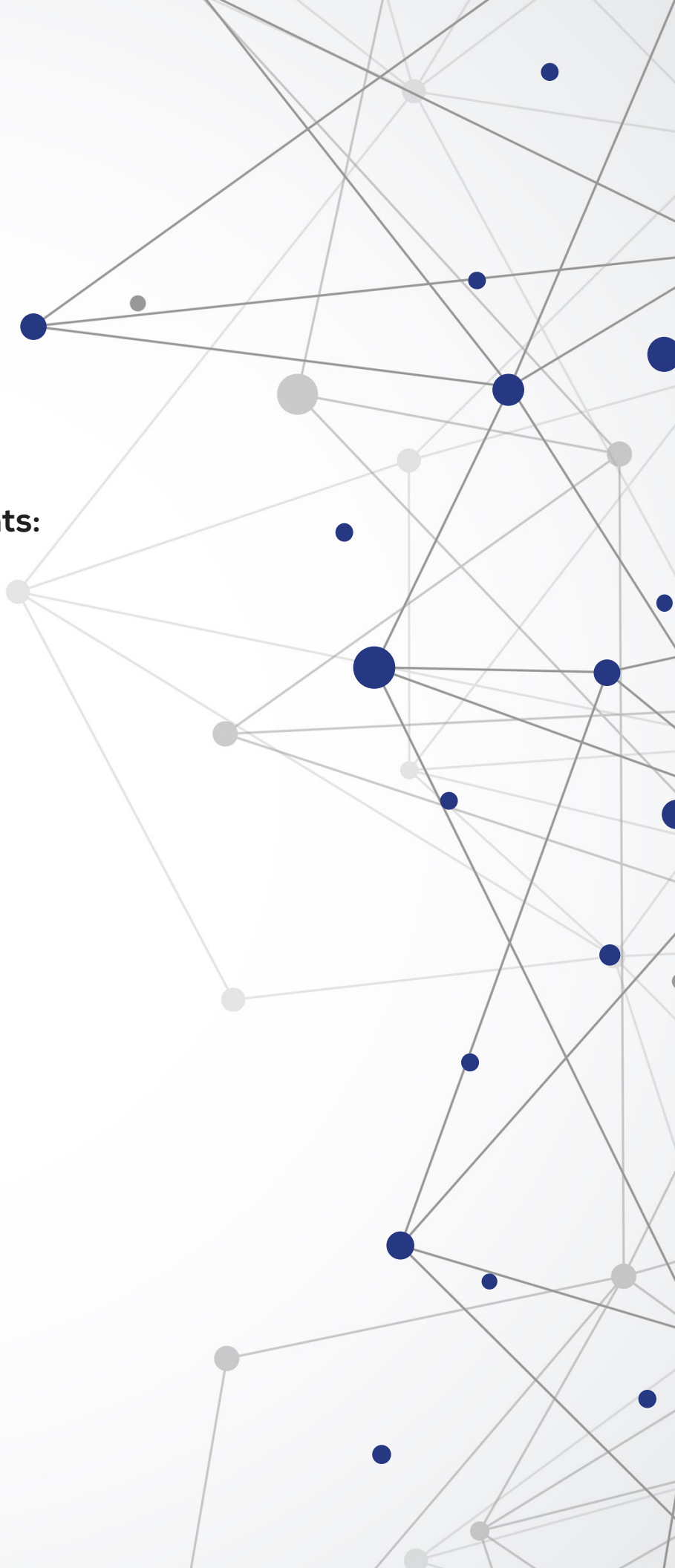
BSF | BOIES SCHILLER FLEXNER



Boies Schiller Flexner Insights:

Annual Global Data Privacy Review

Volume 2 | January 2020

The following Boies Schiller Flexner lawyers assisted in the preparation of this client alert: Mark Mao, James Lee, Albert Giang, Matthew Getz, Michael Jacobs, Matthew Chou, Yanni Lin, Diana Liu, Gabriel Schlabach, and Stephen Wilson.

I. INTRODUCTION

The purpose of this guide is to summarize for our readers developments in privacy law in 2019. Because our world increasingly relies on technology and because technology is often "data driven," privacy law has become more important than ever.

As connected things ("Internet of Things" or "IoT") explode in popularity, the resulting wealth of real-time data make new technologies such as augmented reality (AR) and autonomous vehicles possible. 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. While newer technologies are increasingly data-reliant, they also yield far richer data than older technologies, helping to increase technological performance across all verticals.

Despite all the contributions technology companies have made to increase quality of life, they are now under assault from across the political spectrum. While critics attack companies for their use of data, few have provided viable alternatives for how the American economy should continue to innovate in the face of increased international technological competition. For example, there have been no feasible proposals on how to provide the "just in time" notices demanded within the IoT environment, where most devices may not even have a user-interface.

Regardless, companies whose data collection practices may impact EU residents now face heavy fines for non-compliance with the EU's General Data Protection Regulation (GDPR), which went into effect on May 25, 2018. As of the date of this publication, authorities in the EU have issued significant fines against global corporations that have been found to have violated the GDPR.

Similarly, several U.S. states and cities followed with their own versions of legislation and proposals that capture elements of the GDPR, most prominently, the California Consumer Privacy Act (CCPA), effective January 1, 2020. It remains to be seen whether these localized efforts will create sufficient momentum to help push through a serious federal proposal. State initiatives such as the CCPA may instead fragment the U.S. privacy law landscape rather than unite it under a truly comprehensive federal regulation scheme.

Amidst this global, legal, and political fragmentation on data use, the need for thoughtful privacy design and strategies will be an important differentiator for technology companies. Organizations should strive to remain informed of recent enforcement actions, legal cases, and laws to determine how their technology offerings may be impacted.

BSF is proud of its history of tackling difficult legal and business challenges on behalf of some of the world's largest technology companies. We hope that this desk reference will be helpful in explaining how to better navigate privacy developments across global markets in 2020.

II. NEW LEGISLATION, REGULATIONS, AND INDUSTRY GUIDANCE

While Europe's GDPR is purportedly based on certain recitations of fundamental rights, American privacy law has evolved from a combination of the laws and regulations governing specific sectors, civil case law and regulatory consent decrees limited to their facts, and the contractual norms and practices of the tech industry.

The laws and regulations promulgated in 2019 have not helped to simplify or unify American privacy law. While these laws continue to recite their dedication to "reasonable standards" for the protection of privacy, they generally do not provide concrete guidance on what is permissible.

A. FEDERAL LEGISLATION & REGULATIONS

1. Trump Administration Proposed Regulation of Foreign Investment in Data-Based Products

In late 2018, the Trump Administration announced in the Federal Register its initiative to examine foreign investments in U.S. companies and technologies.[1] Around the same time, the Commerce Department's Bureau of Industry and Security published an advance notice of proposed rulemaking ("ANPRM") in the Federal Register relating to export controls of "emerging technologies" essential to U.S. national security.[2] The non-exhaustive list of flagged technologies includes many of those having substantial consumer-facing applications, such as:

- "Additive manufacturing," including 3D printing;
- Advanced surveillance technologies, including faceprinting and voiceprinting;
- Artificial intelligence and machine learning technologies, including those involved in computer vision, speech, and audio learning and processing;
- Brain-computer interfaces;
- "Data analytics technologies," which is broadly worded and includes visualization, contextualization, and automated analysis algorithms;
- Physical positioning, navigation, and timing technologies;
- Quantum computing, encryption, and sensing technologies;
- Robotics, particularly mini-drone and molecular robots; and
- "Sensing" technologies, which again is broadly worded.[3]

Although it is unclear what export controls will be imposed, many technology companies are already expressing fear that such restrictions will lead to retaliation against similar U.S. technologies abroad.[4]

2. FERC Regulations On Electrical Grid And Critical Infrastructure

On June 20, 2019, the Federal Energy Regulatory Commission (FERC) approved Critical Infrastructure Protection ("CIP") 008-6.[5] Importantly, the new rules now make it mandatory for "Responsible Entities" to report both cyber incidents that have resulted in an actual compromise of high and medium-impact bulk electric systems (BES), and attempts to so compromise such systems. These new rules also impose certain administrative requirements, in addition to testing and documentation consistent with general cybersecurity standards recommended by the National Institute of Standards and Technology (NIST).

First, CIP 008-6 now requires notification of "Reportable Cyber Security Incidents" (i.e., an actual compromise or disruption) within one hour, and notification of "Cyber Security Incidents" (i.e., a malicious or suspicious event that compromises or an was attempt to compromise) within the following calendar day.[6] Responsible Entities shall notify the Electricity Information Sharing and Analysis Center (E-ISAC), and if subject to the jurisdiction of the United States, also the United States National Cybersecurity and Communications Integration Center (NCCIC).[7]

Second, CIP 008-6 now imposes specific ongoing planning and compliance requirements on Responsible Entities:

[1] *See* 31 C.F.R. §§ 801.101, 801.204(f) (2018).
[2] Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201 (proposed Nov. 19, 2018) (to be codified at 15 C.F.R. pt. 744), https://www.govinfo.gov/content/pkg/FR-2018-11-19/pdf/2018-25221.pdf.
[3] *Id.*
[4] Emily Feng, *Stopping Key Tech Exports to China Could Backfire, Researchers and Firms Say*, NPR (May 14, 2019), https://www.npr.org/2019/05/14/722933448/stopping-key-tech-exports-to-china-could-backfire-researchers-and-firms-say.
[5] 167 FERC ¶ 61,230.
[6] FERC, CIP 008-6, Table R4, Part 4.2, at 14.
[7] FERC, CIP 008-6, Section A.R4, at 13.

- Responsible Entities must: a) delineate processes to "identify, classify and respond to cyber incidents," b) define criteria that "evaluate and define attempts to compromise applicable systems," and c) define roles and responsibilities of all response groups or individuals and detailed handling procedures.[8]

- Responsible Entities must test their incident response plans "at least once every 15 calendar months" – although having suffered a reportable incident would count towards satisfying the requirement.[9] Regardless, when responding to an actual or suspected attack, Responsible Entities must document the incident and any deviation from the actual response plan. This includes "dated evidence of a lessons-learned report," with a summary of written documentation of logs, notes, and the like from the test.[10]

- Within 90 days of either an applicable cybersecurity test, or following an actual cybersecurity compromise or disruption, Responsible Entities must document any lessons learned, update applicable cybersecurity response plans, and notify all persons with responsibilities under the plan of any changes. How individuals were notified of the changes must also be documented.[11]

- Initial reporting of incidents must include information on the functional impact, the attack vector used, and the level of intrusion achieved or attempted. Subsequently, however, Responsible Entities must also provide updates within seven days on any known changes to the reported information.[12]

The implementation deadline for CIP 008-6 will be December 2020.

While CIP 008-6 does not currently affect low-impact BES entities, FERC mandated further review of the current cybersecurity practices of low-impact systems and made recommendations about what new requirements, if any, should be imposed on those systems as well. The White House has already made clear that cybersecurity risks to the electric grid are of utmost concern, as demonstrated in Executive Orders 13800 and 13777.[13]

B. STATE LEGISLATION & REGULATIONS

1. The California Consumer Privacy Act & Proposed Attorney General Regulations

The California Consumer Privacy Act (CCPA), as amended, was effective January 1, 2020. Although many organizations are immediately focused on revisions to their privacy policy, the true costs of the CCPA will be in the form of the technical and business investments required for compliance.

