonable security procedures and practices have a private right of action against the business for statutory damages between $100-$750 per violation (after a 30-day notice to cure, if it can be cured), or actual damages, whichever is greater. An enforcement action by the Attorney General allows for stiffer penalties (up to $7,500 per violation). Businesses and third parties may seek guidance from the Attorney General on their compliance obligations.[32]

**2. Vermont's Data Broker and Consumer Protection Legislation**

*Becoming the first state to specifically regulate data brokers, Vermont passed H.764 in May without Governor Phil Scott's signature.[33]*

The aim of the new law is to provide consumers more information about data brokers, data collection practices, and the right to opt out.

The law offers a narrowly tailored definition of a "data broker," defining it as being "in the business of aggregating and selling data about consumers with whom the business does not have a direct relationship." While acknowledging that data brokers provide "critical" information for services offered in the "modern economy," the law notes that there are risks arising from unauthorized or harmful use of consumer information as well as risks related to consumers' ability to know and control information held and sold about themselves. Data brokers will be required to register annually with the Secretary of State and provide information about their data collection activities, opt-out policies, purchaser credentialing practices, and security breaches. The law also requires data brokers to adopt an information security program to protect sensitive personal information, prohibits acquiring personal information through fraudulent means or with intent to commit wrongful acts, and prohibits charging fees for placing or removing a credit security freeze.

**3. Ohio's Senate Bill 18-220**

In 2018, Ohio became the first state to define by way of statute what constitutes a "reasonable cybersecurity program." Ohio Senate Bill 18-220 states that an organization's cybersecurity program "reasonably conforms to an industry recognized cybersecurity framework" if it complies with standards promulgated by the National Institute of Standards and Technology ("NIST").

Notably, the statute provides that:

- The cybersecurity program shall take into consideration the size and complexity of the organization, the nature and scope of its activities, the sensitivity of the information sought to be protected, costs associated with the required safeguards, and the resources available to the organization.
- The bill shall not be construed to provide a private right of action, including a class action.

[32] *See* California Senate Bill 2018-1121, available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

[33] An Act Relating to Data Brokers and Consumer Protection, H.764, 2018 Sess. (VT 2018), https://legislature.vermont.gov/bill/status/2018/H.764.

The statute allows organizations that have implemented the NIST cybersecurity standards "an affirmative defense to any cause of action sounding in tort that is brought under the laws of this state or in the courts of this state and that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information."[34]

### 4. California's Senate Bill 18-327

In September 2018, California signed into law SB 18-327, a bill specifically regulating the security of the IoT.[35] The bill defines a "connected device" as "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address."

SB 18-327 requires connected devices to be equipped with "reasonable security features" (1) appropriate to the nature and function of the device, (2) appropriate to the information it may collect, contain, or transmit, and (3) is designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

Subject to the above, if a connected device is equipped with a means for authentication outside a local area network, this is considered a "reasonable security feature" where (1) the password is unique to each device so manufactured, or (2) the device contains a security feature that requires a user to generate a new means of authentication before access is granted for the first time.

SB 18-327 does not provide a private right of action but allows regulatory enforcement actions. No specific penalties or remedies are specified.

The new law will be effective as of January 1, 2020.[36]

### 5. Summary of General Cybersecurity Laws Across Different States

California, Vermont, and Ohio were not the only states to pass new legislation in 2018 imposing general data privacy requirements. Alabama, Colorado, and Louisiana also passed legislation and amendments that would likely affect most businesses generally. With that, approximately 40% of the states now have some type of general requirement for businesses engaged in data-based products. A high-level summary of the requirements is provided below.

| State | Covered Entity | General Requirement |
|---|---|---|
| Alabama | A covered entity that acquires or uses sensitive personally identifiable information. 2018 Ala. S.B. 318. | Implement and maintain reasonable security procedures and practices to protect sensitive personally identifying information against a breach of security. |
| Arkansas | Any business or person that acquires, owns or licenses personal information. Ark. Code §§ 4-110-104(b) | Implement and maintain reasonable security procedures and practices appropriate to the nature of the information. |
| California | Businesses that own, license, or maintain personal information about a California resident and certain third-party contractors. Cal Civ. Code § 1798.81.5 | Implement and maintain reasonable security procedures and practices appropriate to the nature of the information. New disclosure requirements under 2018 Cal. S.B. 375. |
| Colorado | Any entity that maintains, owns, or licenses personal identifying information in the course of the person's business or occupation. § 6-1-716 (2018 Colo. H.B. 1128) | Implement and maintain reasonable security practices and procedures to protect personal identifying information from unauthorized access. |
| Florida | Entities and third parties that have been contracted to maintain, store, or process personal information. Fla. Stat. § 501.171(2). | Reasonable measures to protect and secure data in electronic form containing personal information. |
| Indiana | A data base owner: a person that owns or licenses computerized data that includes personal information. Ind. Code § 24-4.9-3-3.5 | Implement and maintain reasonable procedures, including taking any appropriate corrective action. |

[34] Provide Legal Safe Harbor If Implement Cybersecurity Program, S. 220, 2018 Sess. (OH 2018), https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA132-SB-220.

[35] Adi Robertson, *California Just Became The First State With An Internet of Things Cybersecurity Law* (The Verge, Sept. 28, 2018), https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law.

[36] California S. 18-327, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

| State | Covered Entity | General Requirement |
|---|---|---|
| Kansas | A person who, in the ordinary course of business, collects, maintains or possesses, or causes to be collected, maintained or possessed, the personal information of any other person. Kansas K.S. § 50-6,139b | Implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure. |
| Illinois | Data collectors that own, license, maintain, or store personal information. 815 ILCS 530 | Implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. |
| Louisiana | Any person that conducts business in the state or that owns or licenses computerized data that includes personal information. La. Rev. Stat. § 3074 (2018 S.B. 361) | Implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. |
| Maryland | A sole proprietorship, partnership, corporation, association, or any other business entity, whether organized to operate at a profit or not, and certain nonaffiliated third-party service providers. Md. Code Com Law §§ 14-3501 through 14-3503 | Implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations. |
| Massachusetts | Any person that owns or licenses personal information. Mass. Gen. Laws. Ch. 93H § 2(a). | Authorizes regulations to ensure the security and confidentiality of customer information in a manner fully consistent with industry standards. The regulations shall take into account the person's size, scope and type of business, resources available, amount of stored data, and the need for security and confidentiality of both consumer and employee information. See 201 Mass. Code of Regs. 17.00-17.04. |
| Nebraska | An individual or commercial entity that owns, licenses, or maintains computerized data that includes personal information. Neb. Rev. Stat. § 87-802 through 87-808 | Establish and maintain reasonable security processes and practices appropriate to the nature of the personal information maintained. Ensure that all third parties to whom the entity provides sensitive personal information establish and maintain reasonable security processes and practices appropriate to the nature of the personal information maintained. |
| Nevada | A data collector that maintains records which contain personal information and any person to whom a data collector discloses personal information. Nev. Rev. Stat. §§ 603A.210, 603A.215(2). | Implement and maintain reasonable security measures (as specified / detailed in statute). |
| New Mexico | A person that owns or licenses personal identifying information of a New Mexico resident. N.M. Stat. § 57-12C-4, 57-12C-5 | Implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure. |
| Ohio | Business or nonprofit entity, including a financial institution, that accesses, maintains, communicates, or handles personal information or restricted information. Ohio Rev. Stat. § 1354.01 to 1354.05 (2018 S.B. 220) | To qualify for an affirmative defense to a cause of action alleging a failure to implement reasonable information security controls resulting in a data breach, an entity must create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information as specified (e.g., conforming to an industry recognized cybersecurity framework as listed in the act). |
| Oregon | Any person that owns, maintains or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities. Or. Rev. Stat § 646A.622 | Develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including disposal of the data (as specified /detailed in statute). |

| State | Covered Entity | General Requirement |
|---|---|---|
| Rhode Island | Businesses that own or license computerized unencrypted personal information and their nonaffiliated third-party contractors. R.I. Gen. Laws § 11-49.3-2 | Implement and maintain a risk-based information security program with reasonable security procedures and practices appropriate to the nature of the information. |
| Texas | Businesses that collect or maintain sensitive personal information, including nonprofit athletic or sports associations. Tex. Bus. & Com. Code § 521.052 | Reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business. |
| Utah | Any person who conducts business in the state and maintains personal information. Utah Code §§ 13-44-101, -201, 301 | Implement and maintain reasonable procedures. |
| Vermont | Data brokers: businesses that knowingly collect and license the personal information of consumers with whom such businesses do not have a direct relationship. 9 V.S.A § 2446-2447 (2018 H.B. 764) | Register annually with the Secretary of State. Implement and maintain a written information security program containing administrative, technical, and physical safeguards to protect personally identifiable information |

Critically, the table does not include state statutes that may affect select industries and certain types of businesses. It is important for organizations to check all state requirements, especially if they are in the health care, insurance, or broadband industries.[37]

## E. LOCAL LAWS AND INITIATIVES

One of the most interesting legislative developments in 2018 was the prospect of local counties and cities passing their own privacy initiatives and ordinances. In June 2018, the City of Chicago announced that it was considering an ordinance that would require businesses to: (1) have Chicago residents opt-in before businesses may disclose or sell their information; (2) register with the City of Chicago if the business qualifies as a "data broker"; and (3) provide notice and obtain consent before collecting mobile device data, including location data. As currently drafted, the ordinance introduced before the City Council would allow for a private right of action.[38]

Additionally, in July 2018, the City of San Francisco announced that it would put onto the November 2018 ballot a "Privacy First Policy." Voters approved the policy initiative on November 6, 2018.[39] The initiative sets forth 11 "privacy principles" that encourage local businesses to respect San Francisco residents' privacy, such as allowing residents to access their personal information, using data only in proportion with the originally disclosed purposes, implementing de-identification techniques, not collecting location data without express consent, and practicing other Fair Information Practice Principles. "Personal information" is defined very broadly under the initiative. The initiative precludes the City and County of San Francisco from issuing permits and entering into contracts with any business that does not comply with the policy.[40]


[37] *See e.g.*, Conn. Gen. Stat. § 38a-999b (health care center and insurance); Minn. Stat. § 325M.05 (internet service providers); S.C. Code § 38-99-10 to -100 (2018 H.B. 4655) (insurance).

[38] Molly DiRago, *A Look At Chicago's Data Protection Proposal*, LAW360 (Jul. 3, 2018), https://www.law360.com/articles/1059126/a-look-at-chicago-s-data-protection-proposal.

[39] Cutler, *San Francisco Voters OK 'Privacy First' Policy* (Bloomberg Law, Nov. 14, 2018), https://news.bloomberglaw.com/privacy-and-data-security/san-francisco-voters-ok-privacy-first-policy.

[40] Xiaoyan Zhang and Ariana Goodell, *San Francisco to Vote On "Privacy First Policy" In November*, TECHNOLOGY LAW DISPATCH (Aug. 1, 2018), https://www.technologylawdispatch.com/2018/08/privacy-data-protection/privacy-first-policy-to-be-on-november-ballot-in-san-francisco/.

Whether such local efforts are preempted by federal and state statutes will be an issue to be resolved in the coming months. Organizations should monitor the developments closely.

## F. THE FIGHT OVER DATA PRIVACY REGULATIONS IN BROADBAND

In August 2016, the Ninth Circuit held in *FTC v. AT&T Mobility (I)* that the Federal Trade Commission ("FTC") and Federal Communications Commission ("FCC") could not share jurisdiction over "common carriers," because whether or not an entity was a common carrier was based on the general status of the entity and not on its activity at any given time[41]. Until *AT&T Mobility (I)*, the telecommunications industry had considered itself to be regulated by the FCC only when it was engaged in "traditional common carrier" activities. But when it engaged in what were traditionally considered "non-common carrier activities" – for example, when it acted merely as an internet service provider ("ISP") – the telecommunications industry argued that it was not subject to the jurisdiction of the FCC. The FTC argued that they would have jurisdiction if the FCC had no jurisdiction over ISP-related activities. *AT&T Mobility (I)* flatly rejected the dichotomy.

Self-proclaimed "privacy advocates" welcomed *AT&T Mobility (I)*, as it followed former FCC Commissioner Tom Wheeler's contentious 2015 announcement that ISPs would be considered "common carriers."[42] Where the FTC had no jurisdiction over ISPs, and ISPs were also considered common carriers, the FCC would have comprehensive jurisdiction over all data carriers.[43] The FCC moved swiftly in accordance with the apparent political winds, issuing FCC 16-148 to regulate the data privacy practices of all common carriers, from cellular phone providers to ISPs. The FCC guidance is noteworthy because it required ISPs to not only maintain comprehensive cybersecurity programs, but also to provide detailed disclosures and obtain consumer opt-ins for data tracking.[44]

With the ascension of the Trump Administration, however, Commissioner Wheeler stepped down and Republican Commissioner Ajit Pai was appointed Chairman of the FCC. Commissioner Pai quickly revoked the classification of ISPs as common carriers[45] and revoked FCC 16-148.[46] Additionally, Commissioner Pai sought to "secure online privacy by putting the FTC . . . back in charge of broadband providers' privacy practices,"[47] while announcing future plans to "restore Internet Freedom by repealing Obama-era Internet regulations."[48]

Subsequently, ISPs were threatened with patchwork regulation due to the flurry of state and local activity. While some ISPs responded by proposing their own "internet bill of rights,"[49] others have requested that federal regulators step back in to prevent potentially conflicting state laws and local codes.[50] Notably,

41 *FTC v. AT&T Mobility LLC*, 835 F.3d 993, 1003 (9th Cir. 2016).