Summary of the CCPA

The definition of Personal Identifying Information (PII) under the CCPA, what CCPA calls "personal information," departs from how U.S. industries have traditionally used the term. The Act requires notice and opt-outs, but in some cases opt-ins, for any business that exchanges consumer data with another for consideration. In addition, companies keeping such data must invest in technical and business solutions that will allow consumers ease of access to their data and sharing histories. CCPA will require businesses to be thoughtful about how they handle data incidents and the subsequent notice-to-cure requests.

The CCPA's Definition of PII Departs from Prior U.S. Usage

Under the CCPA, "personal information" is anything that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including "via a device."[14] This means that the CCPA considers any data that may be associated with both individuals and households to be PII, in addition to immutable identifiers such as Social Security numbers typically referenced by data breach statutes.[15]

Furthermore, the CCPA narrows permissible deidentification techniques, often referenced in adtech and emerging-technology transactions. For PII to be considered "deidentified," the information "cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer." The business claiming the information has been deidentified must also: (a) have implemented technical safeguards and business processes to prevent reidentification, (b) have implemented business processes to prevent inadvertent releases, and (c) make no attempt to reidentify the information. [16]

Using PII under the CCPA Requires Notice and Opt-Outs for Most Situations, but Opt-Ins for Others

To use PII, a covered business must provide notice and obtain consent from consumers from whom it collects data, specifically:

- Businesses that "sell" PII shall provide notice to consumers and give consumers the right to opt out of the sale of their personal information.[17] Importantly, the CCPA defines "selling" very broadly, and includes making PII available in any matter for any type of monetary or non-monetary consideration.[18]

[8] FERC, CIP 008-6, Table R1, Part 1.1–1.3, at 5–7.
[9] FERC, CIP 008-6, Table R2, Part 2.1, at 8.
[10] *Id.*
[11] FERC, CIP 008-6, Table R3, Part 3.1, at 11.
[12] FERC, CIP 008-6, Table R4, Part 4.3, at 14.
[13] *See* Keith Goldberg, *FERC Approves Boost in Grid Cybersecurity Standards,* Law360 (June 21, 2019), https://www.law360.com/articles/1171625/ferc-approves-boost-in-grid-cybersecurity-standards.
[14] Cal. Civ. Code §§ 1798.140(a), 1798.140(o).
[15] Cal. Civ. Code § 1798.140(o).
[16] Cal. Civ. Code § 1798.140(h).
[17] Cal. Civ. Code §§ 1798.115(d), 1798.120(a), 1798.120(d).
[18] Cal. Civ. Code § 1798.140(t)(1).

- For consumers between the ages of 13-16, businesses must obtain the consumers' affirmative authorization before they sell personal information. For consumers under the age of 13, businesses must obtain affirmative authorization from the consumers' parent or guardian before they sell personal information.[19]

One of the largest areas of ambiguity and concern is how corporate affiliates sharing information might be deemed to be "selling" of information between two separate parties. While corporate affiliates might be permitted to use the information for products and services, rarely do they compensate each other financially for the information that they receive. Furthermore, because the information stays within the hands of entities subject to common ownership, consumers arguably do not perceive the differences amongst the entities at all.

Nonetheless, the CCPA broadly defines the term "sale" as including the act of "disclosing" or "making available" personal information "for monetary or other valuable consideration" from one "business" to another.[20] The CCPA further states that two entities under common ownership are considered separate "businesses" unless they "share… common branding."[21] For the purposes of the statute, "common branding" is defined as a "shared name, servicemark, or trademark."[22]

Absent legislative or regulatory clarification, it appears that portfolio companies using a single logo across all affiliated companies without much differentiation amongst the affiliates in public-facing documents face the least risk of being deemed separate businesses under the CCPA. As affiliated companies differ in their use of logos, or where they specifically differentiate themselves from sister companies in public-facing documents notwithstanding a "common name," their risk of being deemed a fleet of separate "businesses" as opposed to one unitary business for the purposes of the CCPA likely increases.

Companies Must Invest in Technical and Business Solutions That Will Allow Consumers Ease of Access to Their PII and Sharing Histories

To continue using harvested PII, even after having consumer consent, a business must provide the following access rights to consumers:

- Accounting of information the business collected and received, including from where the information was collected, for what it was used, and with whom the information was shared.[23]

- Provide a portable copy of the PII of the consumer collected by the business upon request.[24]

- Provide a clear and conspicuous link for consumers on its website homepage to readily allow consumers the ability to opt-out of the sale of their PII.[25]

- Allow consumers to request deletion of their PII.[26]

[19] Cal. Civ. Code § 1798.120(c).
[20] Cal. Civ. Code § 1798.140(t)(1).
[21] Cal. Civ. Code § 1798.140(c)(2).
[22] Cal. Civ. Code § 1798.140(c)(2).
[23] Cal. Civ. Code §§ 1798.100–1798.115, 1798.130.
[24] Cal. Civ. Code §§ 1798.100(d), 1798.130(a)(2).
[25] Cal. Civ. Code §§ 1798.135(a)(1)–(2).
[26] Cal. Civ. Code § 1798.105.

Notably in October 2019, the legislature temporarily excluded from the scope of the CCPA personal information collected in the employment context until January 1, 2021, except with respect to the CCPA's private right of action relating to data breaches and notice obligations under Cal. Civ. Code Section 1798.100.[27]

Minimizing Exposure under the CCPA Requires Not Only Thoughtful Preparation before Data Incidents, but also Careful Handling of Incident Response and Notice-to-Cure Requests

Businesses must take great care in how they respond to data incidents in light of the lack of clarity in what the CCPA sets forth in Cal. Civ. Code Section 1798.150:

"(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business."[28]

The section fails to clarify what is meant by "cure," although the drafters imply that there are situations where a breach can be cured. The section also discusses the 30-day notice to cure as referencing violations "of this title," and not a specific section. How companies respond to the 30-day notice-to-cure will be critical to how statutory penalties would be assessed. The penalties are tied to "the number of violations, the persistence of the conduct, [and] the length of time over which the misconduct occurred…".[29]

Although arbitration agreements and class-action waivers may generally restrict consumers' right to sue,[30] expect the applicability of such restrictions to CCPA claims to be hotly debated in 2020.[31]

Proposed California Attorney General Regulations for the CCPA

On October 10, 2019, the California Attorney General (AG) proposed draft regulations to clarify and operationalize the current text of the CCPA.[32] The draft regulations are divided into seven articles, six of which are substantive. Although the proposals clarified many details, many other questions were left unanswered. While not final, it is important for organizations to assess these provisions when the AG likely begins actively and aggressively policing the CCPA on July 1, 2020.

Article 1 is focused primarily on clarifying certain definitions and the scope of the CPPA. Importantly, the scope provision clarifies that a violation of the regulations also constitutes a violation of the CCPA.[33] This means that organizations violating the regulations can be potentially subject to a fine up to $2,500 for each unintentional violation, or up to $7,500 for each intentional violation. In addition, the proposed regulations provide a definition for "household," which means "a person or group of people occupying a single dwelling."[34]

Article 2 provides guidance on the notices that must be provided to consumers. Article 2 states that notices must be provided at the point of collection[35] to inform consumers of their right to opt-out, and of the business's online and offline privacy practices.[36] Each notice must use plain, straightforward language, use a format that is readable, be available in the languages that the business ordinarily uses, and be accessible to consumers with disabilities.[37] The proposed regulations identify four categories of information that must be provided to consumers in the notice at point of collection, including a list of categories of personal information about the consumer that are to be collected and, for each category, the business or commercial purpose(s) for which the personal information will be used.[38] Notably, if a business fails to provide the notice and required opt-out, Article 2 states that the business shall consider all consumers as having opted out of the sale of personal information.[39]

In addition, Article 2 details the formats for proper notices of financial incentives and a compliant privacy policy.[40] For the former, the notice of financial incentive must:

- Provide a summary of the incentive, price, or service difference offered;
- Describe the material terms, including the categories of data implicated;
- Inform of the consumer's right to withdraw; and
- Explain why the financial incentive is permitted under the CCPA, including the good faith estimate of the data's value, and the method used to calculate the value.[41]

For the latter, the proposed regulation states that privacy policies must:

- Inform consumers that they have the right to:
  - obtain an accounting of what has been collected, disclosed, or sold;
  - request deletion of their personal information;
  - opt-out;
  - non-discrimination;
  - designate an authorized agent to make requests;

[27] *See* A.B. 25 and A.B. 1355, 2019–2020 Leg., Reg. Sess. (Cal. 2019).
[28] Cal. Civ. Code § 1798.150(b).
[29] Cal. Civ. Code § 1798.150(a)(2).
[30] *Lamps Plus, Inc. v. Varela*, 139 S. Ct. 1407 (2019)
[31] *See* Cal. Civ. Code § 1798.192 (contract provisions that attempt to waive or limit rights under the CCPA shall be void and unenforceable).
[32] Proposed Text of California Consumer Privacy Act Regulations, Office of Cal. Att'y Gen. (Oct. 10, 2019), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.
[33] Proposed Text of California Consumer Privacy Act Regulations § 999.300(b).
[34] § 999.301((h).
[35] § 999.305(a)(1).
[36] § 999.305(b).
[37] § 999.305(a)(2).
[38] § 999.305(b).
[39] § 999.306(d)(2).
[40] §§ 999.307, 999.308.
[41] § 999.307.

- Direct consumers to accurate contact information;
- Provide when the privacy policy was last updated; and
- Inform consumers where to access the additional information required under § 999.317 for businesses that sell personal information of more than four million consumers.[42]

Article 3 sets forth regulations for the handling of verifiable consumer requests. For example, businesses must provide two or more designated methods for receiving requests to know, which must include a toll-free telephone number and, if a business operates a website, an interactive web form.[43] In contrast, no specific method is required for submitting requests to delete.[44] Still, the regulations provide that businesses must provide at least two methods, which may include a toll-free telephone number, a link or form available online, a designated email address, or a form submitted online or in person.[45]

The time to respond to requests to know and delete are the same. Businesses must confirm receipt of the request within 10 days, and provide information on how the business will process the request, including an explanation of the identity verification process.[46] Businesses must then further respond within 45 days, or an additional 45 days if they provide the consumer with notice and an explanation of why more time is needed.[47]

For responses to requests to know specific pieces of information, the regulations create new requirements that are intended to protect against identity theft. For example, Article 3 states that a business "shall not" respond to such a request if the disclosure "creates a substantial, articulable, and unreasonable risk to the security of that personal information."[48] The sections specifically say that certain sensitive information may not be disclosed "at any time" in connection with requests.[49] The regulations also provide three potential options for complying with requests to delete: permanently and completely erasing data, deidentifying the information, or aggregating the data.[50] Notably, even where a business has aggregated information that pertains to a "household," they may still be required to comply with requests to know and delete.[51]

With respect to requests to opt-out, businesses are required to respond within 15 days from the date of receipt.[52] They must notify all third parties to whom they have sold the consumer's personal information for the prior 90-day period, and instruct them not to further sell the information.[53]