42 Rebecca Ruiz & Steve Lohr, *FCC Approves Net Neutrality Rules, Classifying Broadband Internet Service As a Utility*, N. Y. TIMES (Feb. 26, 2015), https://www.nytimes.com/2015/02/27/technology/net-neutrality-fcc-vote-internet-utility.html.

43 Fed. Commc'ns Comm'n, FCC 16-148, *Report and Order*; see also Jenna Ebersole, *FCC Sets New Privacy Framework For Broadband Providers*, LAW360 (Oct. 27, 2016), https://www.law360.com/articles/856450/fcc-sets-new-privacy-framework-for-broadband-providers.

44 *Id.*

45 Jacob Kastrenakes, *FCC Announces Plan to Reverse Title II Net Neutrality*, THE VERGE (Apr. 26, 2017), https://www.theverge.com/2017/4/26/15437840/fcc-plans-end-title-ii-net-neutrality.

46 Jenna Ebersole, *3 Things to Watch After FCC's Privacy Rules Get The Ax*, LAW360 (Mar. 31, 2017), https://www.law360.com/articles/908508/3-things-to-watch-after-fcc-s-privacy-rules-get-the-ax.

47 Jenna Ebersole, *FTC, FCC Chiefs Seek to Set 'Record Straight' On Privacy*, LAW360 (Apr. 5, 2017), https://www.law360.com/articles/910144/ftc-fcc-chiefs-seek-to-set-record-straight-on-privacy.

48 *Restoring Internet Freedom For All Americans*, FCC (Apr. 26, 2017), available at: https://www.fcc.gov/document/restoring-internet-freedom-all-americans.

49 Bryan Koenig, *AT&T Ad Pushes 'Internet Bill of Rights'*, LAW360 (Jan. 24, 2018), https://www.law360.com/articles/1005261/at-t-ad-pushes-internet-bill-of-rights-.

50 Brian Fung, *Why Comcast And Verizon Are Suddenly Clamoring to Be Regulated*, THE WASHINGTON POST (Jun. 28, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/06/28/why-comcast-and-verizon-are-suddenly-clamoring-to-be-regulated/?hpid=hp_hp-cards_hp-card-technology%3Ahomepage%2Fcard&utm_term=.55aa48b2fe87 (detailing how four telecom companies are arguing against AT&T and in favor of FTC regulation in the case of FTC v. AT&T Mobility, 835 F.3d 993 (9th Cir. 2016)).

the State of Washington passed its own law which sought to protect net neutrality. [51]

In response to an apparent public outcry, the new Republican FCC and FTC jointly issued a "Restoring Internet Freedom, FCC-FTC Memorandum of Understanding" on December 14, 2017, formally memorializing the FCC and FTC's "joint efforts" to regulate ISPs. The promise was that the FCC would "monitor the broadband market," and the FTC would "investigate and take enforcement action as appropriate . . . ."[52]

With the FCC and FTC standing together, in February 2018, the Ninth Circuit sitting *en banc* overturned its prior decision, holding that the FTC has jurisdiction over activities falling outside the common carrier services. The Ninth Circuit further reaffirmed that common carriers are regulated based on their activities, not their status as a company.[53]

*Apparently still dissatisfied with the compromises made, and perhaps even more angry over the fallout of FCC 16-148, California legislators passed their own comprehensive regulation intended to regulate ISPs.*

ISPs vowed to challenge the constitutionality of any such legislation passed.[54] Once the bill passed, California struck a deal with the FCC to delay the enforcement of the bill until courts resolve any pending litigation over the FCC's rollback of FCC 16-148.[55]

[51] Thuy Ong, *Washington State Has Passed Laws Protecting Net Neutrality*, THE VERGE (Mar. 6, 2018), https://www.theverge.com/2018/3/6/17084246/washington-state-laws-protecting-net-neutrality-fcc-internet.

[52] RESTORING INTERNET FREEDOM: FCC-FTC MEMORANDUM OF UNDERSTANDING, FCC-FTC (Dec. 14, 2017), available at: https://www.ftc.gov/policy/cooperation-agreements/restoring-internet-freedom-fcc-ftc-memorandum-understanding.

[53] *FTC v. AT&T Mobility, LLC*, 883 F.3d 848, 864 (9th Cir. 2018); Kelcee Griffis, 9th Circ. Upholds Limited Common Carrier Exemption at FTC, LAW360 (Feb. 26, 2018), https://www.law360.com/articles/1016208/9th-circ-upholds-limited-common-carrier-exemption-at-ftc.

[54] Cecilia Kang, California Lawmakers Pass Nation's Toughest Net Neutrality Law, N. Y. TIMES (Aug. 31, 2018), https://www.nytimes.com/2018/08/31/technology/california-net-neutrality-bill.html.

[55] Makena Kelly, *California Strikes Deal With FCC to Delay State Neutrality Law* (Oct. 26, 2018), https://www.theverge.com/2018/10/26/18029226/net-neutrality-fcc-california-law-ajit-pai-scott-wiener.

## G. THE NIST PREPARES FOR A MORE CONNECTED WORLD

In covering updates to the NIST special publications, we hope to continue educating lawyers on the importance of historical documentation in any defense against privacy litigation or regulatory investigation. The NIST publications not only identify what should be documented, but they also provide easily accessible and accepted frameworks by which the documentation process itself is attestation of compliance, even in the face of privacy events.

### 1. The NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations

Draft Revision 5 of Publication 800-53 promised a revised Publication 800-37 that would serve as the primary complementing guidelines for the selection of security and privacy controls. The NIST released the final draft of Revision 2 of Publication 800-37 on October 2, 2018 ("Revision 2").[56]

"The RMF (Risk Management Framework) provides a disciplined, structured, and flexible process for managing security and privacy risks that includes security categorization, control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring."[57] Like Draft Revision 5 of Publication 800-53, Revision 2 provides a number of considerations the organization should undertake and document – from preparation to categorization, to selection, to implementation, to assessment, to authorization, and then to monitoring – to demonstrate due diligence in the selection of organizational security and privacy controls.

There are seven major objectives for Revision 2:

- Provide better association and communication between the risk management processes, and activities at the governance and individual processes levels of the organization;
- Institutionalize critical risk management preparatory activities at all risk management levels, to facilitate a more effective and cost-effective execution of the RMF;
- Demonstrate how the NIST Cybersecurity Framework can be aligned with the RMF, and how both can be implemented using established NIST risk management processes;
- Integrate privacy risk management processes into the RMF to increase attention to privacy protection (i.e., and not just security);
- Promote the development of trustworthy secure software and systems, as similarly promoted by other NIST publications;
- Integrate the newer security-related, supply chain risk management concepts into the RMF, to address issues such as untrustworthy suppliers, tampering, insertion of malicious code, and poor manufacturing and development practices; and
- Allow for an organization-generated control selection approach to complement the traditional baseline control selection approach, while also supporting the use of the new consolidated control catalog from the NIST Special Publication 800-53, Revision 5.[58]

Revision 2 also provides a number of practical suggestions on how to best select a streamlined risk management framework:

- "Maximize the use of common controls at the organization level to promote standardized, consistent, and cost-effective security and privacy capability inheritance.
- "Use the tasks and outputs of the Organization-Level and System-Level Prepare Step to promote a consistent starting point within organizations to execute the RMF.

[56] Daniel Wilson, *NIST Issues Final Draft of Updated Risk Management Plan*, Law360 (October 3, 2018), https://www.law360.com/cybersecurity-privacy/articles/1089068/nist-issues-final-draft-of-updated-risk-management-plan?nl_pk=d100b429-aa27-499d-ad44-acee4f8fe74b&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy.

[57] *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Rev. 2 Final (NIST 2018), page ii, available at: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

[58] Dan Chandler, *Summary Thoughts On NIST Special Publication* (SP) 800-37 Revision 2 (Draft), CRITERION SYSTEMS (October 10, 2018), https://criterion-sys.com/summary-thoughts-on-nist-special-publication-sp-800-37-revision-2-draft/.

- Maximize the use of common controls to promote standardized, consistent, and cost-effective security and privacy capability inheritance.
- Maximize the use of shared or cloud-based systems, services, and applications where applicable, to reduce the number of organizational authorizations.
- Employ organizationally-tailored control baselines to increase the speed of security and privacy plan development, promote consistency of security and privacy plan content, and address organization-wide threats.
- Employ organization-defined controls based on security and privacy requirements generated from a systems security engineering process.
- Maximize the use of automated tools to manage security categorization; control selection, assessment, and monitoring; and the authorization process.
- Decrease the level of effort and resource expenditures for low-impact systems if those systems cannot adversely affect higher-impact systems through system connections.
- Maximize the reuse of RMF artifacts (e.g., security and privacy assessment results) for standardized hardware/software deployments, including configuration settings.
- Reduce the complexity of the IT/OT infrastructure by eliminating unnecessary systems, system elements, and services — employ least functionality principle.
- Make the transition to ongoing authorization and use continuous monitoring approaches to reduce the cost and increase the efficiency of security and privacy programs."[59]

We expect the final version of Revision 5 of the NIST Publication 800-53, expected in early 2019, to be consolidated with Revision 2 of the NIST Publication 800-37.

**2. The NIST Cybersecurity Framework Smart Grid Profile**

In November 2018, the NIST announced a smart energy grid workshop focused on smart grid interoperability and cybersecurity, which was accompanied by the release of a discussion draft of the NIST's "Smart Grid Profile" ("the "Profile").[60] The Profile "is an initial attempt to apply risk management strategies (from the NIST's Cybersecurity Framework)," and will likely result in additional smart grid guidelines from the NIST.[61]

The draft Profile is organized along the NIST Cybersecurity Framework's levels of "Implementation Tiers" and core "Functions." Implementation Tiers represent how an organization views the maturity of its cybersecurity risk management practice, while the Functions describe the five main categories of cybersecurity as "Identify," "Protect," "Detect," "Respond," and "Recover." The discussion draft thereby provides numerous important lessons for smart grid developers and participants to consider:

- Identify – The draft Profile notes that it is critical for an organization to catalog its hardware, software, and data assets, particularly the base communication and data flows.[62] Understanding the supply chain and power system dependencies will be critical for maintaining reliability and resilience.[63] A good chunk of the "Identify" section is devoted to assessing stakeholders and vendors in a "distributed resources" model with an "exponentially" high number of connected devices, which the draft notes is what is different about the "modernized grid."[64]

[59] Revision 2 Final, page 25.

[60] *Cybersecurity Framework Smart Grid Profile*, Discussion Draft (NIST 2018), https://www.nist.gov/sites/default/files/documents/2018/11/08/draft_csf_smart_grid_profile.pdf.

[61] *Id.*, at ii.

[62] *Id.*, at 11-12.

[61] *Id.*, at ii.

[62] *Id.*, at 11-12.

[63] *Id.*, at 13.

[64] *Id.*, at 14-17.

- Protect – The draft Profile notes that current systems lack sufficient physical access controls to the power components, and the problem will only increase in a "modernized and distributed grid" environment.[65] The "Protect" section heavily focuses on securing power availability, baseline configurations, and system integrity to ensure safety and reliability, while recommending the segregation and separation of resources so that the attack on one part of the system does not lead to the catastrophic loss of all others.[66]
- Detect – The draft Profile notes that "[a] baseline of network operations and expected data flows is extremely important," because "[u]nderstanding the control information flows will help monitor and detect unusual network behavior and allow for a timely response."[67] In addition, because of the dependencies on third parties for power system owners and operators, the draft Profile strongly suggests that these third parties be constantly monitored in case they become the source of external threats.[68]
- Respond – Because of the distributed nature of the smart grid, the draft Profile points out that the ability to readily share information regarding a data incident across the grid and utility lines will be especially important.[69] Notably, because the modernization of the grid will be a national endeavor spanning decades, the draft Profile notes that legacy and modernized infrastructures will be affected differently, and how they will be impacted differently should be well-thought out in advance.[70]
- Recover – Learning and planning should include plans for both legacy and modernized portions of the grid.[71]

65 *Id.*, at 18; also see 27.
66 *Id.*, at 19, 21-22.
67 *Id.*, at 26.
68 *Id.*, at 28.
69 *Id.*, at 31.
70 *Id.*, at 31-32.
71 *Id.*, at 33-34.

# III. EVOLVING CASE LAW

## A. DATA BREACH LITIGATION: BEYOND *SPOKEO*

### 1. Consumer Breach Litigation: Moving on to 12(b)(6) Motions

Despite mixed results over the past few years, motions to dismiss will likely remain the first line of defense for defendants involved in data privacy litigation. Barring another Article III opinion from the U.S. Supreme Court similar to Spokeo, defendants are now more likely to succeed with motions filed under Federal Rule of Civil Procedure 12(b)(6), rather than with motions filed under Rule 12(b)(1).

This marks a shift. In years past, defendants relied primarily on Rule 12(b)(1) motions, which challenge constitutional standing under Article III. In 2015 and 2016, however, the Seventh Circuit handed down a pair of decisions that changed the legal landscape. The Seventh Circuit's decisions held that plaintiffs could show "concrete and particularized" harm, as required to satisfy Article III, by alleging that a data breach created an increased threat of fraud and identity theft or required plaintiffs to spend time and money to resolve fraud and identify theft concerns. In both instances, the Seventh Circuit held that reasonable inferences must be made in plaintiffs' favor at the pleading stage, particularly on the issue of the sufficiency of fear of future harm to establish Article III standing.[72]

Through 2018, courts are still divided on the Article III issue, with only some courts following the Seventh Circuit.[73] Perhaps more importantly, however, some plaintiffs have been successful in convincing federal courts to remand to state courts after a Rule 12(b)(1) dismissal, as opposed to dismissing with prejudice.[74] Because of the potential for remand, defendants in small- to moderately-sized breach case to moderately-sized breach cases may find it more helpful to use a Rule 12(b)(1) motion to divide plaintiffs, where plaintiffs' counsel would not find it expedient to refile cases on a state-by-state basis.

Given the developments under Rule 12(b)(1), most cases now proceed on to Rule 12(b)(6) motions, which challenge whether plaintiffs have sufficiently pled a viable cause of action. In many cases, with Rule 12(b)(6) motions, defendants have been able to successfully defeat the case, or create substantial issues for a later stage of the litigation.

#### Contractual Terms as a Defense

In dismissing causes of action, some courts have closely applied defendants' terms of use. In the *In re VTech Data Breach Litigation*, for example, the plaintiffs alleged that defendant's connected toys contained cyber vulnerabilities, and that plaintiffs' credit/debit card information, online credentials, and childrens' information were hacked and made vulnerable. The court granted most of VTech's Rule 12(b)(6) challenges on the basis of VTech's written terms and conditions. First, the court focused on separating what was understood or promised at the time the toys were purchased, versus the online terms agreed to in relation to the post-purchase connected services (i.e., "Kid Connect"). Then, the court found that implied contract allegations were subsumed by express contract allegations and dismissed the implied contract and implied warranty claims. The court found that the plaintiffs failed to

[72] *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 691-94 (7th Cir. 2015) (finding risk of future harm sufficient to establish Article III standing based on allegations of harm already suffered); accord Lewert v. P.F. Chang's China Bistro, 819 F.3d 963, 966-67 (7th Cir. 2016) (citing same reasoning in Remijas).

[73] See *e.g., Hutton v. Nat'l Bd. Of Examiners in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018); *Ree v. Zappos.com, Inc.* (In re Zappos.com, Inc.), 888 F.3d 1020 (9th Cir. 2018); *Dieffenbach v. Barnes & Nobles, Inc.*, 2018 U.S. App. LEXIS 9051 (7th Cir. Apr. 11, 2018); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113 (N.D. Cal. 2018); *Fero v. Excellus Health Plan*, 304 F. Supp. 3d 333 (W.D.N.Y. 2018); *Byrne v. Avery Ctr. For Obstetrics & Gynecology*, 327 Conn. 540 (Jan. 16, 2018). But see, *Brett v. Brooks Brothers Grp.*, 2018 U.S. Dist. LEXIS 153150 (C.D. Cal. Sept. 6, 2018) and *Antman v. Uber Techs., Inc.*, 2018 U.S. Dist. LEXIS 79371, at *10 (N.D. Cal. May 10, 2018).

[74] *See e.g., Patton*, 2016 U.S. Dist. LEXIS 60590 (C.D. Cal. May 6, 2016).

allege a violation of the online services agreement. The court therefore also dismissed the unjust enrichment claims, along with the various claims under consumer protection statutes.[75]

More recently in *Flores v. Uber*, the court affirmed the use of rigorous arbitration provisions, even in the context of data breach class actions. Although the question is likely one for the arbitrator, the court noted that the terms contained a class action arbitration waiver. [76]

Likewise, defendants should consider the potential interplay between using the contractual terms and then seeking to apply the economic loss rule. In *Bray v. Gamestop Corp.*, the plaintiffs brought suit for a payment card breach. Although the Rule 12(b)(6) challenges were only granted in part, the court dismissed the breach of contract claims for its failure to allege the contractual terms. The court denied the 12(b)(6) challenge on the implied contract claims, finding that there was conflicting law on whether payment card industry ("PCI") rules could form the basis for an implied contract. But the court then applied the economic loss rule to dismiss the negligence claim on a Rule 12(b)(6) challenge, suggesting that the court would ultimately dismiss other claims based on any applicable terms and conditions, once plaintiffs amended the complaint to allege the written contractual terms.[77]

Nonetheless, defendants should expect plaintiffs to respond to any contractual defenses by asserting contractual unconscionability.[78] Accordingly,

*it would be advisable for all organizations looking to enforce their terms and conditions to consider and review their onboarding and user sign-up procedures.*

**Causes of Action Dismissed for Lack of Credibility**

Some courts have also dismissed claims on the implausibility of the claims alleged. For example, in the retail breach case of *Alleruzzo v. SuperValu*, the Eighth Circuit affirmed a trial court's dismissal under Rule 12(b)(1) for all but one plaintiff. On remand, the district court dismissed the last plaintiff as well for failing to allege that he shopped during the relevant shopping period, and for failing to allege that he was not reimbursed for the fraudulent charge he allegedly suffered.[79]

In *Antman v. Uber Technologies*, the plaintiffs brought suit for breach of Uber drivers' records, including drivers' license information and "banking information," as part of the alleged breach. In granting the motion to dismiss primarily under Rule 12(b)(1), the court closely scrutinized the plausibility of each representative's allegations and their claimed damages. The court found that the plaintiffs' allegations regarding the breach of their drivers' license and banking account details were insufficiently related to their damages allegations. The court also pointed out that the named plaintiffs wanted the court to allow class discovery to find the right representative member, "apparently because the named plaintiffs do not allege that their Social Security numbers were disclosed." The court suggested that it would have granted the concurrently filed Rule 12(b)(6) motions for similar reasons and dismissed the case with prejudice.[80]

In *Razuki v. Caliber Homes Loans*, although the court denied the defendant's Rule 12(b)(1) motion, the court dismissed without prejudice all the causes of action under a Rule 12(b)(6) challenge because the plaintiff "need[ed] to allege more than cagey and indefinite allegations in his complaint." The court even applied the pleading requirements to more general claims such as negligence and delayed notification pursuant to the California Customer Records Act.[81]

[75] *In re VTech Data Breach Litig.*, 2018 U.S. Dist. LEXIS 65060 (N.D. Ill. Apr. 18, 2018).

[76] *Flores v. Uber Technologies*, C.D. Cal. Case No. 17-8503, Dkt. 62 (Sept. 5, 2018).

[77] *See Bray et al. v. Gamestop Corp.*, D. Del. Case No. 17-01365, Dkt. 36 (Mar. 16, 2018).

[78] *See e.g., In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 U.S. Dist. LEXIS 140212 (N.D. Cal. Aug. 30, 2017).

[79] *In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, 2018 U.S. Dist. LEXIS 36944 (D. Minn. Mar. 7, 2018).

[80] *Antman v. Uber Techs., Inc.*, 2018 U.S. Dist. LEXIS 79371, at *10 (N.D. Cal. May 10, 2018).

[81] *Razuki v. Caliber Home Loans, Inc.*, 2018 U.S. Dist. LEXIS 96973, at *5 (S.D. Cal. Jun. 7, 2018).

In a case against a popular beverage company, the defendant beverage company prevailed on its motion for summary judgment because the court found no causation between the damages alleged and the information lost from stolen laptops. After assessing the parties' expert opinions, the court agreed with the defendant that it would not be credible to attribute the alleged compromise of the plaintiff's retail accounts online to the lost laptops, which only contained driver's license information as sensitive information.[82]

In *Brett v. Brooks Brothers*, which involved a retail breach allegedly involving payment cards at more than 200 stores, the defendant prevailed on a Rule 12(b)(1) motion to dismiss. The court found that where the only potentially sensitive information at issue was credit card information, "Plaintiff's linking theory requires the Court to make a series of speculative inferences to conclude that Plaintiffs suffer a credible, imminent risk of identity theft." The court refused to so do, and in granting the motion to dismiss, entered judgment in favor of defendant.[83]

And in *Williams-Diggins v. (Mercy) Health*, the court held that mere vulnerability on a HIPAA-covered entity's website without an actual data breach is not sufficient "harm" to confer Article III standing to the plaintiff, concurrently denying the plaintiff's "overpayment" claims as well. In the court's words, "[e]ven if Defendant's approach to data security was clumsy, it also was harmless, and that is fatal to Plaintiff's claims."[84]

The lesson of these cases is that defendants must press plaintiffs to be very specific about their injuries,

[82] Jon Hyman, *Does an Employer Have a Duty to Protect the Personal Information of Its Employees?* WORKFORCE (July 12, 2018), https://www.workforce.com/2018/07/12/does-an-employer-have-a-duty-to-protect-the-personal-information-of-its-employees/

[83] *Brett v. Brooks Brothers Grp.*, 2018 U.S. Dist. LEXIS 153150 (C.D. Cal. Sept. 6, 2018).

[84] *Williams-Diggins v. Health*, 2018 U.S. Dist. LEXIS 206195 (N.D. Ohio, Dec. 6, 2018).

and carefully consider the compromised data sets at issue. Just because sensitive data has been exposed does not mean that the damages alleged by the putative class representative(s) are plausible. Indeed, in light of Congress' passage of the Economic Growth, Regulatory Relief, and Consumer Protection Act in 2018, which allows consumers to request free "national security freezes" for at least one year,[85] plaintiffs may not be able to plausibly argue that fraudulent accounts continued to be opened in their names after they have been provided notification.

**The Fight Over Negligence as a Cause of Action**

Perhaps the most interesting current debate in the courts is whether consumers have a cause of action for general negligence as a matter of right whenever there is a data breach. In *McConnell v. Georgia Department of Labor*, for example, which involved the inadvertent disclosure of the employment records of those who worked for the State of Georgia, the appellate court found that in Georgia there is no general duty to secure data.[86]

In contrast, in the *In re Arby's Restaurant Group Inc. Litigation*, the plaintiffs defeated a Rule 12(b)(6) motion on a negligence cause of action by arguing that Article 5 of the FTC Act imposes a general duty to secure payment card information. Because the consolidated case included a consumer class – although the issues were being pushed by sponsoring banks of payment cards – plaintiffs in future cases will undoubtedly attempt to argue that the ruling applies to consumer classes as well.[87]

In *Diaz v. Intuit, Inc.*, however, the plaintiffs attempted to argue that Intuit owed a general duty of care to tax filers, regardless of whether or not they were actual users. The plaintiffs argued that Intuit knew that hackers used its website for fraudulent filings by creating fake accounts on behalf of class members. The court disagreed, finding that there were no such general duties owed to non-users, even if hackers may use the identities of non-users on the Intuit website. The court also rejected aiding and abetting claims against Intuit.

As the 2018 landscape shows, the courts and litigants are still struggling with whether a general duty of care can and should be imposed in the data breach context. As with Diaz v. Intuit, Inc., organizations hosting data may not necessarily have any interactions with the consumer plaintiff, and courts may feel that imposing a duty would ultimately be unfair and create poor public policies.

Defendants should note that the economic loss rule may be available as a defense to a claim for negligence, even when the residents of multiple states are involved. The fact that different states treat the economic rule differently may not necessarily prevent a court from applying the rule as a bar to all of the negligence claims.[89]

**Certifiability and Settlements**

One of the most interesting issues in data breach actions has been the viability of class action settlements. Because only one small class action in the data breach context has ever obtained class certification,[90] it remains to be seen whether larger class actions can ever successfully obtain class certification. Many courts that have denied motions to dismiss have noted the difficulties of certifiability of the class.[91]

---

85 Bureau of Consumer Financial Protection Issues Updated FCRA Model Disclosures, CFPB (Sept. 12, 2018), https://www.consumerfinance.gov/about-us/newsroom/bureau-consumer-financial-protection-issues-updated-fcra-model-disclosures/.

86 *McConnell v. Dep't of Labor*, 345 Ga. App. 669 (Ct. App. Ga. May 11, 2018). But see *Dittman v. University of Pittsburg Medical Center*, 2018 Pa. LEXIS 6051 (Nov. 21, 2018), in which the Supreme Court of Pennsylvania held that there is a common law duty on the party of employers to safeguard employee information – at least in the State of Pennsylvania.

87 *In re Arby's Restaurant Group Litig.*, 2018 WL 2128441 (N.D. Ga. Mar. 5, 2018).

88 *Diaz v. Intuit, Inc.*, 2018 U.S. Dist. LEXIS 82009 (N.D. Cal. May 15, 2018).

89 *See e.g., Gordon v. Chipotle Mexican Grill*, 2018 U.S. Dist. LEXIS 165314 at *24 (D. Colo. Sept. 26, 2018).

90 *See Smith v. Triad of Ala.*, LLC, 2017 U.S. Dist. LEXIS 38574 (M.D. Ala. Mar. 17, 2017) (involving less than 1,300 patients, and with relatively straight forward facts).

91 *See e.g., Dieffenbach v. Barnes & Nobles, Inc.*, 2018 U.S. App. LEXIS 9051, at *8-9 (7th Cir. Apr. 11, 2018) (noting class issues need to be considered upon remand); see also Dolmage v. Combined Ins. Co. of Am., 2017 U.S. Dist. LEXIS 67555 (N.D. Ill., May 3, 2017) (denying class certification); In re Zappos.com, Inc. Customer Data Sec. Breach Litig., 2016 U.S. Dist. LEXIS 115598 (D. Nev. Aug. 29, 2016) (affirming prior order striking class allegations).

When the parties reach a settlement, both sides often feel compelled to argue certifiability so that the dispute can be finally resolved. Nonetheless, sometimes third-party counsel may attempt to take the settlement hostage by objecting to the certifiability. In *Target Corp. Customer Data Security Breach Litigation*, an objecting class member alleged that class members who could claim money under the settlement had a conflict with those who could not, because the latter were treated differently for not claiming actual injury.