Critically, Article 3 also speaks to service providers, training, and record-keeping requirements. "Service providers" are required to respond to requests, even if it is ultimately to direct the consumer to the business the service provider services.[54] Of particular note, the regulations create a new reporting requirement for businesses that sell or share the personal information of four million or more consumers. Among other things, those businesses will need to make disclosures in their online privacy policies regarding the number of requests that they have received, the type received, and the median number of days it took the organization to respond.[55]

Article 4 creates a "totality of the circumstances" analysis for verifying the identity of a consumer making the request. Specifically, the regulations provide that businesses must establish, document, and comply with a reasonable method for verifying identities.[56] The regulations also set forth specific requirements for instances in which the business maintains a password-protected account with the consumer, and in that case may also need to verify the consumer's identity through the business's existing authentication practices.[57] Notably, if a consumer does not have or cannot access a password-protected account, the business must still conduct a totality-of-circumstances analysis and take certain steps to confirm the consumer's identity against known data points.[58] For example, requests to know what categories of information have been collected may require a degree of certainty that is less than a request to access the actual personal information of individuals.[59]

Article 5 relates to the use of personal information of children 16 years and younger. First, businesses that have actual knowledge of collecting or maintaining information of children under 13 years of age are required to establish a reasonable method for determining that the person affirmatively authorizing the sale of the information is an actual parent or guardian.[60] For children 13 to 16 years of age, the business is required to establish a reasonable process for allowing minors to opt-in to the sale of their information.[61]

Article 6 provides some guidance on the CCPA's nondiscrimination provision. It suggests an eight-factor method for how a business can calculate "the value of a consumer's data," although it is unclear if the calculations will truly yield accurate values.[62]

[42] § 999.308.
[43] § 999.312(a).
[44] § 999.312(b).
[45] *Id*.
[46] § 999.313(a).
[47] § 999.313(b).
[48] § 999.313(c)(3).
[49] § 999.313(c)(4).
[50] § 999.313(d)(2).
[51] § 999.318.
[52] § 999.315(e).
[53] § 999.315(f).
[54] § 999.314.
[55] § 999.317(g).
[56] § 999.323(a).
[57] § 999.324.
[58] § 999.325.
[59] § 999.325(e).
[60] § 999.330.
[61] § 999.331.
[62] § 999.337.

While the above analysis provides an overview of the AG's proposed regulations, these are only proposed regulations. The AG has been holding regular public meetings with significant public commentary and the proposed regulations are therefore susceptible to change. Nonetheless, they provide much-needed guidance on the CCPA's requirements, while still leaving many questions unanswered.

2. Nevada Senate Bill No. 19-220

In June 2019, the State of Nevada enacted Senate Bill 220, which amends the existing Nevada Privacy of Information Collected on the Internet from Consumers Act (NPICICA). Effective October 1, 2019, the new law provides a new but narrower set of rights to Nevada consumers as compared to the CCPA.

Bill 220 covers website operators that collect "covered information" directly from Nevada consumers and "sell" that information. Bill 220 refers to NRS 603A.320's definition of "covered information," which includes "[a]ny other information concerning a person collected from the person through the Internet website or online service of the operator and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable."[63] As of this publication, there is not yet any authority addressing whether "personally identifiable" under Bill 220 includes household and device data, which is covered by sections of the CCPA.

Covered entities must establish a designated address where consumers can submit opt-out requests directing the entities not to sell their covered information. "Sale" is defined more narrowly under Bill 220 than under the CCPA and is limited only to the exchange of covered information for monetary consideration to a person for purposes of licensing or selling the covered information to additional parties.[64]

Senate Bill 220 requires that operators respond to opt-out requests within 60 days of receipt.[65] An operator can have a 30-day extension if reasonably necessary, provided the operator notifies the consumer about the delay.

While Senate Bill 220 does not provide a private right of action like the CCPA, operators that fail to comply are at risk of incurring civil penalties enforceable by the Nevada AG, up to $5,000 for each violation.[66]

3. California and Oregon IoT Law

In September 2018, California signed into law SB 18-327, a bill specifically regulating the security of the IoT, effective January 1, 2020.[67] 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."[68]

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) designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

[63] Nev. Rev. Stat. § 603A.320(7).
[64] S.B. 220 § 1.6, 2019 Leg., 80th Reg. Sess. (Nev. 2019).
[65] S.B. 220 § 2.4, 2019 Leg., 80th Reg. Sess. (Nev. 2019).
[66] S.B. 220 § 7.2(b), 2019 Leg., 80th Reg. Sess. (Nev. 2019).
[67] 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.
[68] S.B. 327, 2017–2018 Leg., Reg. Sess. (Cal. 2018).

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

On May 30, 2019, Oregon added its own IoT law by enacting House Bill 19-2395. In contrast to California, Oregon defines an IoT "connected device" more narrowly as "any device or physical object that connects directly or indirectly to the Internet and is used primarily for personal, family or household purposes."[69]

Like California's SB 18-327, Oregon's HB 2395 requires IoT devices to be provided with "reasonable security features," which is defined as features "appropriate to the nature and function of the device" and the "information it may collect, contain or transmit."

Both statutes define a "reasonable security feature" to include providing IoT devices with a means for authentication outside of a local area network 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.

Like California, Oregon generally carves out any security requirements imposed on connected devices by federal law or regulation, and separately explicitly exempts entities or persons that are subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[70]

4. Changes to State Data Breach Laws

ARKANSAS – On April 15, 2019, Arkansas revised its Personal Information Protection Act, effective July 23, 2019. Key changes include:

- Expanding the definition of "personal information" to include certain biometric data;
- Establishing that if more than 1,000 individuals are affected, notice must also be provided to the Arkansas Attorney General at the same time notice is provided to the affected individuals or within 45 days after there is a determination of a reasonable likelihood of harm to customers, whichever occurs first;
- Establishing that a written report and supporting documentation concerning a breach must be kept for five years; and
- Establishing that if the Attorney General requests a copy of the written report, such report must be provided within 30 days of the request.[71]

CALIFORNIA – On October 11, 2019, California amended its data breach notification law to require notification in additional situations where the name is compromised with additional governmental identifiers (such as tax identification numbers, passport numbers, or military identification numbers), and where the name is compromised with biometric identifiers. In the case of biometric data, the reporting entity may provide "instructions on how to notify other entities that used the same type of biometric data as an authenticator to no longer rely on [that] data for authentication purposes," in addition to the other breach reporting requirements.[72]

ILLINOIS – On August 9, 2019, Illinois passed an amendment to its Personal Information Protection Act, effective January 1, 2020. Key changes include:

- Requiring companies to notify the Illinois Attorney General where the breach affects more than 500 state residents, specifying the steps taken to fix the breach; and
- Notification to the Illinois Attorney General must be provided in the most expedient time possible, and no later than when the data collector provides notice to consumers.[73]

MARYLAND – On April 30, 2019, Maryland revised its Personal Information Protection Act, effective October 1, 2019. Key changes include:

- Requiring businesses that maintain personal information of Maryland residents to conduct an investigation when they discover or are notified of a breach;
- Prohibiting the business that incurred the breach (if not the owner or licensee of the computerized data) from charging the owner or licensee of the computerized data a fee for providing the information needed for notification; and
- Prohibiting owners or licensees of computerized data from using "information relative to the breach" for purposes other than "providing notification of the breach," "protecting or securing applicable personal information," or "providing notification to national information security organizations created for information-sharing and analysis of security threats, to alert and avert new or expanded breaches."[74]

MASSACHUSETTS – On January 10, 2019, Massachusetts revised its data breach notification law, effective April 11, 2019. Key changes include:

- Establishing that if a breach involves a resident's Social Security number, complimentary credit monitoring must be offered for a period of not less than 18 months (consumer reporting agencies that experience such a breach must provide such services for not less than 42 months);
- Requiring notification to regulators to include additional information, including whether the entity maintains a written information security program;
- Requiring notification to affected residents to include additional information, including information about security freezes and credit monitoring; and
- Establishing that notification may not be delayed on grounds that the total number of residents affected is not yet ascertained.[75]

[69] H.B. 2395 §5, 2019 Leg., Reg. Sess. (Or. 2019).
[70] H.B. 2395 §10(h), 2019 Leg., Reg. Sess. (Or. 2019).
[71] H.B. 1943, 92nd Gen. Assemb., Reg. Sess. (Ark. 2019).
[72] A.B. 1130, 2019–2020 Leg., Reg. Sess. (Cal. 2019).
[73] S.B. 1624, 101st Gen. Assemb., Reg. Sess. (Ill. 2019).
[74] H.B. 1154, 2019 Leg., Reg. Sess. (Md. 2019).
[75] H.B. 4806, 2017–2018 Leg., 190th Reg. Sess. (Mass. 2019).

NEW JERSEY – On May 10, 2019, New Jersey revised its data breach notification law, effective September 1, 2019. Key changes include:

- Expanding the definition of "personal information" to include user names, email addresses, or any other account holder identifying information, in combination with any password or security question/answer that would permit access to an online account;
- Establishing that in the event of a breach involving a user name or password, in combination with any password or security question and answer that would permit access to an online account, but where no other personal information is involved, electronic notification that directs the customer to take steps to protect their online accounts, including changing their password and security question or answer, is permitted; and
- Establishing that an entity that furnishes an email account shall not provide notification to the email account that is subject to a breach.[76]

NEW YORK – On July 25, 2019, New York passed the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), amending New York's data breach notification law. This adds to the growing list of states enacting privacy and data security laws. The SHIELD Act introduces significant changes, including:

- Broadening the definition of "private information" to include biometric information and username/email address in combination with a password or security questions and answers. It also includes an account number or credit/debit card number, even without a security code, access code, or password if the account could be accessed without such information;
- Expanding the definition of "breach of the security of the system" to include unauthorized "access" of computerized data that compromises the security, confidentiality, or integrity of private information, and providing sample indicators of access. Previously, a breach was defined only as unauthorized acquisition of computerized data;
- Expanding the territorial application of the breach notification requirement to any person or business that owns or licenses private information of a New York resident. Previously, the law was limited to those that conduct business in New York; and
- Requiring companies to adopt reasonable safeguards to protect the security, confidentiality, and integrity of private information. A company should implement a data security program containing specific measures, including risk assessments, employee training, vendor contracts, and timely data disposal.

The breach notification amendments became effective October 23, 2019, while the data security requirements take effect on March 21, 2020.[77]

OREGON – On May 24, 2019, Oregon revised its data breach notification law, newly named the Oregon Consumer Information Protection Act, effective January 1, 2020. Key changes include:

- Expanding the definition of "breach of security" to include an unauthorized acquisition of computerized data that a person possesses;
- Expanding the definition of "personal information" to include a "user name or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the user name or means of identification";
- Defining "covered entity" as "a person that owns, licenses, maintains, stores, manages, collects, processes, acquires or otherwise possesses personal information in the course of the person's business, vocation, occupation or volunteer activities." Of note, a covered entity does not include a person to the extent that the person acts solely as a vendor;
- Defining "vendor" as "a person with which a covered entity contracts to maintain, store, manage, process or otherwise access personal information for the purpose of, or in connection with, providing services to or on behalf of the covered entity";
- Requiring vendors that have discovered a breach of security or have reason to believe a breach of security has occurred to notify a covered entity (or another vendor if the other vendor has a contract with the covered entity) with which it has as a contract, no later than 10 days of discovery;
- Requiring vendors to notify the Oregon Attorney General if more than 250 consumers were affected, or if the number of consumers affected is unknown (notification by the vendor is not required if the covered entity has already notified the Oregon Attorney General); and
- Providing exemptions for covered entities and vendors that comply with HIPAA or the GLBA.[78]

TEXAS – On June 14, 2019, Texas revised its Texas Identity Theft Enforcement and Protection Act, effective September 1, 2019 (except Section 1 which is effective as of January 1, 2020). Key changes include:

- Establishing that notification to affected residents must be made no later than 60 days after it has been determined a breach occurred;
- Establishing that if the breach affects more than 250 Texas residents, notification is required to the Texas Attorney General no later than 60 days after it has been determined that a breach occurred;
- Establishing the Texas Privacy Protection Advisory Council, which will "study data privacy laws in this state, other states, and relevant foreign jurisdictions."[79]

UTAH – On March 26, 2019, Utah revised its Protection of Personal Information Act, effective May 14, 2019. Key changes include:

- Establishing that published notice to Utah residents is acceptable only if notification by first-class mail, electronic means, or telephone is not feasible;
- Exempting the $100,000 civil penalty limit from violations that concern 10,000 or more consumers who are residents of the state, 10,000 or more consumers who are residents of other states, or if the person agrees to settle for a greater amount; and
- Establishing that administrative actions must be brought no later than 10 years, and civil actions must be brought no later than 5 years, after the alleged breach occurred.[80]

VIRGINIA – On March 18, 2019, Virginia revised its data breach notification statute, effective July 1, 2019. Key changes include:

[76] S.B. 52, 2018–2019 Leg., Reg. Sess. (N.J. 2019).
[77] S.B. S5575B, 2019–2020 Leg., Reg. Sess. (N.Y. 2019).
[78] S.B. 684, 2019 Leg., Reg. Sess. (Or. 2019).
[79] H.B. 4390, 86th Leg., Reg. Sess. (Tex. 2019).
[80] S.B. 193, 2019 Leg., Reg. Sess. (Utah 2019).

- Expanding the definition of "personal information" to include first name (or first initial) and last name in combination with or linked to a passport number or military identification number.[81]

WASHINGTON – On May 7, 2019, Washington revised its data breach notification law, effective March 1, 2020. Key changes include:

- Expanding the definition of "personal information" to include date of birth; a private key unique to an individual that is used to authenticate or sign an electronic record; student, military, or passport identification number; health insurance policy number or health insurance identification number; medical history or condition information; certain biometric data; and username or email address in combination with a password or security questions and answers that would permit access to an online account;
- Establishing that notification to affected residents must be made no later than 30 calendar days after discovery of the breach (certain exceptions allowed);
- Establishing that if more than 500 Washington residents are affected, notification to the Washington Attorney General must be made no later than 30 days after discovery of the breach;
- Establishing new notification requirements for breaches involving a username or password; and
- Establishing that an entity that furnishes an email account shall not provide notification to the email account that is subject to a breach.[82]

5. Additional General Cybersecurity Laws across Different States

Nearly half of the states now have some type of general requirement for businesses engaged in data-based products. A high-level summary of each of these states' current requirements is provided below.

[81] H.B. 2396, 2019 Leg., Reg. Sess. (Va. 2019).
[82] H.B. 1071, 2019–2020 Leg., Reg. Sess. (Wash. 2019).

STATE	COVERED ENTITY	GENERAL REQUIREMENT
Alabama	A person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information. ALA. CODE § 8-38-2(2).	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. New notice, opt-out, access, and deletion obligations for businesses that "sell" personal information under the California Consumer Privacy Act.	Implement and maintain reasonable security procedures and practices appropriate to the nature of the information. For new disclosure requirements under the California Consumer Privacy Act, see Section II(B)(1) above.
Colorado	Any entity that maintains, owns, or licenses personal identifying information in the course of the person's business or occupation. COLO. REV. STAT. § 6-1-716(b).	Implement and maintain reasonable security practices and procedures to protect personal identifying information from unauthorized access.
Delaware	Any person who conducts business that owns, licenses, or maintains personal information. 6 DEL. CODE § 12B-100.	Implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business.
Florida	Entities that acquire, maintain, store, or use personal information and third parties that have been contracted to maintain, store, or process personal information. FLA. STAT. §§ 501.171(1)(b), 501.171(1)(h).	Reasonable measures to protect and secure data in electronic form containing personal information.
Illinois	Data collectors that own, license, maintain, or store personal information. 815 ILL. COMP. STAT. 530/5.	Implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.
Indiana	Database owners – persons that own or license computerized data that includes personal information. IND. CODE § 24-4.9-2-3.	Implement and maintain reasonable procedures, including taking any appropriate corrective action.
Kansas	A person who, in the ordinary course of business, collects, maintains, possesses, or causes to be collected, maintained, or possessed, the personal information of any other person. KAN. STAT. § 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.
Louisiana	Any person that conducts business in the state or that owns or licenses computerized data that includes personal information. LA. REV. STAT. § 51:3074.	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.

STATE	COVERED ENTITY	GENERAL REQUIREMENT
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 §§ 14-3501–14-3503.	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.
Nebraska	An individual or commercial entity that owns, licenses, or maintains computerized data that includes personal information. NEB. REV. STAT. §§ 87-802–87-808.	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 establishes and maintains 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). Senate Bill 19-220 imposes notice and opt-out requirements for website operators engaged in "sale" of personal information.	Implement and maintain reasonable security measures (as specified in statute). For details on new obligations under Nevada Senate Bill 19-220, see Section II(B)(2) above.
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.
New York	Any person or business that owns or licenses computerized data which includes private information of a resident of New York. N.Y. GEN. BUS. LAW § 899-bb.	Implement a data security program containing specific measures, including risk assessments, employee training, vendor contracts, and timely data disposal.
Ohio	Any business that accesses, maintains, communicates, or processes personal information or restricted information in or through one or more systems, networks, or services located in or outside this state. OHIO REV. CODE. §§ 1354.01–1354.05.	Implement a data security program containing specific measures, including risk assessments, employee training, vendor contracts, and timely data disposal. 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 in the statute).
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 that contains reasonable security procedures and practices to protect from unauthorized access, use, modification, destruction, or disclosure and to preserve the confidentiality, integrity, and availability of personal 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 §§ 13-44-201, 13-44-301.	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 VT. STAT. tit. 9, §§ 2446–2447.	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.

C. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY INDUSTRY GUIDANCE

1. NIST Special Publication 1800-4: Mobile Device Security (Cloud and Hybrid Builds)

Amidst the debate over the security of bring-your-own-devices (BYODs), the National Institute of Standards and Technology (NIST) embarked on a special publication with industry professionals at Microsoft, Intel, and Symantec to provide actual examples of feasible implementations of "mobile device security" using cloud and hybrid infrastructures.[83] By its own terms, the publishing team sought to show "how commercially available technologies can enable secure access … from users' mobile devices … built [on] … a lightweight enterprise architecture."[84]

The team used primarily Microsoft operating systems and tools to build two different mobile security designs: one was based on a cloud architecture, and the other was based on a part cloud, part on-premises architecture. The two different builds shared certain characteristics, which NIST mapped to existing guidance and requirements, thereby suggesting that organizations should be able to demonstrate at least some of these characteristics if they optimized their mobile device security:

Protected Content:

- Device-level and application-level encryption;
- Trusted key storage: protected locations in software, firmware, or hardware in which long-term cryptographic keys or secrets are safeguarded from unauthorized disclosure or modification; and
- Protected communications.

Remote Wiping Capabilities:

- Remote wipe (action that prevents the unauthorized access of data stored on a lost or stolen device by rendering data recovery techniques infeasible);
- Selective wipe (remote wipe that affects only enterprise data, leaving personal data intact); and
- Automatic wipes (action that reactively wipes all device data in response to multiple subsequent failed attempts to unlock a locked device).

Physical and Virtual Separations:

- Hardware security modules: embedded or removable tamper-resistant hardware used to perform cryptographic operations and provide secure storage to protect security operations or data from unauthorized access or modification;
- Sandboxing: operating system or application-level virtualization, isolation, and integrity mechanisms utilizing multiple protection, isolation, and integrity capabilities to achieve higher levels of overall process isolation; and
- Memory isolation: operating-level enforced separation of memory spaces allocated to running processes to protect their integrity.

User, Device, and Execution Validation:

- Local authentication of user to device;
- Local user authentication to applications;
- Remote user authentication;
- Device provisioning and enrollment;
- Device resource management: ability to selectively disable unused or unnecessary peripherals to prevent their abuse;
- Trusted execution: protection of security processes within an isolated and trustworthy environment;
- Boot validation: integrity checks on the content of boot files and the execution of boot processes to verify the operating system has been launched from a known and trustworthy state;
- Application verification: integrity checks on application installation packages and validation of the digital signature to verify that applications come from a trusted source and have not been modified prior to installation;
- Application whitelisting/blacklisting: allowing or disallowing the use of applications based on a prespecified list; and
- Verified application and operating system updates prior to execution.

Ongoing Detection and Management:

- Mobile malware detection;
- Inventory of mobile device hardware and software;
- Asset management;
- Compliance checks;
- Root and jailbreak detection;
- Auditing and logging: capture and store security events for devices, including enrollment, failed compliance checks, administrative actions, and unenrollment; and
- Canned reports and ad hoc queries: use preconfigured reports or active searches or filters on security logs to manage incidents and audit compliance.[85]

While the list of design characteristics is not meant to be prescriptive or exhaustive,[86] organizations would do well to cite to the publication regarding what they considered and used in their mobile device security designs.

2. NIST Cybersecurity Whitepaper (Draft): Mitigating the Risk of Software Vulnerabilities (by Adopting a Secure Software Development Framework)

NIST has been attempting to assemble a secure software development framework (SSDF). In a white paper released on June 11, 2019 NIST noted that "[f]ew SDLC (software development life cycle) models explicitly address software security in detail," and proceeded to describe "a subset of high-level practices based on established standards, guidance, and secure software development practice documents."[87] Because the publication is one of NIST's first

[83] Joshua Franklin et al., *Mobile Device Security: Cloud and Hybrid Builds*, Nat'l Inst. Standards & Tech. S.P. 1800-4 1, 1 (Feb. 2019), https://csrc.nist.gov/publications/detail/sp/1800-4/final.
[84] *Id.* at 1.
[85] *Id.* at 17–19.
[86] *See id.* at 3.
[87] Donna Dodson et al., *Draft: Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)*, Nat'l Inst. Standards & Tech. 1, 1 (June 11, 2019), https://csrc.nist.gov/publications/detail/white-paper/2019/06/11/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft.

efforts focused entirely on developing an officially-sanctioned SSDF framework, privacy practitioners should heed the specific practices it discusses.