After initially agreeing with the objector, the Eight Circuit eventually affirmed the district court's revised order preliminarily approving the settlement, where the district court explained how the class members' different interests were not antagonistic to each other. Specifically, the Eight Circuit explained that both the "uninjured" and "injured" class members could suffer future harms.[92]

In light of the specter of such challenges, courts have been more closely scrutinizing class action settlements.[93] Indeed, legal commentators believe that several nationwide trends are making class certification more difficult.[94] Counsel should therefore pay more attention to the motion and supporting papers submitted for preliminary approval of class settlements.

**2. Business-to-Business Breach Litigation: Split Circuits**

After the District Court of Minnesota refused to dismiss the negligence cause of action brought by financial institutions against Target arising from its data breach,[95] many financial institution plaintiffs had high hopes for retail business-to-business data breach litigation. Although they have recovered some significant settlements amidst certain large retail breaches, financial institution plaintiffs have also lost several significant cases since *Target*.

For example, in *Community Bank of Trenton v. Schnuck Markets*, the Seventh Circuit affirmed the opinion of the Southern District Court of Illinois, which granted a motion to dismiss by the defendant supermarket chain. On the claims for negligence filed by the credit card issuing bank plaintiffs, the lower court had found that while some other courts had found a duty of care existed between the plaintiff banks and the defendants, those decisions were made assessing the state laws at issue in those cases, but not the laws of the State of Missouri at issue. "In the absence of such legislation, this court declines to sua sponte create a duty where the Missouri government has declined to do so."[96] The Seventh Circuit on appeal affirmed, and further applied the economic loss rule under Missouri and Illinois law.[97]

On the other hand, in the *In re Arby's Restaurant Group Inc. Litigation*, the plaintiffs defeated a Rule 12(b)(6) challenge on the negligence cause of action by arguing that Article 5 of the FTC Act imposed a general duty on the defendant to reasonably secure the payment card information allegedly compromised. Similarly, in *CVS Pharmacy v. Press America*, where CVS's vendor misprinted certain patients' envelopes that ultimately revealed their identities and conditions, the court held that the customer-vendor relationship was sufficient to confer a duty of care on the defendant.[98] These rulings are good illustrations of the current split amongst the district courts.[99]

Notably, to deter the likelihood of incoming litigation from business partners and enterprise customers, organizations should insist on strong contractual terms in their customer, vendor, and partnership agreements. In *O'Neil v. Bank of America*, for example, the court held that the bank's service agreement allowed it to honor a fraudulent wire transfer request, notwithstanding subsequent requests by the transferor to amend and cancel payment, where the service agreement provided that

92 *Scaroni v. Target Corp.* (In re Target Corp. Customer Data Sec. Breach Litig.), 2018 U.S. App. LEXIS 15839 (8th Cir. Jun. 13, 2018).

93 *Reimjias v. Neiman Marcus Group*, 2018 U.S. Dist. LEXIS 158250 (N.D. Ill. Sept. 17, 2018) (rejecting settlement application); Walters v. Kimpton Hotel & Restaurant Group, LLC, N.D. Cal. Case No. 16-05387, Dkt. 102 (Sept. 13, 2018)

94 *See also Espinosa v. Aheran* (In re Hyundai & Kai Fuel Econ. Litig.), 881 F.3d 679 (Jan. 23, 2018) (finding that a district court in assessing a settlement class must conduct a Fed. Rules of Civ. Proc. Rule 23 analysis).

95 *In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304 (D. Minn. 2014).

96 *Cmty. Bank of Trenton v. Schnuck Mkts.*, 2017 U.S. Dist. LEXIS 66014, at *10 (S.D. Ill. May 1, 2017).

97 *Cmty. Bank of Trenton v. Schnuck Mkts.*, 887 F.3d 803 (7th Cir. 2018).

98 *CVS Pharm., Inc. v. Press Am. Inc.*, 2018 U.S. Dist. LEXIS 2282 (S.D.N.Y. Jan. 3, 2018).

99 *In re Arby's Restaurant Group Inc. Litig.*, 2018 WL 2128441 (N.D. Ga. Mar. 8, 2018).

the bank had discretion to honor transfers initiated by agreed protocols.[100]

## B. DATA MISUSE LITIGATION: WHERE TECHNICALITIES MATTER

Unlike data breach cases, it is difficult to break down data misuse cases as lessons for how data may be used in different contexts. Privacy laws in the U.S. that affect data use are still very much in development and exist in patches across different sectors and industries. While all fifty states now have data breach statutes, and while some states have requirements for data controllers to secure information, the only state with any real patchwork of privacy laws is California. The U.S. does not yet have a comprehensive regulation like the EU's GDPR, and as such, plaintiffs often struggle with finding viable liability theories.

This is especially true when plaintiffs try to reconcile emerging technologies with antiquated statutes like the federal Electronic Communications Privacy Act ("ECPA," also known as the "Wiretap" statute). Indeed, one court's idea of data misuse may not be shared by another court.

### 1. Cases Involving Online Tracking and Aggregation

Most of the important cases in 2018 relating to online tracking and aggregation have focused on data aggregation and scraping. Demonstrating the importance of privacy policies, courts have applied their terms on choice of law, mandatory arbitration, and even anonymized use of collected email data:

- In *Bernardino v. Barnes & Noble Booksellers*, a New York federal judge upheld the validity of "sign-in wrap" and "checkout-wrap" agreements. The plaintiff alleged that Barnes and Noble allowed her information and activities on the retailer's website to be shared with Facebook Inc., and that such sharing was done without her knowledge. In adopting portions of the magistrate recommendation, the court found that the plaintiff was bound by the arbitration provision in the bookseller's terms of use. Although the plaintiff was not required to click a box showing acceptance of the terms, the link to the bookseller's terms was posted during the checkout process and was reasonably conspicuous to users of its websites.[101]
- In *Cooper v. Slice Techs*, the plaintiffs alleged that defendants' email software, which assisted in the unsubscribing of unwanted junk emails, improperly collected and read data relating to their emails. The court found that the plaintiffs had agreed to defendants' privacy policy, which had disclosed that defendants would use their data to build anonymous market research products and services with business partners. The court found that the privacy policy was not unconscionable, thereby dismissing the ECPA and unjust enrichment claims.[102]
- In *Cohen v. Casper Sleep*, plaintiff alleged that his keystrokes and clicks were improperly intercepted by defendants on websites through the real-time activity tracking technologies of Navistone. The court found that the plaintiff's claims for violation of the ECPA failed because consent under the act only required that of one party, and ISPs could not be construed to be an intended party. Further, the plaintiff's Stored Communications Act ("SCA") claim failed because the defendants' access to cookies planted and stored on the plaintiff's personal devices was not tantamount to access to electronic storage under the SCA, and the SCA only covered devices temporarily storing electronic communications. The claims under New York's General Business Law failed because the alleged injury was insufficient, and the privacy policy did not amount to advertising.[103] Similar Wiretap claims filed by the same plaintiffs' law firm against Navistone and Quicken Loans, on the latter's website, were also dismissed in *Allen v. Quicken Loans*.[104]

[100] *O'Neill v. Bank of Am. Corp.*, 2018 U.S. Dist. LEXIS 193302 (E.D. Penn. Nov. 13, 2018).

[101] *Bernardino v. Barnes & Noble Booksellers, Inc.*, 2018 U.S. Dist. LEXIS 15812 (S.D.N.Y. Jan. 31, 2018).

[102] *Cooper v. Slice Techs., Inc.*, 2018 U.S. Dist. LEXIS 95298 (S.D.N.Y. June 6, 2018).

[103] *Cohen v. Casper Sleep Inc.*, 2018 U.S. Dist. LEXIS 116372 (S.D.N.Y. Jul. 12, 2018).

[104] *Allen v. Quicken Loans*, 2018 U.S. Dist. LEXIS 192066 (D. N.J., Nov. 9, 2018) (alleging illegal wiretapping based on illegality arising from violations of the Gramm-Leach-Bliley Act).

- In *Alan Ross Machinery Corp. v. Machinio Corp.*, the plaintiff brought suit involving the defendant's scraping practices off of the plaintiff's website sales listings, alleging that the defendant violated the plaintiff's terms and conditions and the Computer Fraud and Abuse Act ("CFAA"). The court disagreed and dismissed the case with leave to amend, finding that the plaintiff failed to plead the damages required by the CFAA, and that the browsewrap website terms the plaintiff sought to enforce were questionable, especially without allegations that the defendant actually knew about the terms.[105]
- By contrast, in *Smith v. Facebook*, the Ninth Circuit affirmed the lower court's dismissal of the plaintiff's case, alleging that Facebook improperly tracked the plaintiffs' activities, even on healthcare websites. The appellate court found that Facebook's broadly worded terms and conditions covered cookies and tracking technologies Facebook disseminated on third-party sites. In addition, the court refused to adopt a broad interpretation of "sensitive information" under HIPAA, and instead found that clickstream data on public websites were particularly different or sensitive.[106]

**2. Cases Involving Mobile Device Tracking and Aggregation**

There have not been many reported cases involving mobile devices in 2018, although a number of decisions are still noteworthy, particularly in the area of mobile location data:

- In a case alleging that a certain laptop manufacturer pre-installed "spyware" on its laptops, thereby creating performance, privacy, and security issues, a district court in California found that the plaintiffs lacked standing to assert claims under New York's Deceptive Acts and Practices Statute. The plaintiffs did not allege that they were New York residents, nor that any conduct or deceptive transaction occurred within New York, despite the fact that the parties agreed that New York substantive law applied to the case. The district court found that the plaintiffs improperly conflated choice-of-law with statutory standing, and that even if the parties agreed that New York law should apply to the litigation, the plaintiffs still must adequately allege a claim under that law. Additionally, the district court held that

[105] *Alan Ross Mach. Corp. v. Machinio Corp.*, 2018 U.S. Dist. LEXIS 113012 (N.D. Ill. Jul. 9, 2018).

[106] *Smith v. Facebook*, 2018 U.S. App. LEXIS 34397 (9th Cir., Dec. 6, 2018).

even if the consumers had statutory standing, they failed to allege sufficient facts to show they overpaid for the computers or did not receive the full value of their laptops free of malware.[107]

- Federal and state anti-wiretap acts have been used for years awkwardly by plaintiffs in cases involving various types of mobile tracking. However, in 2018, plaintiffs suffered setbacks in several jurisdictions that may limit what kind of data collection such statutes could cover. For example, in *Vasil v. Kiip*, the court found that the use of APIs to collect geolocation data when the APIs were imbedded in another application, was not "interception" within the purview of the ECPA.[108] Similarly, in *Gruber v. Yelp*, the court held that California's Invasion of Privacy Act was not intended to cover recordings on voice-over-IP technologies.[109]
- Plaintiffs who have attempted to use the SCA for data misuse cases also suffered setbacks in 2018. In *Gonzalez v. Uber*, the plaintiff attempted to bring a data misuse class action for Uber's alleged use of its mobile application to spy on user activities with competitor applications such as Lyft, through the creation and use of fake Lyft transactions. After dismissing the Wiretap claims for lack of allegation of interception of "content,"[110] the court then dismissed the SCA claims, finding that there were no allegations that Uber actually accessed data intended to be cached or stored temporarily, as opposed to real time geolocation data.[111]
- In *Carpenter v. U.S.*, the Supreme Court held that the federal government generally needs a warrant to access historical cellphone location records, finding that the data requires more stringent protection than other customer information held by service providers.[112] Although a criminal case, plaintiffs in civil cases will inevitably cite to *Carpenter* in support of how GPS and location data are sensitive personal information.

### 3. Cases Involving IoT and Emerging Technologies

Illinois's Biometric Information Privacy Act ("BIPA"), which governs the use of biometric data, continues to generate the most cases in the realm of emerging technologies. Although heavily litigated, no court has yet to award the statutory fines that may be available under BIPA. Instead, most cases are still stuck on whether mere procedural violations of BIPA are sufficient for claims to proceed.

As of the date of this publication, it appears that Illinois courts are distinguishing procedural violations for first-party use, as opposed to third-party use. In *Howe v. Speedway*, for example, the Illinois District Court held that the plaintiff's "mental anguish over his uncertainty" regarding what his employer will do with his biometric fingerprint data, without allegations that the data was or is likely to be misused, "is precisely the type of conjectural or hypothetical injury that cannot support Article III standing." The court found that the defendant's alleged failure to provide proper BIPA disclosures, alleged failure to obtain the plaintiff's written authorization, and alleged failure to create a biometric data retention and destruction policy were procedural insufficient to confer Article III standing, although the case was remanded to state court.[113] Subsequent decisions in 2018 followed *Howe*.[114]

In contrast, courts have been less lenient where there are allegations of third-party use of biometric data. For example, an employer disclosing employee fingerprint data to a third party without authorization "distinguishes [the] case from others in which alleged violations of BIPA were determined insufficiently concrete to constitute an injury in fact for standing purposes." Thus, the court in *Dixon v. Washington & Jane Smith Community* allowed

[107] *In re Lenovo Adware Litig.*, 2018 U.S. Dist. LEXIS 15015 (N.D. Cal. Jan. 30, 2018).

[108] *Vasil v. Kiip, Inc.*, 2018 U.S. Dist. LEXIS 35573 (N.D. Ill. Mar. 5, 2018).

[109] *Gruber v. Yelp, Inc.*, San Francisco Sup. Ct. Case No. 16-554784 (Apr. 16, 2018).

[110] *Gonzalez v. Uber Techs*, 305 F. Supp. 3d 1078 (N.D. Cal., Apr. 18, 2018).

[111] *Gonzalez v. Uber Techs*, 2018 U.S. Dist. LEXIS 165646 (N.D. Cal., Sept. 26, 2018).