The guidance organizes software development along four groups of practices, cross-referencing each practice to other NIST guidance, in addition to specific rules from other organizations such as The Software Alliance (BSA) and the International Organization for Standardization (ISO). Security professionals should note certain practices recommended by the publication:

- Preparing the Organization (PO): NIST views proper preparations as requiring that "security requirements for software development are known to at all times so they can be taken into account throughout the SDLC," which means that all policies should be written at the onset of the development cycle. This includes preparing and maintaining internal as well as external requirements.[88] In addition, NIST recommends using "automation to reduce the human effort needed and improve the accuracy, consistency, and comprehensiveness of security practices throughout the SDLC."[89]

- Protect the Software (PS): In addition to protecting the source code, NIST recommends that software releases utilize cryptographic signatures and verification.[90]

- Produce Well-Secured Software (PW): To produce well-secured software, NIST recommends threat and attack modeling;[91] using third party and automation to review and test the design and code;[92] testing new components and usage with trusted components and established procedures;[93] and setting security as the default value and state for the software.[94]

- Respond to Vulnerability Reports (RV): After software releases, NIST recommends that organizations actively collaborate with outside researchers while monitoring vulnerabilities; create toolchains to perform automated code analysis and testing on a regular basis;[95] assess and prioritize vulnerabilities, using issue or bug tracking software to document vulnerabilities;[96] and conduct root-cause analysis to reduce future vulnerabilities on an ongoing basis.[97]

3. NIST'S Core Cybersecurity Feature Baseline for Securable Devices: A Starting Point for IoT Device Manufacturers (Draft)

"Baseline state" has been an important topic of discussion for the purposes of secure software development. NIST released a draft guideline numbered NISTIR 8259, on baseline features and protections for IoT devices in August 2019. At the outset, the publication recognizes that "many IoT devices interact with the physical world in ways conventional IT devices usually do not," and that "many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can.[98] Thus, "the availability, efficiency, and effectiveness of cybersecurity features are often different for IoT devices than conventional IT devices."[99]

The draft guidance recommends the following features for all IoT devices:

- Proper Device Identification: The IoT device should be able to reliably identify itself when connecting to networks.

- Authorized Device Configuration: An authorized user should be able to change the device's software and firmware configuration.

- Clear Explanation of Data Protection Mechanisms: It should be clear how the IoT device protects the data in storage and transit from unauthorized access and modification.

- Limited Access to Interfaces: The device should limit access to its local and network interfaces, and nothing else unless the access is authorized. Any access should be authenticated.

- Updatable Software and Firmware: A device's software and firmware should be updatable using a secure and configurable mechanism. Automatic updates from the manufacturer may be advisable.

- Cybersecurity Event Logging: IoT devices should log cyber security events, while making the logs accessible to the owner or manufacturer. These logs can help users and developers identify vulnerabilities in devices to secure or fix them.[100]

As to the process for "secure development practices for IoT devices," the guide recommends the following:

- Manufacturers should make sure that their workforce has the necessary skills to develop IoT devices and software;

- Manufacturers should protect code releases, and give customers the ability to verify code integrity;

[88] *Id.* at 4, PO.1.
[89] *Id.* at 6–7, PO.3–PO.4.
[90] *Id.* at 7, PS.2–PS.3.
[91] *Id.* at 8, PW.1.
[92] *Id.* at 8–9, 12–13, PW.2–PW.3, PW.7–PW.8.
[93] *Id.* at 10, PW.4.
[94] *Id.* at 14, PW.9.
[95] *Id.* at 15, RV.1.
[96] *Id.* at 16, RV.2.
[97] *Id.* at 16, RV.3.
[98] Michael Fagan et al., *Draft: Core Cybersecurity Features Baseline for Securable IoT Devices*, Nat'l Inst. Standards & Tech. 1, 3 (July 2019), https://csrc.nist.gov/publications/detail/nistir/8259/draft.
[99] *Id.*
[100] NIST Releases Draft Security Feature Recommendations for IoT Devices, Nat'l Inst. Standards & Tech. (Aug. 1, 2019), https://www.nist.gov/news-events/news/2019/08/nist-releases-draft-security-feature-recommendations-iot-devices.

- With regard to third party integrations, manufacturers should verify the software and components of third parties; and

- Manufacturers should reuse existing, well-secured software when feasible, instead of duplicating functionality. In addition, they should test executables when possible, and review human-readable code manually when feasible.[101]

Because the guide recognizes that IoT devices can be used in unconventional ways, or have unanticipated use cases, it recommends that manufacturers map out use cases, such as by mapping out early on:

(1) the likely methods for device management, (2) configurability of the device, (3) potential network characteristics, (4) the nature of the device data, and (5) potential methods and levels of access.[102]

For compliance officers, the guide includes a standard set of NIST-tables for "core baseline" features, against which requirements can be mapped.[103]

[101] Fagan et al., *supra* note 98, at 20–21.
[102] *Id*. at 6–7.
[103] *Id*. at 10–13.

III. EVOLVING CASE LAW

The privacy law landscape is constantly evolving due to new civil case law. With states starting to pass statutes such as the CCPA, which carry stiff statutory penalties and that have not yet been comprehensively interpreted by the courts, organizations should move into 2020 with awareness of and strategies to address the evolving case law landscape.

Arbitration agreements with class action waivers could emerge as the main defense for companies in data breach and misuse cases. For product liability and security cases, it will be more important than ever for organizations to be able to demonstrate the lack of foreseeable harm.

A. DATA BREACH LITIGATION

1. Consumer Breach Litigation: Contractual Clauses as the Main Defense?

Until the last few years, defendants in data breach class actions were often able to obtain dismissals as part of a Rule 12(b)(1) motion, arguing that plaintiffs have not in fact suffered damages sufficient to constitute Article III standing under the U.S. Constitution. Then, in *Spokeo v. Robins*, the U.S. Supreme Court was presented with the issue of whether a plaintiff that suffered no injury-in-fact may nonetheless have Article III standing for a mere procedural violation under the Fair Credit Reporting Act (FCRA). Although the Court emphasized that "Article III standing requires a concrete injury even in the context of a statutory violation," it avoided clarifying what is meant by "an injury that is both 'concrete and particularized,'" leaving open the possibility that even an "intangible harm" may nonetheless still be "concrete."[104]

On remand, the Ninth Circuit provided no more clarity than the Supreme Court. The Circuit Court provided a two-prong test for ascertaining whether an "intangible harm" allegedly prohibited by statute is sufficiently "concrete" for Article III purposes: (a) whether the harm is the type of intangible harm for which the legislature created legislation to protect consumers' concrete interest; and (b) whether the alleged violations actually harm or create a "material risk of harm" to the concrete interest.[105] While the court found that the allegations at issue related to accuracy risks covered by the FCRA, the court noted that some inaccuracies may be too trivial for purposes of the FCRA.[106]

Since *Spokeo*, it has become increasingly difficult for defendants to prevail simply on a Rule 12(b)(1) motion. Although it is unclear how any particular court will side on the various untraditional types of damages arising from data breach litigation, defendants now must also file a Rule 12(b)(6) motion concurrent with a Rule 12(b)(1) motion. Further, even when defendants win a 12(b)(1) motion, plaintiffs are often able to convince federal courts to remand the case to state courts thereafter, rather than dismiss with prejudice.[107]

Types of Damages as "Concrete and Particularized" Injury

Since *Spokeo*, courts have debated what type of damages would constitute concrete and particularized injury. Courts have taken different views about particular kinds of alleged injuries, and decisions in 2019 have shown that results can be unpredictable. For example:

- "Threat of future harm" – In *21st Century Oncology Customer Data Security Breach Litigation*, a Middle District of Florida court noted that the Eleventh Circuit has yet to clarify whether an increased threat of identity theft is sufficient as cognizable injury-in-fact.[108] The court noted that there were decisions in the Sixth, Seventh, Ninth, and D.C. Circuits favoring standing,[109] but decisions in the First, Second, and Eighth Circuit denying standing. The court found the Third and Fourth Circuits straddling the middle, with findings depending on the facts.[110] The court observed that common issues considered by the circuits were: (a) the alleged motive for the intrusion, (b) the type of information, and (c) whether there was evidence of the information being used by malicious actors.[111]

- "Time spent" mitigating a data breach – A court in the Middle District of Florida found such time spent sufficient for Article III standing in one case.[112] But in another case, a court in the Middle District of Florida found such damages too speculative.[113]

- Lost opportunity to use credit card – The Florida district courts have also differed on this point within the Eleventh Circuit.[114]

[104] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1545–50 (2016) (citations omitted).
[105] *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1113 (9th Cir. 2017), *cert. denied*, 138 S. Ct. 931 (2018).
[106] *Id.* at 1117 n.4.
[107] *See, e.g.*, *Patton v. Experian Data Corp.*, 2016 U.S. Dist. LEXIS 60590 (C.D. Cal. May 6, 2016.
[108] *In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1250 (M.D. Fla. 2019).
[109] *Id.* at 1251. *See, e.g.*, *Adkins v. Facebook, Inc.*, 2019 U.S. Dist. LEXIS 206271 (N.D. Cal. Nov. 26, 2019) (denying motion to strike class on basis of lost time damages).
[110] *In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d at 1251. *See, e.g., Alleruzzo v. SuperValu, Inc.* (*In re SuperValu, Inc.*), 925 F.3d 955 (8th Cir. 2019) (in class action involving malware installed at the point-of-sale of defendant retailer, court finding threat of future harm insufficient for Article III purposes); *see contra*, *AFGE v. OPM* (*In re U.S. OPM Data Sec. Breach Litig.*), 928 F.3d 42 (D.C. Cir. 2019) (reversing lower court and finding loss of privacy and the threat of future harm sufficient for Article III purposes).
[111] *In re 21st Century Oncology Customer Data Security Breach Litig.*, 380 F. Supp. 3d at 1251–54.
[112] *In re Brinker Data Incident Litig.*, 2019 U.S. Dist. LEXIS 128573, at *14 (M.D. Fla. Aug. 1, 2019).
[113] *Tsao v. Captiva MVP Rest. Partners, LLC*, 2018 U.S. Dist. LEXIS 187119, at *5 (M.D. Fla. Nov. 1, 2018).
[114] *Compare In re Brinker Data Incident Litig.*, 2019 U.S. Dist. LEXIS 128573 *with Tsao*, 2018 U.S. Dist. LEXIS 128573.

- Diminishment of value – The Ninth Circuit continued to deny diminishment of the alleged value of personal information as a viable theory for Article III standing in the case associated with the Cambridge Analytica incident, although it allowed the case to proceed on the basis of "violation of privacy expectations."[115]

Consistent with the 2018 trends, it is unlikely that the differences amongst different circuits and district courts will clear in the immediate future. Regardless, parties should keep in mind that the damages analysis that a court applies for its Article III analysis is not the same as what it is supposed to apply to assess whether plaintiffs have sufficiently stated viable causes of action.[116]

New Plaintiffs on the Horizon

Besides federal and state authorities, cities and municipalities are now bringing suit on behalf of their residents against organizations held responsible for data breaches. In *City of Chicago v. Marriott Int'l, Inc.*, the City of Chicago sued Marriott International for the hotel chain's data breach, alleging that it violated a city ordinance requiring reasonable data privacy practices. Marriott argued that the city did not have standing to sue on behalf of its residents, especially as it was dealing with issues that were statewide and national in nature. The court disagreed, finding that the Illinois legislature gave municipalities the ability to protect their citizens unless otherwise prohibited, and that data breaches could be local in nature, not just statewide or national.[117]

Similarly, the District of Columbia also individually sued on the basis of the Cambridge Analytica incident. The Superior Court of the District of Columbia denied defendant's motion to dismiss on the basis of lack of specific jurisdiction.[118]

HIPAA Claims as Other Causes of Action

The Health Insurance Portability and Accountability Act (HIPAA) is not supposed to be enforceable by private parties. Since 2018, however, at least two state supreme courts have acknowledged privacy claims based on technical HIPAA violations, styled and stated as another type of claim.