[112] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

[113] *Howe v. Speedway LLC*, 2018 U.S. Dist. Lexis 90342, at *2 (N.D. Ill. May 31, 2018).

[114] *See e.g., Aguilar v. Rexnord LLC*, 2018 U.S. Dist. LEXIS 110765 (N.D. Ill. July 3, 2018) (finding notice and consent violations do not without more create a risk of disclosure; quoting Howe, the court stated: "Proper compliance with BIPA's disclosure and written authorization requirements would only have made explicit what should have already been obvious."); *Goings v. UGN, Inc.*, 2018 U.S. Dist. LEXIS 99273 (N.D. Ill. June 13, 2018) (Plaintiff was aware that he was providing his biometric (fingerprint) data to defendants; case was nearly identical to Howe and remanded for lack of Article III standing).

plaintiff's BIPA and negligence claims to survive defendant's motion to dismiss.[115]

The pressure created by potential statutory damages, notwithstanding the lack of any real damages, cannot be overstated. After denying an earlier motion to dismiss on the basis of Rule 12(b)(1),[116] the U.S. District Court for the Northern District of California granted class certification for a group of Illinois users in *In re Facebook Biometric Info. Privacy Litigation*. The Court found that a class comprised of users located in Illinois for whom Facebook allegedly created and stored facial geometry information satisfied class certification requirements. Facebook, relying heavily on *Rosenbach v. Six Flags Entertainment Corp.*, a state appellate court opinion that stated BIPA required a showing of actual harm, argued there was no simple or unified way to show that all users had been "aggrieved."[117] The court disagreed, finding that BIPA did not require users to show injury or harm beyond statutory violation.[118]

Ironically, after the California court ruled on the Illinois statute, an Illinois federal court disagreed with the interpretations taken on by the California court. In *Rivera v. Google*, the Illinois court disagreed with *Facebook* and held that creation of facial geometries by Google for its own use does not create damages sufficient to confer standing because the photographed consumers were exposing their faces in public every day. Accordingly,

*the court found that the practice did not create a real threat of identity theft, which was the only real concern expressed by the Illinois legislature in enacting BIPA.*

[115] *Dixon v. Washington & Jane Smith Cmty.*, 2018 U.S. Dist. LEXIS 90344, at *29 (N.D. Ill. May 31, 2018).

[116] *Patel v. Facebook, Inc.*, 290 F. Supp. 3d 948 (N.D. Cal. 2018).

[117] *Rosenbach v. Six Flags Entm't Corp.*, 2017 IL App. (2d) 170317 (Ill. App. Ct. Dec. 21, 2017) (finding that BIPA required a showing of actual harm).

[118] *In re Facebook Biometric Info. Privacy Litig.*, 2018 U.S. Dist. LEXIS 63930 (N.D. Cal. Apr. 16, 2018).

Even looking under a traditional privacy tort analysis to assess "harm" beyond what the legislature expressed, the court found that the practice was not so outrageous as to be tortious because the geometries were of what people were already exposing in public.[119] Notably, there was no discussion of *Rosenbach*.

Interestingly, now that *Rosenbach* is on appeal before the Supreme Court of Illinois, the First District Illinois Appellate Court held in *Sekura v. Krishna Schaumburg Tan Inc.* that even without allegations of some additional injury, a plaintiff could maintain a BIPA claim simply by alleging noncompliance with the statute's procedural requirements.[120] The Illinois state courts are now officially split over the issue while awaiting additional direction from the state's highest court.

## C. PRODUCT LIABILITY LITIGATION

Privacy and security vulnerabilities in consumer goods and products have been the source of much debate these past few years, but plaintiffs have had a tough time finding good examples to make headway and create convincing precedence.

For example, in *Flynn v. FCA US LLC (Fiat)*, the plaintiffs alleged that the automobile manufacturer should be liable for cyber vulnerabilities in its connected cars. Although Fiat argued that no vehicles of the plaintiffs had actually been hacked, the lower court denied the manufacturer's motion to dismiss for lack of Article III standing, finding that the plaintiffs sufficiently alleged that they overpaid for their vehicles, which may be a viable theory.[121] But when the plaintiffs sought class certification, the court granted smaller state classes and denied larger national classes. The court found that it "would be unwieldly and would require highly individualized inquiries" to sort through the underlying state laws governing the implied warranty, fraud and products liability claims at issue.[122]

In contrast to *Flynn*, the Ninth Circuit affirmed the lower district court's refusal in *Cahen v. Toyota Motor Corp* to allow a case alleging cyber vulnerability against Toyota to proceed beyond the pleadings stage. In particular, as to the plaintiffs' unjust enrichment theory, the court noted, "plaintiffs have only made conclusory allegations that their cars are worth less and have not alleged sufficient facts to establish Article III standing."[123] And in *Williams-Diggins v. (Mercy) Health*, discussed supra, the Northern District Court of Ohio held that allegations of mere vulnerability on a HIPAA-covered entity's website, without any allegation of actual harm, were not sufficient to maintain "overpayment" claims brought by the plaintiff.[124]

As with more traditional examples of product liability litigation, organizations will likely best defend themselves with strong terms of use and disclosures. *In re VTech Data Breach Litigation*, for example, the plaintiffs alleged that defendant's connected toys contained cyber vulnerabilities. In granting VTech's motion to dismiss, the court made full use of VTech's written applicable terms and conditions. Importantly, the court found that no violation of the online services agreement were alleged. Then, the court found that implied contract allegations were subsumed by express contract allegations, dismissing the implied contract and implied warranty claims. The court proceeded to dismiss the unjust enrichment claims as well, along with the various consumer protection statutes.[125]

## D. SECURITIES LITIGATION

Until 2017, plaintiffs alleging loss to the value of their securities and stakeholder interests from privacy events have been relatively unsuccessful in securities class actions.[126] However, when plaintiffs in the Yahoo! breach derivative action reportedly obtained a $80 million settlement in early 2018, many experts feared that the "first major recovery" in a privacy-

[119] *Rivera v. Google, Inc.*, 2018 U.S. Dist. LEXIS 217710 (N.D. Ill., Dec. 29, 2018).

[120] *Sekura v. Krishna Schaumburg Tan Inc.*, 2018 IL App (1st) 180175 (Ill. App. Ct. Sept. 28, 2018).

[121] *Flynn v. FCA US LLC dba Chrysler Group LLC*, Case No. 15-0855 (S.D. Ill. Aug. 21, 2017).

[122] *Flynn v. FCA US LLC*, 2018 U.S. Dist. LEXIS 111963 (S.D. Ill. Jul. 5, 2018).

[123] *Cahen v. General Motors LLC*, 2017 U.S. App. LEXIS 26261, at *4 (9th Cir. Dec. 21, 2017).

[124] *Williams-Diggins v. Health*, 2018 U.S. Dist. LEXIS 206195 (N.D. Ohio, Dec. 6, 2018).

[125] *In re VTech Data Breach Litig.*, 2018 U.S. Dist. LEXIS 65060 (N.D. Ill. Apr. 18, 2018).

[126] *See e.g., Order, Davis v. Steinhafel*, D. Minn. Case No. 14-203, ECF 88 (July 7, 2016) (dismissing claims against board of directors of Target Corporation).

based securities class action would precipitate similar large settlements in other instances.[127]

Recent litigation suggests that plaintiffs still face substantial challenges in privacy-based securities class actions. In *PayPal Holdings, Inc., Securities Litigation*, for example, the plaintiff shareholders alleged they were misled by PayPal's press release on a data breach suffered by one of its acquisitions. Plaintiffs alleged that PayPal's initial discussions of the event were misleading because they failed to disclose the size and seriousness of the breach which, when later revealed, caused a sharp drop in PayPal's price.

In dismissing the case, the court noted that the plaintiffs were unable to demonstrate that PayPal knew of the actual size of the breach when it initially conducted its investigation. Although the plaintiffs were given an opportunity to amend, the court noted that the plaintiffs appeared to be having great difficulty demonstrating scienter.[128]

*PayPal* demonstrates an inherent problem with similar securities class actions: it would not be fruitful to accuse organizations disclosing privacy events to be lying in their statements when organizations are typically aware of the fact that they will be subject to immediate scrutiny and will be required to further update their findings later. It would likewise not be fruitful to contend that a disclosing organization is intentionally hiding privacy events, when the disclosure itself contradicts any such intent. At minimum, these inherent contradictions will likely continue make it difficult for most plaintiffs to show scienter.


[127] Kevin LaCroix, Yahoo Settles Data Breach-Related Securities Suit For $80 Million (The D&O Diary, Mar. 5, 2018), https://www.dandodiary.com/2018/03/articles/securities-litigation/yahoo-settles-data-breach-related-securities-suit-80-million/.

[128] *PayPal Holdings, Inc., Sec. Litig.*, 2018 WL 6592771 (N.D. Cal., Dec. 13, 2018).

# IV. DEVELOPMENTS IN REGULATORY ENFORCEMENT

## IV. DEVELOPMENTS IN REGULATORY ENFORCEMENT

Perhaps due in part to the international environment on privacy law, regulators are taking aggressive stances on privacy practices, many of which have been responsible for the technological growth in the U.S. for the past two decades.

It is important to note that while the FTC and State Attorneys General ("AGs") continue to be very active, the Office of Civil Rights ("OCR") and the Department of Health and Human Services ("HHS") continue to impose the highest fines per consumer through regulatory enforcement.

### A. The Federal Trade Commission

- *In re VTech*: In January 2018, the FTC entered into a $650,000 settlement with toymaker VTech for allegedly collecting personal information from hundreds of thousands of children without providing direct notice and obtaining their parents' consent, and for allegedly failing to take reasonable steps to secure the data.[129]
- *In re Prime Sites, Inc.*: In February 2018, Prime Site, Inc. settled FTC charges that it violated the Children's Online Privacy Protection Act ("COPPA") by collecting information of children under the age of 13 without proper parental consent and that it violated the FTC Act by misrepresenting benefits of an upgraded membership. The FTC alleged that Prime Site collected information of more than 100,000 users who were registered as under age 13, although its privacy policy stated it did not knowingly collect information of children under 13. Prime Site agreed to pay a civil penalty of $500,000, which will be suspended upon payment of $235,000. Prime Site also agreed to comply with COPPA requirements in the future and to delete information previously collected from children under the age of 13.[130]
- *In re Sears Holding Management*: In February 2018, the FTC approved a petition by Sears Holding Management company to reopen and modify a 2009 FTC order, whereby Sears settled charges with the FTC that it deceptively failed to disclose the extent of its software's data collection. The 2009 FTC Order required Sears to provide clear and prominent notice of any "Tracking Application" and to obtain express consent before downloading or installing the software. The FTC agreed with Sears' petition requesting that, as a result of changing circumstances and in the public interest, the definition of "Tracking Application" should be modified to exclude software that tracks only the configuration or software or application itself; information regarding whether the software or application is functioning as represented; or information regarding consumers' use of the software or application itself. The Commission vote approving Sears' petition was 2-0.[131]
- *In re Uber*: In October 2018, the FTC gave final approval to a settlement with Uber Technologies, Inc. Uber agreed to expand its proposed 2017 settlement with the FTC over charges that the company deceived customers about its privacy and data security practices. After the 2017 proposed settlement, the FTC allegedly discovered that Uber failed to disclose a 2016 breach during its FTC investigation. Under the new settlement, Uber could be subject to civil penalties if it fails to notify the FTC of certain future incidents involving unauthorized access to consumer information. Uber is also "prohibited from misrepresenting" how it monitors internal access

[129] Press Release, Electronic Toy Maker VTech Settles FTC Allegations That It Violated Children's Privacy Law and the FTC Act, FTC (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.

[130] Press Release, Online Talent Search Company Settles FTC Allegations it Collected Children's Information without Consent and Misled Consumers, FTC (Feb. 5, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/online-talent-search-company-settles-allegations-it-collected.

[131] FTC Approves Sears Holdings Management Corporation Petition to Reopen and Modify Commission Order Concerning Tracking Software, FTC (Feb. 28, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/ftc-approves-sears-holdings-management-corporation-petition.

to consumers' personal information and the extent to which it protects the privacy, confidentiality, security, and integrity of personal information. Uber must implement a comprehensive privacy program and for 20 years obtain biennial independent, third-party assessments, which it must submit to the Commission, certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order."[132]

- *In re PayPal, Inc.*: In May 2018, the FTC gave its final approval on its settlement with PayPal, Inc. involving allegations that its Venmo service violated the FTC Act and the GLBA. The FTC alleged that Venmo failed to disclose material conditions of external transfers and misled consumers about their privacy controls. Venmo also allegedly violated the GLBA by misrepresenting the "bank grade security system" protections. Venmo is now prohibited from making material misrepresentations regarding its services, privacy controls, and security levels. Venmo must also make certain disclosures to consumers, is prohibited from violating the GLBA, and must obtain biennial third-party assessments of its compliance with the settlement for 10 years.[133]
- *In re ReadyTech*: In July 2018, the FTC settled with ReadyTech Corporation, which provides online training services, over allegations that ReadyTech violated Section 5 of the FTC Act by falsely claiming it was in the process of certifying compliance with the EU-U.S. Privacy Shield Framework ("Privacy Shield"). The FTC alleged that while ReadyTech initiated an application with the U.S. Department of Commerce, it did not complete the required steps for certification. Because of the settlement, ReadyTech is prohibited from misrepresenting its participation in any government or industry sponsored privacy or security program and is also now required to comply with standard reporting and compliance requirements.[134]
- *In re BLU Products, Inc.*: In September 2018, the FTC settled with mobile phone manufacturer, BLU Products, Inc., and its co-owner over allegations that they made misrepresentations to consumers regarding their data collection and disclosure practices as well as their data security practices. The FTC further alleged that they failed to oversee their service providers and failed to implement appropriate security procedures, which resulted in the third party collecting more information from consumers than was necessary. As part of the settlement, BLU and its co-owner are prohibited from misrepresenting their data privacy and security practices and are required to maintain a comprehensive security program. BLU will undergo third-party assessments of its security programs for 20 years and be subject to record keeping and compliance monitoring requirements.[135]
- *In re IDmission, LLC; mResource LLC; SmartStart Employment Screening Inc.; and VenPath Inc.:* In September 2018, the FTC settled with four companies over allegations that they falsely claimed certification under the Privacy Shield framework. The FTC alleged that IDmission applied for Privacy Shield certification but never completed it, that SmartStart, VenPath, and mResource received the Privacy Shield certification in 2016 but allowed their certifications to lapse, and that VenPath and SmartStart failed to continue applying the Privacy Shield protections to personal information they collected while participating in the program. As part of the settlements with the FTC, all four companies must not misrepresent "the extent to which they participate in any privacy or data security program sponsored by the government or any self-regulatory or standard-setting organization, and must comply with FTC reporting requirements." Additionally, VenPath and SmartStart "must continue to apply the Privacy Shield protections

[132] Federal Trade Commission Gives Final Approval to Settlement with Uber, FTC (Oct. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/federal-trade-commission-gives-final-approval-settlement-uber

[133] FTC Gives Final Approval to Settlement with PayPal Related to Allegations Involving its Venmo Peer-to-Peer Payment Service, FTC (May 24, 2018), https://www.ftc.gov/news-events/press-releases/2018/05/ftc-gives-final-approval-settlement-paypal-related-allegations; Press Release, PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act, FTC (Feb. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.