In *Lawson v. Halper-Reiss*, the plaintiff alleged that the hospital impermissibly disclosed the plaintiff as a drunk driver to an on-premises police officer, in violation of HIPAA. While the Supreme Court of Vermont ultimately granted the defendant's summary judgment motion on the basis of a good faith defense, the court noted in dicta that it believed that "the vast majority of jurisdictions" now allow for HIPAA-based wrongful disclosure to be used as a basis for other claims.[119]

The *Lawson* court cited to a 2018 decision of the Supreme Court of Connecticut. In *Bryne v. Avery Center for Obstetrics & Gynecology, P.C.,* the plaintiff alleged that the defendant medical center improperly disclosed medical information in response to a subpoena in a paternity lawsuit, contrary to both HIPAA and common law.[120] In reversing the trial court's ruling on summary judgment, the court found that it had the right to recognize new causes of action, based on what it found in other jurisdictions.[121] And the court also found that, because of the fiduciary relationship between doctor and patient, the plaintiff had a private right of action for breach of confidentiality against the medical center.[122]

The Fight over Negligence as a Cause of Action

A key debate has been over whether a general negligence cause of action may be stated whenever there is a data breach. Aside from the business-to-consumers context, the fight has relevance over whether negligence may be stated in other contexts where there is no express agreement amongst the parties on the issues of privacy and security.

- Employer to employee: In *McConnell v. Georgia Department of Labor,* 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.[123] Plaintiffs appealed, but the Supreme Court of Georgia affirmed the lower court's finding of no general duty.[124]

- Employer to employee: In *McKenzie v. Allconnect, Inc.*, which arose from a data breach involving employee data arising from a phishing attack on a company that connects consumers with offers for internet services, television, home security, electricity, and other products, the court found that there was an implied agreement to safeguard personal information by the defendant.[125]

- Care provider to patient: In *K.A. v. Children's Mercy Hospital*, plaintiffs brought a data breach class action resulting from the employee of defendant hospital creating an unauthorized website containing patient information. In an order partially denying dismissal, including on the negligence claim, the court held that the economic loss rule does not apply where there may be a fiduciary duty.[126]

- Retailer to customer: In *Alleruzzo v. SuperValu*, the Eighth Circuit affirmed the lower court's finding that the retailer did not owe customers a general duty to safeguard payment card information in a data breach case, notwithstanding the fact that the defendant retailer was required pursuant to Payment Card Industry (PCI) rules to safeguard consumer payment card information.[127]

[115] *In re Facebook, Inc.*, 402 F. Supp. 3d 767, 784 (N.D. Cal. 2019). *But see Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1050 (N.D. Cal. 2018) (recognizing diminishment of value of data as a potential theory for data misuse causes of action on a motion to dismiss).
[116] *See, e.g., Attias v. Carefirst, Inc.*, 365 F. Supp. 3d 1, 5 (D.D.C. 2019) (noting that the damages sufficient to show standing to survive a Rule 12(b)(1) motion may not be sufficient to show damages for the purposes of a rule 12(b)(6) motion).
[117] *City of Chicago v. Marriott Int'l, Inc.*, 2019 U.S. Dist. LEXIS 215154 (D. Md. Dec. 13, 2019).
[118] *District of Columbia v. Facebook, Inc.*, Sup. Ct. of D.C. Case No. 2018CA8715B (May 31, 2019).
[119] *Lawson v. Halpern-Reiss*, 2019 VT 38, *P11 (2019).
[120] 175 A.3d 1, 3–4 (Conn. 2018).
[121] *Id.* at 9–10.
[122] *Id.* at 17.
[123] *McConnell v. Dep't of Labor*, 345 Ga. App. 669 (2018).
[124] *Ga. Dep't of Labor v. McConnell*, 305 Ga. 812 (2019).
[125] *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810 (E.D. Ky. 2019).
[126] *K.A. v. Children's Mercy Hosp.*, 2019 U.S. Dist. LEXIS 82725 (W.D. Mo. May 17, 2019).
[127] *Alleruzzo v. SuperValu, Inc.* (*In re SuperValu, Inc.*), 925 F.3d 955 (8th Cir. 2019).

- Third party "processor" (or "aggregator") to consumer: The old adage amongst attorneys is that "bad facts make bad law." In *In re Equifax, Inc. Consumer Data Security Breach Litigation*, the court had difficulty finding grounds for the plaintiffs involved in the allegedly enormous breach to be able to directly sue the consumer reporting agency Equifax, as plaintiffs could not easily plead a direct relationship between them and Equifax. As a result, the court held that Section 5 of the Federal Trade Commission Act (the FTC Act), which prohibits "unfair and deceptive acts," could be used as the basis for a negligence cause of action[128] Notably, however, in *Alleruzzo, supra*, the Eighth Circuit found that there is no private right of action under the FTC Act,[129] and other district courts have held that there is no case law precedent for using Section 5 as the basis for a negligence per se cause of action.[130]

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 negligence claims.[131]

Class Certification

Although some data breach cases have now reached class certification and trial, plaintiffs' efforts demonstrate how difficult it can be to obtain class certification. In *Adkins v. Facebook*, although the court certified an injunctive class, it found the proposed class based on users who allegedly lost time to mitigate threats to their identity to be too individualized on the issues of "fact of injury, causation … and extent of damage," thus denying a Federal Rule of Civil Procedure 23(b)(3) class.[132]

Nonetheless, plaintiffs obtained the first jury verdict on behalf of a putative breach class in 2019, receiving a jury award of $68 million in damages relating to the inadvertent public disclosure of 68,000 prisoners' records data.[133]

Arbitration Clauses as a Defense

Arbitration agreements will be more important than ever in privacy disputes. In *Lamps Plus. v. Varela*, the U.S. Supreme Court addressed whether an arbitration agreement was enforceable in a lawsuit involving the data breach of employee data. The Ninth Circuit had construed the employer's arbitration agreement where it was silent on the issue of class arbitration against the employer as the drafter, thereby permitting class arbitration.

The Supreme Court reversed, holding that not only was an arbitration provision enforceable in a privacy dispute between an employer and employee under the Federal Arbitration Act (FAA), but that absent an express agreement to arbitrate on a class-wide basis, a court cannot compel class arbitration because arbitrations result from private agreements between parties pursuant to the FAA. Silence is insufficient.[134] Thus, class arbitration waivers are arguably the default for arbitration agreements, not an expressly carved exception.

Aside from *Varela*, courts have continued to enforce arbitration agreements in numerous contexts across different industries.[135] Notably, even where the arbitration agreement was offered in the form of browsewrap as opposed to clickwrap, courts will enforce the arbitration provision where there is constructive or actual notice.[136]

[128] *In re Equifax, Inc.*, 362 F. Supp. 3d 1295 (N.D. Ga. 2019). *But see Diaz v. Intuit, Inc.*, 2018 U.S. Dist. LEXIS 82009 (N.D. Cal. May 15, 2018).
[129] *In re SuperValu, Inc.*, 925 F.3d 955 (8th Cir. 2019).
[130] *See Gordon v. Chipotle Mexican Grill,* 344 F. Supp. 3d 1231, 1246 (D. Colo. 2018) (affirming magistrate judge's analysis on Section 5 of the FTC Act as basis for a negligence per se claim).
[131] *See, e.g., id. But see, Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024 (N.D. Cal. 2019) (while applying the economic loss rule, court still allowed a negligence cause of action to proceed because of the contractual language of the terms and conditions with the end-users).
[132] *Adkins v. Facebook, Inc.*, 2019 U.S. Dist. LEXIS 206271, at *23 (N.D. Cal. Nov. 26, 2019) (in case where plaintiffs allege that an application access token vulnerability resulted in hackers being able to use Facebook's single-sign on feature to access other connected applications).
[133] Matt Fair, *Pa. County Hit With Up to $68M In Damages In Privacy Case*, Law360 (May 28, 2019), https://www.law360.com/articles/1163520/pa-county-hit-with-up-to- 68m-in-damages-in-privacy-case.
[134] *Lamps Plus, Inc. v. Varela*, 139 S. Ct. 1407, 1417 (2019).
[135] *See, e.g., O'Neil v. Comcast Corp.*, 2019 U.S. Dist. LEXIS 31031 (N.D. Ill. Feb. 27, 2019) (granting motion to compel arbitration where users allege that customer and payment information was not stored securely, and equipment was fraudulently purchased using their identities); *Murray v. Under Armour Inc.*, No. 18-4032, Dk. 36 (C.D. Cal. Feb. 11, 2019) (granting motion to compel arbitration where MyFitnessPal and MapMyFitness fitness applications acquired by Under Armour allegedly suffered data breaches affecting 150 million users, including hashed passwords).
[136] *Gutierrez v. FriendFinder Networks, Inc.*, 2019 U.S. Dist. LEXIS 75310 (N.D. Cal. May 3, 2019).

There will be renewed heavy scrutiny on class arbitration waivers in the coming year due to momentum created by plaintiff-friendly statutes such as the California Consumer Privacy Act (CCPA). While *Varela* clearly implies that arbitration agreements would apply to CCPA claims pursuant to the FAA, plaintiffs will likely contend that class arbitration waivers are against the public policy provisions of such statutes.[137]

Court Approvals and Settlement Values

One of the most interesting issues in data breach actions has been the viability of class action settlements. When parties reach a settlement, both sides often feel compelled to argue certifiability so that the dispute can be finally resolved.

However, parties are facing two counteracting trends. On the one hand, courts have become more critical of settlements because of current political views regarding privacy. For example, in *Parsons v. Kimpton Hotel & Restaurant Group, Yahoo Customer Data Security Breach Litigation*, and *Remijas v. The Neiman Marcus Group*, it took the parties multiple submissions before the courts would preliminarily approve the settlement.[138] Even after the settlement in *In re Equifax, Inc., Customer Data Security Breach Litigation* received final approval from the court, it is unclear if objectors will try to appeal the deal.[139]

On the other hand, some courts have begun relaxing the requirements for class certification for the purposes of settlement. In *Hyundai & Kia Fuel Economy Litigation*, for example, the Ninth Circuit expressly held that the class certification assessment undertaken at the settlement stage may be less rigorous than for the purposes of active litigation.[140] This is of course not all courts. In fact, some have conducted their own *Spokeo* analysis at the point of settlement, finding that they lack jurisdiction to certify a class if there is no evidence of exposure of data to third parties and therefore no damages for Article III purposes.[141]

We are also seeing two counteracting trends regarding settlement values. As attorneys have become more accustomed to data breach litigation, negotiated settlement values are becoming more consistent and predictable for most types of data. In previous years, there was great disparity amongst negotiated settlements involving sensitive data, where some cases settled for hundreds of dollars per consumer record. In 2019, the highest reported negotiated settlement per consumer in a non-healthcare data context was in *Hutton v. National Board of Examiners in Optometry*, which provided for approximately $3.25 million for 61,000 class members involving their professional licensure data.[142] Although still disproportionally high when compared to the settlement value per user of most other types of data breach cases, *Hutton* as an outlier is less of a discrepancy than the deviant settlements of prior years. It will be interesting to see whether new statutes like the California Consumer Privacy Act change settlement values with their statutory damages provisions.