[134] Press Release, California Company Settles FTC Charges Related to Privacy Shield Participation, FTC (July 2, 2018), https://www.ftc.gov/news-events/press-releases/2018/07/california-company-settles-ftc-charges-related-privacy-shield.

[135] FTC Gives Final Approval to Settlement with Phone Maker BLU, FTC (Sept. 10, 2018), https://www.ftc.gov/news-events/press-releases/2018/09/ftc-gives-final-approval-settlement-phone-maker-blu?utm_source=govdelivery.


to personal information they collected while participating in the program, protect it by another means authorized by the Privacy Shield framework, or return or delete the information within 10 days of the order."[136]

### B. HIPAA Enforcement

- *In re Fresenius Medical Care*: In February 2018, the medical care group agreed to pay $3.5 million for five data breaches at five of its locations in 2012. This was one of the largest OCR consent decrees of all time.[137]

[136] FTC Gives Final Approval to Settlements with Four Companies Related to EU-U.S. Privacy Shield, FTC (Nov. 19, 2018), https://www.ftc.gov/news-events/press-releases/2018/11/ftc-gives-final-approval-settlements-four-companies-related-eu-us

[137] Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules, U.S. DEP'T OF HEALTH & HUMAN SERVICES (Feb. 1, 2018), https://www.hhs.gov/about/news/2018/02/01/five-breaches-add-millions-settlement-costs-entity-failed-heed-hipaa-s-risk-analysis-and-risk.html.

- *In re Filefax, Inc.*: In February 2018, Filefax settled charges with OCR over allegations that Filefax violated HIPAA by failing to properly safeguard protected health information ("PHI"). Filefax allegedly allowed an unauthorized individual to transport PHI to a shredding facility but left the PHI in an unlocked truck and left it unsecured outside Filefax's facility. Although Filefax closed its doors during the OCR investigation, it was still found liable for its failure to comply with the law. Filefax agreed to pay $100,000 and to properly store and dispose of the remaining PHI in compliance with HIPAA.[138]
- *In re EmblemHealth*: In March 2018, EmblemHealth settled charges brought against it by the New York Attorney General alleging that Emblem Health violated HIPAA's requirement to safeguard PHI and violated New York's general business law by including policy holders' Social Security numbers on mailing labels of mail sent to them. EmblemHealth agreed to pay $575,000 and to conduct a comprehensive risk assessment.[139]
- *In re Virtua Medical Group*: In April 2018, Virtua Medical Group entered into a consent decree with the New Jersey Attorney General and the New Jersey Division of Consumer Affairs involving allegations that Virtua violated HIPAA and the New Jersey Consumer Fraud Act when the medical records of 1,650 patients were viewable on the internet due to a server misconfiguration by a third-party vendor. Allegedly, the third-party vendor inadvertently changed the web server when updating the software and allowed the FTP site hosting electronic protected health information ("ePHI") to be accessed without a password. While the exposure was a result of the third-party vendor, the New Jersey Attorney General and the New Jersey Division of Consumer Affairs held Virtua responsible as the owner of the data and therefore responsible for its protection. Virtua was also alleged to have violated HIPAA by failing to implement security awareness and training, implementing procedures relating to the ePHI maintained on its FTP site, and failing to maintain a written log of each time the FTP Site was accessed. Virtua agreed to pay civil penalties of $417,816, implement remediation measures, and report on such implementation to the Division 180 days after the settlement and every two years thereafter.[140]
- *In re University of Texas MD Anderson Cancer Center*: An HHS Administrative Law Judge granted OCR's motion for summary judgment, finding that MD Anderson violated HIPAA and required MD Anderson to pay penalties to OCR in the amount of $4,348,000. OCR investigated MD Anderson following three separate breaches of unencrypted devices. OCR concluded that while MD Anderson had written encryption policies and MD Anderson's own risk assessments noted that lack of device-level encryption posed significant risks of exposure of ePHI, MD Anderson nevertheless failed to timely adopt an enterprise-wide solution and failed to encrypt its devices. The HHS Administrative Law Judge rejected MD Anderson's arguments that it was not obligated to encrypt the devices and that the ePHI was for research and therefore not subject to HIPAA's nondisclosure requirements.[141]
- *In re Boston Medical Center*; In re Brigham and Women's Hospital; In re Massachusetts General Hospital: In September 2018, the OCR announced three separate settlements with three hospitals over potential violations of HIPAA, with agreed

[138] Consequences for HIPAA violations don't stop when a business closes, U.S. DEP'T OF HEALTH & HUMAN SERVICES (Feb. 13, 2018), https://www.hhs.gov/about/news/2018/02/13/consequences-hipaa-violations-dont-stop-when-business-closes.html.

[139] Allison Grande, NY AG Announces EmblemHealth Data Breach Settlement, LAW360 (Mar. 6, 2018), https://www.law360.com/articles/1019179/ny-ag-announces-emblemhealth-data-breach-settlement; A.G. Schneiderman Announces $575,000 Settlement With EmblemHealth After Data Breach Exposed Over 80,000 Social Security Numbers, NEW YORK STATE OFFICE OF THE ATTORNEY GENERAL (Mar. 6, 2018), https://ag.ny.gov/press-release/ag-schneiderman-announces-575000-settlement-emblemhealth-after-data-breach-exposed.

[140] Virtua Medical Group Agrees to Pay Nearly $418,000, Tighten Data Security to Settle Allegations of Privacy Lapses Concerning Medical Treatment Files of Patients, NEW JERSEY OFFICE OF THE ATTORNEY GENERAL (April 4, 2018), https://nj.gov/oag/newsreleases18/pr20180404b.html.

[141] Judge rules in favor of OCR and requires a Texas cancer center to pay $4.3 million in penalties for HIPAA violations, U.S. DEP'T OF HEALTH & HUMAN SERVICES (June 18, 2018), https://www.hhs.gov/about/news/2018/06/18/judge-rules-in-favor-of-ocr-and-requires-texas-cancer-center-to-pay-4.3-million-in-penalties-for-hipaa-violations.html.

settlement amounts totaling almost $1 million. Additionally, each entity must provide workforce training as part of a corrective action plan that will include OCR's guidance on disclosures to film and media. The three hospitals had invited film crews on their premises to film a television network documentary series without first obtaining authorization from patients.[142]

- In October 2018, a large medical insurance carrier agreed to pay a record $16 million to OCR and take substantial corrective action to settle potential HIPAA violations after a series of cyberattacks allegedly led to the largest U.S. health data breach in history and exposed ePHI of potentially 79 million people. In addition to impermissible disclosure of ePHI, OCR's investigation revealed that the carrier failed to conduct an enterprise-wide risk analysis, had insufficient procedures to regularly review information system activity, failed to identify and respond to suspected or known security incidents, and failed to implement adequate minimum access controls to prevent the cyber-attackers from accessing sensitive ePHI, beginning as early as February 18, 2018. The $16 million settlement exceeds the previous high of $5.55 million paid to OCR in 2016.[143]
- *In re Allergy Associations of Hartford*: In November 2018, Allergy Associates of Hartford, P.C. agreed to pay a $125,000 settlement to the OCR and to undertake a corrective action plan to settle potential HIPAA violations relating to one of its doctor's impermissible disclosure of a patient's PHI to a local television station reporter. OCR's investigations alleged that the doctor's discussions with the reporter demonstrated a "reckless disregard for the patient's privacy rights" and also revealed that Allergy Associates failed to take any disciplinary or correction action following the impermissible disclosure. OCR alleged that "[b]ecause egregious disclosure can lead to substantial penalties, covered entities need to pay close attention to HIPAA's privacy rules, especially when responding to press inquiries."[144]
- *In re Advanced Care Hospitalists PL*: In December 2018, the Florida physician contractor group agreed to pay $500,000 to settle multiple possible HIPAA violations stemming from sharing the unprotected PHI of over 9,000 individuals with an unknown vendor, allegedly without ensuring a business associate agreement was in place. Between November 2011 and June 2012, ACH worked with a third party who said he was from third-party billing company. The physician group gave the person protected health information for processing bills. In February 2014, a hospital told ACH that personal, demographic, and clinical information (including Social Security numbers, names and birthdays) from its patients was listed on the billing company's website. ACH also allegedly broke HIPAA rules by failing to put in place proper security measures. Until years after the breach, ACH, operational since 2005, had never conducted a risk analysis or implemented security safeguards. On top of the $500,000 it agreed to pay, ACH agreed to a corrective action plan and must provide HHS with the names of its business associates as well as any copies of business associate agreements it has with other parties and perform a full "enterprise wide risk analysis."[145]
- *In re Pagosa Springs Medical Center*: In December 2018, a medical center agreed to pay $111,400 to the OCR for failure to terminate a former employee's access to ePHI. In 2013, PMCA allegedly failed to deactivate the former employee's user name and password after separation such that the former employee

[142] Unauthorized Disclosure of Patient's Protected Health Information During ABC Television Filming Results In Multiple HIPAA Settlements totaling $999,000, U.S. DEP'T OF HEALTH & HUMAN SERVICES (Sept. 20, 2018), https://www.hhs.gov/about/news/2018/09/20/unauthorized-disclosure-patients-protected-health-information-during-abc-filming.html.

[143] Christopher Crosby, Insurer to Settle Health Care Data Breach For Record $16 Million (Law360, Oct. 15, 2018), https://www.law360.com/articles/1092533/anthem-to-settle-health-care-data-breach-for-record-16m.

[144] Allergy Practice Pays $125,000 to Settle Doctor's Disclosure of Patient Information to a Reporter, U.S. DEP'T OF HEALTH & HUMAN SERVICES (Nov. 26, 2018), https://www.hhs.gov/about/news/2018/11/26/allergy-practice-pays-125000-to-settle-doctors-disclosure-of-patient-information-to-a-reporter.html.

[145] Florida Contractor Physicians' Group Shares Protected Health Information With Unknown Vendor Without a Business Associate Agreement, U.S. DEP'T OF HEALTH & HUMAN SERVICES (Dec. 4, 2018), https://www.hhs.gov/about/news/2018/12/04/florida-contractor-physicians-group-shares-protected-health-information-unknown-vendor-without.html.

continued to have access to a Google web-based scheduling calendar, which included patients' protected health information. The failure resulted in improper sharing of health information (patient names, and in some instances, a statement of a procedure that was going to be performed) from 557 patients. PMCA also apparently did not have a business associate agreement in place with the scheduling vendor. The hospital was charged $100 per patient each time information was released. Following the breach, the hospital notified all affected patients in writing, published information about the breach in a local paper, and over the next two years, conducted an internal investigation and implemented a plan to prevent information from being released improperly again. In addition to these steps, PMCA will also have to complete a two-year action plan which requires staff training, updating security management, and revising agreements it must have with businesses before it can release patient information. [146]

### C. State AG Enforcement

- In January 2018, the New York Attorney General and a healthcare provider entered into a $1.15 million deal to end an investigation alleging the healthcare provider risked revealing the HIV status of 2,460 New Yorkers by mailing them information in transparent window envelopes.[147]
- In March 2018, a major retailer settled charges by the California Attorney General alleging that the retailer failed to properly manage disposal of hazardous materials and customer information, giving it an unfair advantage over its rivals. The parties settled for $27.84 million and a permanent injunction against similar violations.[148]
- *Massachusetts v. Equifax Inc.*: In April 2018, a superior court judge denied Equifax's motion to dismiss the Massachusetts Attorney General's action against it, holding that the Massachusetts Attorney General plausibly alleged that Equifax's failure to act on a known issue with respect to its data security violated Massachusetts's Standards for the Protection of Personal Information of Residents of the Commonwealth.[149]
- *In re Meitu Inc.*: In May 2018, Meitu and the New Jersey Attorney General signed a consent order involving allegations that Meitu violated COPPA by collecting their personally identifiable information through their photo editing apps without obtaining verifiable consent from parents or guardians of children under the age of 13. Meitu agreed to pay a penalty of $100,000 and agreed to provide clear and conspicuous notice of its privacy policy with notice of its information collection, use, and disclosure practices; to obtain verifiable consent

[146] *Colorado Hospital Failed to Terminate Former Employee's Access to Electronic Protected Health Information*, U.S. DEP'T OF HEALTH & HUMAN SERVICES (Dec. 11, 2018), https://www.hhs.gov/about/news/2018/12/11/colorado-hospital-failed-to-terminate-former-employees-access-to-electronic-protected-health-information.html.