On the other hand, healthcare data settlements continue to boast some of the largest data breach settlements to date. In *John Doe One v. Caremark*, for example, plaintiffs settled for approximately $1,000 a person, in a case where approximately 4,500 individuals with HIV-prescriptions had marketing and administrative materials sent to them in envelopes that disclosed what the envelopes contained.[143]

Importantly, 2019 provided for the first time two verdicts in privacy cases in favor of plaintiffs. In one case, police officers were found to have violated a fellow officer's privacy, with the Minnesota jury awarding $585,000.[144] In another, involving the inadvertent public disclosure of 68,000 prisoners' records data, the jury awarded the certified class $68 million in damages.[145]

2. Business-to-Business Breach Litigation: The Continued Fight over Negligence Claims

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,[146] many businesses willing to initiate such litigation had high hopes for large recoveries in business-to-business data breach litigation. Nearly five years later, however, it is still unclear whether businesses can recover against other businesses in the context of a data breach, absent an express agreement between them.

[137] *See* Cal. Civ. Code §§ 1798.175, 1798.192 (contract provisions that attempt to waive or limit rights under the CCPA shall be void and unenforceable); *see also McGarry v. Delta Air Lines, Inc.*, 2019 U.S. Dist. LEXIS 106236, at *13–14 (C.D. Cal. Jun. 18, 2019) (finding preemption on basis of Airlines Deregulations Act in lawsuit arising from malware breach through online customer software).

[138] Celeste Bott, *$1.6M Neiman Marcus Breach Deal Approved On 2nd Try*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220629/-1-6m-neiman-marcus-breach-deal-approved-on-2nd-try; Joyce Hanson, *3rd Time's A Charm For $600K Kimpton Breach Settlement*, Law360 (Jan. 10, 2019), https://www.law360.com/articles/1117103/3rd-times-a-charm-for-600k-kimpton-breach-settlement; Dorothy Atkins, *Yahoo's Revised $117M Data Breach Deal Gets Koh's Initial OK*, Law360 (July 22, 2019), https://www.law360.com/articles/1180718.

[139] Allison Grande, *Contested Equifax Data Breach Deal Gets Final Nod*, Law360 (Dec. 20, 2019), https://www.law360.com/cybersecurity-privacy/articles/1230211/contested-equifax-data-breach-deal-gets-final-nod.

[140] *In re Hyundai & Kia Fuel Econ. Litig.*, 926 F.3d 539 (9th Cir. 2019) (*en banc*).

[141] *Steven v. Carlos Lopez & Assocs.*, 2019 U.S. Dist. LEXIS 203621 (S.D.N.Y. Nov. 22, 2019) (rejecting small breach class settlement on Spokeo grounds, finding no evidence of third party exposure of data sufficient for damages).

[142] Dani Kass, *Optometry Board Reaches $3M Deal In Data Breach Suit*, Law360 (Mar. 7, 2019), https://www.law360.com/articles/1136542/optometry-board-reaches-3m-deal-in-data-breach-suit.

[143] *See* Mike Lasusa, *CVS to Pay $4.4M for Divulging HIV Status of 6,000 Patients*, Law360 (Sep 10, 2019), https://www.law360.com/articles/1197622/cvs-to-pay-4-4m-for-divulging-hiv-status-of-6-000-patients. On the other hand, we have also observed some healthcare settlements yielding very low settlement values in 2019, such as at approximately $6 per patient in *Morrow v. Quest Diagnostic Inc.* (D. NJ) (*see* Bill Wichert, *Quest Settlement Of Data Breach Suit Gets Waved Through*, Law360 (Oct. 25, 2019), https://www.law360.com/articles/1213698/quest-settlement-of-data-breach-suit-gets-waved-through), and approximately $2 per patient *In re Banner Health Data Breach Litig.* (D. Ariz.) (*see* Adam Lidgett, *Data Breach Victims To Get Up To $6M In Banner Health Deal*, Law360 (Dec. 6, 2019), https://www.law360.com/articles/1225959/data-breach-victims-to-get-up-to-6m-in-banner-health-deal).

[144] Human Rights Watch, US: Police Found to Violate Fellow Officer's Privacy (Jun. 20, 2019), https://www.hrw.org/news/2019/06/20/us-police-found-violate-fellow-officers-privacy.

[145] Fair, *supra* note 133.

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

For example, in *Bellwether Community Credit Union v. Chipotle Mexican Grill*, a Tenth Circuit court again rejected plaintiffs' attempts to argue that PCI rules and Section 5 of the FTC Act could form the basis for negligence claims.[147] However, in *Equifax Consumer Data Breach Litigation*, an Eleventh Circuit court held that both the Safeguard Rule under the GLBA and Section 5 of the FTC Act could form the basis for negligence claims against Equifax.[148] These rulings are good illustrations of the current split amongst the district courts. Indeed, the courts are split even within the same state, as illustrated by the difference between the Georgia district courts and Supreme Court on the viability of general negligence claims within data breach contexts.[149]

Notably, where plaintiffs are too ambitious with their negligence claims, they also run the risk of destroying class certification. In *Southern Independent Bank v. Fred's Inc.*, involving the breach of a general goods retailer, the court found that the negligence theories for 50 states were too varied for Rule 23(b)(3) certification on issues of predominance, including on issues of duty, economic loss rule, and damages. The court therefore denied plaintiffs' motion for class certification.[150]

Lastly, because of the uncertainty of negligence as a viable cause of action in business-to-business disputes, plaintiffs must often state a breach of contract claim in the alternative. Doing so, however, may not only risk the application of the economic loss rule, but allow defendants to use the contractual provisions in their favor.[151]

B. DATA MISUSE LITIGATION

While all fifty states now have data breach statutes, and approximately half have general requirements on securing data, only a handful of states have comprehensive regulations over how data may be used. In the absence of clear statutory guidance, plaintiffs and defendants continue to argue about emerging technologies using antiquated statutes such as federal and state wiretap laws, and common law tort principles.

1. Children's Online Privacy Protection Act (COPPA) Litigation

COPPA-based litigation has increased in 2018 and 2019 primarily due to the increased enforcement efforts of regulators. Plaintiffs' lawyers and regulators appear to be working together, with regulators feeding plaintiffs' leads.

Regardless, for plaintiffs to state a viable cause of action based on a technical COPPA violation, courts will still require that plaintiffs present the claim as something other than a direct COPPA claim, which can only be enforced by regulators.

Setting aside the Article III standing debate, some courts have held that mere technical violations of COPPA are not sufficient for the alleged violations to constitute an actionable privacy tort. In *Manigault-Johnson v. Google LLC*, for example, plaintiffs alleged that Google and its subsidiary YouTube impermissibly collected information from the online activities of children under thirteen. In dismissing the claims under a Rule 12(b)(6) motion, after having conducted an analysis under both California and South Carolina law, the court pointed out that pursuant to the tort laws of both states, the activities alleged have to be sufficiently "offensive" for the invasion of privacy tort to be viable. The court held that the allegations did not appear offensive, as plaintiffs should have known that the platform would be receiving information on their activities, and there are no acts of deception alleged.[152]

However, in *McDonald v. Kiloo Aps*, which alleged that various games embedded software development kits (SDKs) allowing third parties to impermissibly collect children's data through the games in violation of COPPA, the court denied attempts by the parties to dismiss the privacy tort claims. The complaint alleged that the SDKs aggregated data and then enriched them, including by supplementing the data with what was collected from other sources. In light of the allegations, the court found that for the intrusion into seclusion claims, the pleadings were sufficiently offensive against social norms.[153] One might reconcile the different results from the *Manigault-Johnson* and *McDonald* cases as the difference between first-party versus third-party data collection.

2. Biometric Information Protection Act (BIPA) Litigation

Prior to the Illinois Supreme Court's holding in *Rosenbach v. Six Flags Entertainment*, Article III challenges appeared to turn on whether biometric information was actually provided to third parties.[154] However, the Illinois Supreme Court stated in *Rosenbach* that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her right under the Act, in order to qualify as an 'aggrieved' person entitled to seek liquidated damages and injunctive relief pursuant to the Act."[155]

A number of pending BIPA cases were reversed due to *Rosenbach*.[156] And since then, at least one BIPA case has been class certified, with the certification order approved by an appellate court.[157]

[147] *Bellwether Cmty. Credit Union v. Chipotle Mexican Grill*, 353 F. Supp. 3d 1070 (D. Colo. 2018).
[148] In *re Equifax, Inc.*, 362 F. Supp. 3d 1295 (N.D. Ga. 2019). *See also Standifer v. Best Buy Stores, L.P.*, 364 F. Supp. 3d 1286 (N.D. Ala. 2019) (finding fiduciary owed by Best Buys to plaintiff, who purchased services for his computer to be repaired, from which data was subsequently transferred without authorization).
[149] *See Ga. Dep't of Labor v. McConnell*, 305 Ga. 812 (2019) (finding no general duty to secure data).
[150] *Southern Indep. Bank v. Fred's Inc.*, 2019 U.S. Dist. LEXIS 40036 (M.D. Ala. Mar. 13, 2019).
[151] *See, e.g., Spec's Family Partners, Ltd. v. First Data Merch. Services, LLC,* 777 Fed. App'x 785 (6th Cir. 2019) (in lawsuit by payment processor to recover PCI DSS assessments, court applies limitation of damages provision to disallow plaintiff from seeking recovery of PCI assessments).
[152] *Manigault-Johnson v. Google, LLC,* 2019 U.S. Dist. LEXIS 59892, at *17 (D.S.C. Mar. 31, 2019).
[153] *McDonald v. Kiloo Aps*, 385 F. Supp. 3d 1022, 1035–36 (E.D. Cal. 2019).
[154] *See, e.g., McGinnis v. U.S. Cold Storage, Inc.*, 382 F. Supp. 3d 813 (N.D. Ill. 2019).
[155] *Rosenbach v. Six Flags Entm't Corp.*, 129 N.E. 3d 1197, 1207 (Ill. 2019).
[156] *See, e.g., Rapai v. Hyatt Corp.*, No. 2017-CH-14483 (Ill. Cir. Ct. Sept. 26, 2019); *see also Miller v. Southwest Airlines Co.*, 926 F.3d 898 (7th Cir. 2019); *Rottner v. Palm Beach Tan, Inc.*, 2019 Ill. App. 180691-U (Ill. App. Ct. 2019).
[157] *See, e.g., Patel v. Facebook*, 932 F.3d 1264 (9th Cir. 2019).