[147] *A.G. Schneiderman Announces Settlement With Aetna Over Privacy Breach of New Yorker Members' HIV Status*, NEW YORK STATE OFFICE OF THE ATTORNEY GENERAL (Jan. 23, 2018), https://ag.ny.gov/press-release/ag-schneiderman-announces-settlement-aetna-over-privacy-breach-new-york-members-hiv.

[148] Mike Mills & Shannon Morrissey, *Another Hazardous Waste Enforcement Action Costs a Major Retailer Millions*, CALIFORNIA ENVIRONMENTAL LAW (Mar. 21, 2018), https://www.californiaenvironmentallawblog.com/environmental-contamination/another-hazardous-waste-enforcement-action-costs-a-major-retailer-millions/.

[149] Kat Greene, *Equifax Can't Skip Mass. AG Suit Alleging Security Failures*, LAW360 (April 4, 2018), https://www.law360.com/articles/1030065/equifax-can-t-skip-mass-ag-suit-alleging-security-failures.

from parents prior to collection, use, or disclosure; and to comply with COPPA's requirements.[150]

- *Multi-State Agencies adv. Equifax Inc.*: In June 2018, Equifax Inc. entered into a consent decree with multi-state regulatory agencies resulting from the 2017 Equifax data breach. The order requires Equifax to take a number of compliance measures, including reviewing and improving information security, improving oversight of the audit program, improving oversight and documentation of critical vendors and ensure sufficient controls to safeguard information consistent, improve standards for supporting patch management, and enhance oversight of IT operations relating to disaster recovery. The Equifax Board is required to submit to the Multi-State Regulatory Agencies a list of all remediation projects in response to the 2017 breach and must have independent third-party test controls relating to such projects and provide an update to the Multi-State Regulatory Agencies by December 31, 2018. The order is effective until it has been suspended, terminated, modified, or set aside by the Multi-State Regulatory Agencies.[151]
- *In re Unixiz*: In August 2018, the New Jersey Attorney General settled with Unixiz, the company that owned and operated the online social website "i-Dressup," alleging that it had violated COPPA and state consumer protection statutes, by failing to properly secure information and obtain verifiable parental consent. The investigation was initiated after media outlets began reporting that the website had been breached by an unknown hacker. In addition to injunctive relief, the company also agreed to pay $98,618 in civil penalties.[152]
- *In re LightYear Dealer Technologies LLC*: In September 2018, the New Jersey Attorney General settled with data management company, LightYear Dealer Technologies LLC d/b/a DealerBuilt, as a result of a data breach that exposed personal information of car dealership customers. The data breach occurred as a result of a misconfigured "file synchronizing program," which enabled unauthorized online access to the DealerBuilt databases containing unencrypted backup files. The personal data included names, addresses, Social Security numbers, driver's license numbers, and bank account information. DealerBuilt agreed to implement and maintain an information security program to be managed by a chief information security officer and to maintain proper encryption protocols for portable devices, among other requirements. DealerBuilt also agreed to pay $80,785, of which $49,420 is for civil penalties; the remainder is for attorneys' fees, investigation costs, and expert fees.[153]
- *In re Tiny Lab Productions et al.*: In September 2018,

*the New Mexico Attorney General filed suit against gaming company Tiny Lab Productions, alleging that it mislabeled its game as not being targeted towards children in contravention of COPPA.*

In addition, the New Mexico Attorney General filed suit against one of the mobile application store owners for offering the game, notwithstanding the alleged COPPA violations, in addition to a number of ad-tech and ad

[150] Jeannie O'Sullivan, *App Developer Collected Kids' Personal Info, NJ AG Says*, LAW360 (May 8, 2018), https://www.law360.com/articles/1041526/app-developer-collected-kids-personal-info-nj-ag-says; *NJ Division of Consumer Affairs Announces $100,000 Settlement with App Developer Resolving Investigation Into Alleged Violations of Children's Online Privacy Law*, NEW JERSEY OFFICE OF THE ATTORNEY GENERAL (May 8, 2018), https://nj.gov/oag/newsreleases18/pr20180508a.html.

[151] Consent Order, New York State Dep't of Financial Services (June 27, 2018), available at https://www.dfs.ny.gov/about/ea/ea180627.pdf.

[152] *Operator of Teen Social Website Breached by Hacker Agrees to Close Site and Reform Practices to Settle Allegations it Violated Children's Online Privacy Protection Act*, NEW JERSEY OFFICE OF THE ATTORNEY GENERAL Aug. 3, 2018), https://nj.gov/oag/newsreleases18/pr20180803a.html.

[153] Bill Wichert, *Software Co. Settles Auto Dealer Data Breach Claims in NJ*, LAW360 (Sept. 7, 2018), https://www.law360.com/cybersecurity-privacy/articles/1080689/software-co-settles-auto-dealer-data-breach-claims-in-nj?nl_pk=d100b429-aa27-499d-ad44-acee4f8fe74b&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy.

exchanges for embedding their SDKs within the game.[154] Although it is far from clear whether any of the defendants will ultimately be held liable, the case is important for all ad-tech companies, ad exchanges, and ecosystem owners to note. It appears that the New Mexico Attorney General has decided to take up the mantle formerly undertaken by the New York Attorney General, to not only investigate application "backdoors," but to also hold ecosystem owners liable.

- *In re UMass Memorial Medical Group, Inc.*; In re UMass Memorial Medical Center, Inc.: In September 2018, the medical groups agreed to pay a total of $230,000 to resolve claims stemming from two separate data breaches involving more than 15,000 Massachusetts residents. The breaches were perpetrated by two former employees who improperly accessed patients' personal and health information for fraudulent purposes. The information accessed included names, addresses, Social Security numbers, clinical information, and health insurance information, which the former employees used to open fraudulent cell phone and credit card accounts. In addition to the monetary penalty, the medical groups also agreed to: (1) conduct employee background checks and ensure proper employee discipline; (2) train employees on the proper handling of patient information; (3) limit employee access to patient information; (4) identify and remediate potential data security issues; and (5) promptly investigate suspected improper access to patient information.[155]
- *In re Uber*: In September 2018, Uber agreed to pay $148 million with all 50 states' enforcement officers over its 2016 data breach, which it allegedly paid hackers to resolve. The record monetary penalty and injunctive relief agreed to in the joint settlement agreement resolves allegations made by several states that Uber's failure to disclose the hack when it happened violated state data breach notification and data security statutes. The injunctive relief requires Uber to change its business practices to avoid future breaches and to reform its corporate culture. Specifically, Uber is required to incorporate privacy-by-design into its products, to hire a third-party to regularly assess its data security, and to implement a corporate integrity program that allows employees to report ethical concerns to Uber.[156]
- In October 2018, a large insurance carrier agreed to settle with four state AGs over claims involving the mailing of envelopes with transparent windows that revealed medical conditions. An investigation by these attorneys general resulted from two separate privacy breaches. The investigations concluded that the mailings may have contravened the insurance carrier's statements on its website that its insureds' personal health information would be reasonably safeguarded and afforded privacy protections. As a result of the settlement, the carrier agreed to enact policy, protocol and training reforms to protect individuals' health information, and ensure the confidentiality of mailings. The carrier also agreed to pay $365,211.59 to New Jersey in civil penalties (in addition to the $17 million settlement as a result of the class action lawsuit filed on behalf of individuals affected by the HIV/AIDS mailer incident). Connecticut and Washington D.C. each received $100,000 and $175,000 in settlement, respectively.[157]
- *In re ATA Consulting*: In November 2018, the New Jersey Attorney General settled with ATA Consulting over a data breach involving the medical records of patients through a server misconfiguration that allegedly resulted in patients' personal health information being made publicly available and searchable through common internet search engines. ATA transferred files with its client using a secured FTP site, but after the

[154] Jennifer Valentino-DeVries et al., *How Game Apps That Captivate Kids Have Been Collecting Their Data*, THE NEW YORK TIMES (Sept. 12, 2018), https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html; see also Complaint, State of New Mexico ex rel Hector Balderas, Attorney General v. Tiny Lab Productions et al., No. 18-00854 (D. New Mexico filed Sept. 11, 2018) .

[155] UMass Memorial Health Care Entities to Pay $230,000 to Resolve AG's Lawsuit Over Data Breaches (Mass Gov., Sept. 20, 2018), https://www.mass.gov/news/umass-memorial-health-care-entities-to-pay-230000-to-resolve-ags-lawsuit-over-data-breaches.

[156] *Hochman et al., Uber, States Strike $148M Deal to End Data Breach Dispute*, Law360 (Sept. 26, 2018), https://www.law360.com/articles/1086585/uber-states-strike-148m-deal-to-end-data-breach-dispute.

[157] *AG Grewal Reaches settlement With Aetna Over Privacy Violations*, NJ OFFICE OF THE AG (Oct. 10, 2018), https://www.nj.gov/oag/newsreleases18/pr20181010c.html.

client updated its software, ATA unintentionally misconfigured the web server, allowing the FTP Site to be accessed without a password. One patient's daughter located her medical records though a google search. The state launched an investigation and ultimately filed suit against ATA and its client, alleging that they had violated HIPAA's Security Rule, Breach Notification Rule, and Privacy Rule. ATA settled for $200,000 in civil fines and fees. The settlement also permanently bars owner from managing or owning a business in New Jersey.[158]

- In December 2018, the New York Attorney General settled a case where it alleged that an ad exchange company conducted billions of auctions for ad space on hundreds of websites the company knew were directed to children under the age of 13. The company agreed to pay $4.95 million in penalties and to adopt comprehensive reforms to protect children from improper tracking. This is the largest COPPA-related enforcement penalty to date in the U.S. The company agreed to implement functionality to indicate each website or portion of a website subject to COPPA and disclose to each third-party bidder that relevant ad space is subject to COPPA. It will also destroy all personal information it has collected from children.[159]
- *In re Target*: In December 2018, Target agreed to pay $7.4 million to resolve claims that it violated California law by improperly dumping hazardous waste, some of which included customer's confidential medical information. This settlement is in addition to the 2011 settlement between Target and the California Attorney General over other environmental violations. Since the 2011 settlement, the California Attorney General conducted further inspections and found new environmental violations. Target allegedly improperly dumped electronics, batteries, aerosol cans, compact fluorescent light bulbs, medical waste, pharmaceuticals, and confidential customer medical information into landfills.[160]
- *In re Western Union Financial Services, Inc.; In re Priceline.com LLC; In re Equifax Consumer Services, LLC; In re Spark Networks Inc.*; and In re Credit Sesame Inc.: In December 2018, the New York Attorney General settled its claims against five companies for vulnerabilities in their mobile applications that failed to keep personal information safe during transmission. Because the enforcement took place before user information was actually stolen, no money was exchanged as part of the settlement.[161]
- *In re Yapstone*: In December 2018, the Massachusetts Attorney General settled its claims against the payment processor for alleged online vulnerabilities, in exchange for $155,000 and certain security commitments.[162]

### D. Other Administrative Enforcement Efforts

- In February 2018, the North American Electric Reliability Corp. ("NERC") reached a settlement with an unnamed power company to resolve two violations alleging failure to protect critical cyber assets. Allegedly, a third-party contractor of the power company improperly copied data to its unprotected network. The data included IP addresses and host names, as well as other critical cyber assets. The data was exposed for 70 days, though there was no evidence anyone other than a researcher, who tipped off the NERC, had downloaded the data. The power company

[158] *Defunct Georgia Vendor Responsible For Exposing Virtua Medical Group Patient Files Online Agrees to $200,000 Settlement*, NJ Office of the AG (Nov. 2, 2018), https://www.nj.gov/oag/newsreleases18/pr20181102a.html.

[159] *A.G. Underwood Announces Record COPPA Settlement With Oath – Formerly AOL – For Violating Children's Privacy*, NEW YORK STATE OFFICE (Dec. 4, 2018), https://ag.ny.gov/press-release/ag-underwood-announces-record-coppa-settlement-oath-formerly-aol-violating-childrens.

[160] Hailey Konnath, *Target Inks $7.4M Deal Over Calf. Waste Disposal Claims*, LAW360 (Dec. 6, 2018), https://www.law360.com/articles/1108522/target-inks-7-4m-deal-over-calif-waste-disposal-claims.

[161] *A.G. Underwood Announces Settlements With Five Companies Whose Mobile Apps Failed to Secure User Information Transmitted Over The Internet*, New York State Office (Dec. 14, 2018), https://ag.ny.gov/press-release/ag-underwood-announces-settlements-five-companies-whose-mobile-apps-failed-secure-user.

[162] *Payment Processor to Pay $155,000 Over Data Breach Affecting Thousands of Massachusetts Residents*, MASS.GOV) (Dec. 19, 2018), https://www.mass.gov/news/payment-processor-to-pay-155000-over-data-breach-affecting-thousands-of-massachusetts.

self-reported the breach, agreed to a $2.7 million penalty, and agreed to carry out a mitigation plan to improve its security systems.[163]

- *In re AMP Global Clearing LLC*: In February 2018, the U.S. Commodities Futures Trading Commission ("CFTC") settled charges against a futures commission merchant, AMP Global Clearing LLC, for its failure to diligently supervise an IT provider's implementation of its written information security program, resulting in a data breach of customer records and information. The vulnerability existed for 10 months, and an unauthorized actor had even blogged about exploiting the vulnerability. AMP paid $100,000 in penalties and agreed to cease and desist from future violations of the Regulation.[164]
- *In re Mizuho Securities USA LLC*: In July 2018, the SEC settled charges against Mizuho Securities USA LLC for alleged failures to safeguard information, including failing to maintain and enforce policies and procedures aimed at preventing misuse of material nonpublic information. The SEC charged Mizuho for regularly disclosing material nonpublic customer information to other traders and to its hedge fund clients in violation of Section 15(g) of the SEC Act of 1934. The settlement included a penalty of $1.25 million, a censure, and a cease and desist order from committing future violations.[165]
- *In re Voya Financial Advisors Inc.*: In September 2018, the SEC obtained a $1 million settlement for its first action under its "ID Theft Rule." Voya also agreed to retain an independent third party to evaluate its policies and procedures for compliance. The SEC brought charges against Voya relating to a cyber incident that compromised personal information of thousands of customers and alleged that Voya's cybersecurity policies and procedures failed to adequately protect confidential customer information.[166]
- *In re Source for Public Data, L.P.*: In September 2018, the Fifth Circuit reversed the District Court's order granting the CFPB's petition to enforce a civil investigative demand (CID), holding that the CFPB did not comply with the governing statute when it issued the CID. Specifically, the Fifth Circuit found that the CID did not state the "conduct constituting the alleged violation which is under investigation" and did not identify "the provision of law applicable to such violation" as required under the applicable statute. The Court concluded that "the CFPB does not have 'unfettered authority to cast about for potential wrongdoing.' . . . As such, it must comply with statutory requirements, and here it did not."[167]

[163] Keith Goldberg, *Power Co. Fined $2.7M For Exposing Critical Grid Data*, LAW360 (Mar. 5, 2018), https://www.law360.com/articles/1018678/power-co-fined-2-7m-for-exposing-critical-grid-data; NERC Full Notice of Penalty Regarding Registered Entity, FERC Docket No. NP18-_-000, North American Electric Reliability Corporation (Feb. 28, 2018), available at https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_CIP_NOC-2569%20Full%20NOP.pdf.

[164] *CFTC Brings Cybersecurity Enforcement Action*, HUNTON PRIVACY & INFORMATION SECURITY LAW BLOG (Feb. 14, 2018), https://www.huntonprivacyblog.com/2018/02/14/cftc-brings-cybersecurity-enforcement-action/; George Lynch & Daniel R. Stoller, Futures Regulator, Broker Settle Lax Cybersecurity Charges, BLOOMBERG BNA (Feb. 15, 2018), https://www.bna.com/futures-regulator-broker-n57982088869/.

[165] Press Release, *SEC Charges Mizuho Securities for Failure to Safeguard Customer Information U.S. Securities and Exchange Comm'n* (July 23, 2018), available at https://www.sec.gov/news/press-release/2018-140.

[166] *SEC Charges Firm With Deficient Cybersecurity Procedures*, SEC (Sept. 26, 2018), https://www.sec.gov/news/press-release/2018-213; see also Petrick, SEC Gets $1M In First Action Under ID Theft Rule (Law360, Sept. 26, 2018), https://www.law360.com/articles/1086479/sec-gets-1m-in-first-action-under-id-theft-rule.

[167] *Consumer Fin. Prot. Bureau v. Source for Pub. Data*, L.P., 903 F.3d 456 (5th Cir 2018).

# V. NOTABLE INTERNATIONAL DEVELOPMENTS

## A. Developments in the EU Regarding the GDPR and Privacy Class Actions

It has been less than a year since the European Union's GDPR went into effect in May 2018. While private organizations and data protection authorities ("DPAs") are still getting acquainted, a number of lessons have emerged. The following developments have important implications for any organization looking to provide data-based services or products to EU residents, as the full ramifications of the GDPR become further defined:

- The "Transparency Guidelines" of the Article 29 Data Protection Working Party ("WP29") require that organizations making changes to comply with the GDPR highlight such changes, that disclosures be provided in "clear and plain language," and that disclosures should be available to data subjects in one single place that shall be continually easily accessible to them thereafter, and that "substantive and material" changes made to the privacy statement shall be communicated to data subjects in the same manner disclosures were initially made.[168]
- European countries and courts may ask companies to change online terms and conditions that they consider "abusive." [169]
- WP29's "Guidelines on Automated Individual Decision-Making And Profiling" will likely make autonomous technologies and artificial intelligence ("AI") very difficult to implement. Specifically, the guidance arguably limits AI from processing data in ways different from the initial purposes of collection (e.g., further derivations of use), imposes data minimalization, and requires data storage limitations. These constraints will likely be significant limiters to research and developments that were the genesis of current AI technologies.[170]
- Where a non-EU organization intends to use consent as the mechanism for onward transfers en masse, the organization may need to report and justify why it is not using another exemption mechanism to the DPA to whom it reports.[171]
- Honoring data subjects' rights and requests to delete data can be a time-consuming process that takes months to complete. [172]
- Europe's "right to be forgotten" (RFBT) may extend even to indefinitely newsworthy information, such as information on a search engine about a man who had previously been convicted of murder.[173]
- Some in the EU intend to argue that RFBT should be honored even outside of European borders, not just within.[174]

[168] Muge Fazlioglu, *What's New In WP29's Final Guidelines On Transparency*, IAPP (Apr. 18, 2018), https://iapp.org/news/a/whats-new-in-wp29s-final-guidelines-on-transparency/.

[169] *French Court Orders Twitter to Change Smallprint After Privacy Case*, PHYS.ORG (Aug. 10, 2018), https://phys.org/news/2018-08-french-court-twitter-smallprint-privacy.html.

[170] *Guidelines On Automated Individual Decision-Making And Profiling For The Purposes of Regulation* 2016/679, DATA PROTECTION WORKING PARTY (Aug. 22, 2018), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[171] *See International Transfers*, INFORMATION COMMISSIONER'S OFFICE (Sept. 20, 2018, 10:57 AM) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

[172] Eric Chiang, *Deleting Your Data In Google Cloud Platform*, GOOGLE CLOUD BLOG (Sept. 13, 2018), https://cloud.google.com/blog/products/storage-data-transfer/deleting-your-data-in-google-cloud-platform.

[173] *Finnish Court Issues Precedent "Right to Be Forgotten" Decision For Google to Remove Data*, UUTISET (Aug. 17, 2018), https://yle.fi/uutiset/osasto/news/finnish_court_issues_precedent_right_to_be_forgotten_decision_for_google_to_remove_data/10358108.

[174] Mark Scott, *Europe's High Court Wades Into Google Privacy Fight*, POLITICO (Sept. 10, 2018), https://www.politico.eu/article/google-right-to-be-forgotten-privacy-ecj/; but Europeans appear divided on the issue, see Sam Schechner, *EU Opposes France on Global "Right to Be Forgotten"*, THE WALL STREET JOURNAL (Sept. 17, 2018).

- Even if no fines are ultimately imposed, DPAs may instead issue swift "stop processing" orders under the GDPR.[175]
- EU commission officials have reported that "new" EU GDPR fines will be issued for "old" and unreported data breaches.[176]

Notably, one of the biggest developments in the EU that will likely affect how seriously companies take the GDPR is the EU's recent promulgation of class action rules for privacy class actions. In 2018, a UK court refused to allow claims against an American ecommerce company for mobile phone tracking to proceed as a class action.[177] The class action process is still very limited in the EU as a means for consumers to aggregate relief. And as all class action lawyers know, if a class with a relatively small number of individual claims cannot be certified to proceed as a class, interest in the claims will often be lost altogether.

In December 2018, the EU approved rules that would allow groups of individuals to seek compensation through collective actions, including for privacy violations, against businesses. [178]

**B. New Privacy Legislation Under Consideration in China**

On June 27, 2018, China's Ministry of Public Security published the Draft Regulations on The Classified Protection of Cybersecurity for public commentary.

*The draft regulation is an interesting attempt to combine cybersecurity, legal data processing, and "national security" for the incumbent Chinese regime.*

Network operators are required to: (1) assess their grade; (2) file and report their "grade"; (3) protect network infrastructure, operation, and data and information; (4) guard against "cybercrimes"; (5) construct and ratify commensurate cybersecurity safeguards and procedures; and (6) effectively handle and report network security accidents. The obligations of operators will differ across different grades, which are evaluated across different classified levels dependent on considerations of network functions, scope of services, types of service recipients, and types of data processed.

| The Degree of Injury Suffered | | | |
|---|---|---|---|
| **Type of Injury** | **General Damage** | **Serious Damage** | **Extremely Serious Damage** |
| Legitimate Interests of Citizens, Legal Entities, And Other Organizations | Level 1 | Level 2 | Level 3 |
| Social Order and Public Interests | Level 2 | Level 3 | Level 4 |
| National Security | Level 3 | Level 4 | Level 5 |

The following obligations should be noted:

- Online events must be reported to local public security authorities within 24 hours, which may require concurrent reports to the local secrecy administration with jurisdiction over the matter.
- For networks graded Level 2 and above, the operator is required to conduct an expert review and seek approval from the relevant industry regulators.
- For networks graded Level 3 and above, the responsible organizations must create and designate specific procedures for any material changes in their networks and operations, review their network plans and strategies with technical professionals, conduct background checks on key personnel, manage the security of service providers, and constantly monitor and report their cybersecurity findings to relevant authorities. In

[175] Miranda Jang, *Cease Processing Orders Under GDPR: How The Irish DPA Views Enforcement*, IAPP (Aug. 28, 2018), https://iapp.org/news/a/cease-processing-orders-under-the-gdpr-how-the-irish-dpa-views-enforcement/.

[176] Peter Teffer, *New EU Fines Will Apply to "Old" Data Breaches*, EUOBSERVER (Apr. 9, 2018), https://euobserver.com/justice/141548

[177] Ben Kochman, *Google Escapes UK Suit On IPhone Snooping Claims*, LAW360 (Oct. 9, 2018), https://www.law360.com/articles/1090289/google-escapes-uk-suit-on-iphone-snooping-claims.

[178] Najivya Budaly, *EU Approves Class Action Rules Amid Calls For Safeguards*, LAW360 (Dec. 6, 2018), https://www.law360.com/articles/1108607/eu-approves-class-action-rules-amid-calls-for-safeguards.

addition, maintenance of Level 3 and above must be conducted in China.[179]

The final version of the regulation is not expected to substantially differ from the draft version.

### C. "Meaningful Consent" Guidance in Canada

The Office of the Privacy Commissioner of Canada (the "Office") announced that it intends to enforce new "meaningful consent" rules for online activities starting January 1, 2019. The Office stated that the new rules are meant to "work to improve the current consent model under the Personal Information Protection And Electronic Documents Act ("PIPEDA")." [180]

According to the Office, organizations are expected to be guided by the following principles in obtaining "meaningful consent":

1. Emphasize key elements, including: (i) what personal information is being collected; (ii) which parties the personal information will be shared with, (iii) for what purposes personal information is collected, used or disclosed; and (iv) the risk of harm and other consequences;
2. Allow individuals to control the level of detail they get and when;
3. Provide individuals with clear options to say "yes" or "no";
4. Be innovative and creative;
5. Consider the consumer's perspective;
6. Make consent a dynamic and ongoing process, which includes providing some interactive and dynamic ways to anticipate and answer users' questions and notifying users and obtaining additional consent when organizations plan to introduce significant changes to its privacy practices;
7. Be accountable and be ready to provide demonstrate compliance.

The new guidance is important because it suggests that while Canada has historically been relatively lenient with enforcing PIPEDA against online activities, it intends to become more active going forward. Companies should not take the release of the guidelines lightly. «

[179] *China Publishes The Draft Regulations On The Classified Protection of Cybersecurity*, HUNTON PRIVACY & INFORMATION SECURITY LAW BLOG (Jul. 17, 2018), https://www.huntonprivacyblog.com/2018/07/17/china-publishes-draft-regulations-classified-protection-cybersecurity/.

[180] *Guidelines For Obtaining Meaningful Consent* (Office of the Privacy Commissioner of Canada, May 2018), https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

# VI. CONTACTS


**Mark C. Mao**
Partner
*San Francisco*
mark.mao@troutman.com
415.477.5717

**Ronald I. Raether, Jr.**
Partner
*Orange County*
ron.raether@troutman.com
949.622.2722

**Stacy R. Hovan**
Counsel
*San Francisco*
stacy.hovan@troutman.com
415.477.5747

**Timothy Butler**
Associate
*Atlanta*
timothy.butler@troutman.com
404.885.3697

**Molly DiRago**
Associate
*Chicago*
molly.dirago@troutman.com
312.759.1926

**Oscar A. Figueroa**
Associate
*Orange County*
oscar.figueroa@troutman.com
949.622.2743

**Julie D. Hoffmeister**
Associate
*Richmond*
julie.hoffmeister@troutman.com
804.697.1448

**Yanni Lin**
Associate
*San Francisco*
yanni.lin@troutman.com
415.477.5738

**Katharine Malone**
Associate
*San Francisco*
katharine.malone@troutman.com
415.477.5755

**Sadia Mirza**
Associate
*Orange County*
sadia.mirza@troutman.com
949.622.2786

**Sheila M. Pham**
Associate
*San Francisco*
sheila.pham@troutman.com
415.477.5728

**Jonathan Yee**
Associate
*Orange County*
jonathan.yee@troutman.com
949.622.2758

**Dan Waltz**
Attorney
*Chicago*
daniel.waltz@troutman.com
312.759.5948