Interestingly, at least one court has held that notwithstanding the reversal of Rosenbach, a mere procedural violation of BIPA may not be sufficient to hold an organization liable for heightened statutory damages. Instead, intentional conduct must be of the sort that "desires to cause [the type of] consequences" that BIPA was meant to protect against.[158]

3. Driver's Privacy Protection Act (DPPA) Litigation

One of the lingering issues in DPPA cases has been what constitutes a "motor vehicle record," and whether information gleaned off of drivers' licenses is covered. In *Wilcox v. Swapp*, plaintiff alleged that law firms misused police reports from "SECTOR" software, which scanned drivers' licenses as part of the creation of police reports, in violation of DPPA. The *Wilcox* court ultimately granted plaintiffs class certification.[159]

By contrast, in *Andrews v. Sirius XM Radio*, a case where plaintiffs alleged that Sirius XM was misusing drivers' license information provided at the point of sale with car dealerships, the Ninth Circuit held that "record" within the DPPA referred to records with the DMV. A driver's license, on the other hand, belongs to the driver, and therefore is not a motor vehicle record under the statute.[160]

4. Wiretap and Illegal Interception Litigation

Plaintiffs continue to use federal and state wiretap statutes in creative ways against new technology, even though the wiretap statutes were clearly written in the days of landlines and early cellphones.[161]

In *S.D. v. Hytto Ltd., dba Lovense*, the complaint alleged that a Chinese connected sex toy company illegally intercepted "Body Chat" signals between users. While assessing defendant's motion to dismiss, the court held that for the purposes of the federal wiretap claims, the vibration signals could be communications content because they meant to communicate touch.[162]

Hytto highlights how courts have struggled with whether the capturing of various types of data could be an interception of "content" under various wiretapping statutes. However, courts have become increasingly willing to interpret wiretap statutes beyond their plain meaning to allow plaintiffs into discovery. For example, one court held that the use of a third-party technology to track how a user navigates a website could constitute unlawful interception.[163] Another court held that even the use of pixels for tracking viewable content could constitute an "interception of content," even though the pixel does not intercept the streaming content at all.[164]

[158] *Rogers v. CSX Intermodal Terminals, Inc.*, 2019 U.S. Dist. LEXIS 151135, at *12 (N.D. Ill. Sept. 5, 2019).
[159] *Wilcox v. Swapp*, 330 F.R.D. 584 (E.D. Wash. 2019).
[160] *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253 (9th Cir. 2019).
[161] Indeed, at least one court in 2019 expressed doubt that wiretap acts like the California Invasion of Privacy Act were meant to cover software as "devices." *See In re Google Location History Litig.*, 2019 U.S. Dist. LEXIS 219258 (N.D. Cal. Dec. 19, 2019) (granting motion to dismiss).
[162] *S.D. v. Hytto*, No. 18-00688, Dk. 44 (N.D. Cal. May 15, 2019).
[163] *Popa v. Harriet Carter Gifts, Inc.*, 2019 U.S. Dist. LEXIS 210889 (W.D. Pa. Dec. 6, 2019).
[164] *White v. Samsung Electronics America, Inc.*, No. 17-1775 (D.N.J. Aug. 20, 2019).

Not all attempts to apply wiretap legislation to new technologies are successful, however. In *Zak v. Bose*, for example, the plaintiffs alleged that Bose headphone mobile software secretly listens and tracks user listening preferences. On a Rule 12(b)(6) challenge, the court held that the Federal Wiretap Act claims should be stricken because a defendant does not have to be an intended participant in the conversation, just a participant. The court held that the defendant can even be a participant simply "through fraud in the inducement," citing to Seventh Circuit law.[165]

One of the most interesting developments in California Invasion of Privacy Act (CIPA) cases is the reversals of class certification orders in 2019. In *NEI Contracting Engineering v. Hanson Aggregates*, plaintiffs alleged that the defendant illegally recorded customers' incoming cell phone calls to place orders. The lower court initially certified a class, and then decertified the order because the defendant later showed that at least nine customers had consented to being recorded, notwithstanding the allegation that there was a failure to warn about the recording practices.

Similarly, in *Reyes v. Educational Credit Management*, plaintiffs alleged that a federal loan program guaranty agency violated CIPA in the course of dealing with plaintiffs and other putative class members. Although the lower court granted class certification, defendant followed *NEI* and appealed the order. The Ninth Circuit reversed the order and remanded the case back to district court, finding that the lower court failed to assess whether plaintiff even had standing under the statute because some putative class members may have given consent to recording for all practical purposes. Perhaps most importantly, the court held that under state law, plaintiffs had the burden to prove that defendant did not have the consent of the plaintiffs to record, and not the other way around.

Importantly, defendants should be mindful of how consent is not only a defense to wiretap claims, but may also be used to destroy class certification. In *Jensen v. Cablevision Systems Corp.*, for example, where plaintiff lessees of smart routers alleged that their routers were being used to cast a public Wi-Fi network, in contravention of wiretap laws, the court agreed that class certification should be denied because of individualized issues regarding consent, and a potentially applicable arbitration provision.[166]

5. Miscellaneous Privacy Misuse Cases

Three additional privacy misuse cases in 2019 are particularly noteworthy because of the interesting legal issues arising from the use of emerging technologies. It has been unclear whether there can be a violation where the only information shared about a consumer is identifying information knowable to the sharing party. In *Wheaton v. Apple*, the court stated that even if Apple was engaged in such practices regarding its music users' listening histories by sharing encrypted "tokens," there can be no privacy violation under Rhode Island and Michigan's music rental privacy statutes, as no personal information was shared.[167]

Dancel v. Groupon presented issues on user geolocation tagging, where third party non-users may be tagged as well. In *Dancel*, Instagram users brought commercial misappropriation of likeness against Groupon for its alleged misuse of Instagram photos of locations where it offered Groupons, allegedly also tagging Instagram users. Plaintiffs alleged that Groupon never obtained their consent, while Groupon stated that it only used photos of Instagram users who did not have their settings set to "private." Ultimately, the court denied plaintiffs' motion for class certification on the basis that it was impossible to tell whether each photo was being misappropriated, without looking at each username and photo on a case-by-case basis.[168]

Zabriskie v. Fannie Mae presented the issue of whether all companies with data-based products risk becoming consumer reporting agencies (CRAs) under the Fair Credit Reporting Act (FCRA). Plaintiffs in *Zabriskie* alleged that Fannie Mae violated the FCRA as a CRA, by making the personal data of borrowers from its underwriting files available to purchasers of Fannie Mae loans through the computer program "Desktop Underwriter," which had aggregated the underwriting data. In reversing the lower court, the Ninth Circuit found that Fannie Mae was not a CRA because it was merely assembling data. A consumer's credit report was independently issued by the national credit bureaus, and whether someone would receive a loan was determined by the lenders. Just because it made this underwriting data available to purchasers of its loans did not make it a CRA.[169]

6. Arbitration as a Defense

As in the context of data breach litigation, arbitration provisions have proven to be similarly useful in the context of data misuse cases. Absent ambiguity in the contract as to whether the topic in dispute is covered by the language of the provision,[170] arbitration agreements have been enforced against all types of data misuse cases.[171]

Indeed, arbitration is so favored, that even when the arbitration agreement is in the form of a "sign-in wrap," – which falls between a browsewrap and a clickwrap – courts have still found in favor of arbitration.[172] One Florida court also held that monthly text messages, with a hyperlink to the arbitration agreement, were sufficient to compel arbitration.[173]

---

[165] *Zak v. Bose Corp.*, 2019 U.S. Dist. LEXIS 54871, at *8 (N.D. Ill. Mar. 31, 2019).
[166] *Jensen v. Cablevision Sys. Corp.*, 372 F. Supp. 3d 95 (E.D.N.Y. 2019).
[167] *Wheaton v. Apple, Inc.*, 2019 U.S. Dist. LEXIS 185524 (N.D. Cal. Oct. 25, 2019).
[168] *Dancel v. Groupon, Inc.*, 2019 U.S. Dist. LEXIS 33698 (N.D. Ill. Mar. 4, 2019); *aff'd Dancel v. Groupon, Inc.*, 2019 U.S. App. LEXIS 37515 (7th Cir. Dec. 18, 2019).
[169] *Zabriskie v. Fannie Mae*, 912 F.3d 1192 (9th Cir. 2019). *Contra McCalmont v. Fannie Mae*, 677 F. App'x 331 (9th Cir. 2017) (unpublished opinion).
[170] S*ee, e.g., Liu v. Four Seasons Hotel*, 2019 Ill. App. 182645 (Ill. Ct. App. 2019) (affirming lower court's refusal to compel arbitration because the language of the arbitration agreement did not cover the BIPA dispute).
[171] *See, e.g., Baron v. Sprint Corp. et al.*, 2019 U.S. Dist. LEXIS 184435 (D. Md. Oct. 24, 2019) (compelling non-signatory family members who used broadband services); *Hughes v. Ancestry.com*, 580 S.W.3d 42 (Mo. Ct. App. 2019) (compelling arbitration in the context of alleged misuse of DNA data); *Horton v. Dow Jones & Co.*, 2019 U.S. Dist. LEXIS 31403 (S.D.N.Y. Feb. 27, 2019) (compelling arbitration in the context of alleged Michigan Video Rental Privacy Act violations).
[172] *See, e.g., Bernardino v. Barnes & Noble Booksellers, Inc.*, 763 F. App'x 101 (2d Cir. 2019).
[173] *MetroPCS Commc'ns, Inc. v. Porter*, 273 So. 3d 1025, 1028–29 (Fla. Ct. App. 2018).

And in the context of collective bargaining agreements, arbitration agreements have been enforced against some of the most draconian of privacy statutes, including BIPA.[174] Thus, as it is with data breach litigation, arbitration agreements will likely remain a primary defense tool for companies in data misuse cases.

Notably, including a 30-day opt out provision has precluded plaintiffs from being able to argue procedural and substantive unconscionability in at least one case, notwithstanding the plaintiff arguing that there was substantial disproportionate bargaining power and the defendant reserving the right to unilaterally change the contract.[175]

7. Settlements

Data misuse cases present unique difficulties in terms of class settlement, because there is often difficulty identifying the actual identities of the entire class. As data is mixed and intermixed, retracing the data back to the actual data subjects can be extremely challenging, if not impossible. As such, *cy pres* settlements may make the most sense.

However, *cy pres* settlements have been heavily criticized in the past two years, as with various settlements involving Google – such as in the settlements of *Google Cookie Placement Consumer Privacy Litigation* and *Google Referrer Header Privacy Litigation*.[176] In the case of *Google Cookie Placement Consumer Privacy Litigation*, which involved Google's online tracking practices using cookies and other similar tagging technologies, the Third Circuit rejected the $5.5 million *cy pres* settlement and remanded, directing the lower court to reassess the settlement under a Rule 23(b)(3) analysis, believing that the lower court had conducted analysis more appropriate of a Rule 23(b)(2) analysis.[177]

And in *Google Referrer Header Privacy Litigation*, involving Google's alleged use of website header information from online traffic, the Supreme Court rejected the $8.5 million *cy pres* settlement and remanded for further analysis. The Court ordered further analysis to assess whether the plaintiffs even had Article III standing.[178] However, commentators saw the result as affected by certain dissenting justices, who would have preferred to reverse the deals.[179]

C. PRODUCT LIABILITY LITIGATION

1. "Unjust Enrichment" Claims Based on Data Vulnerability

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 precedent.[180]

Plaintiffs' most significant recent success is *Flynn v. FCA (Fiat)*, where the plaintiffs alleged that the automobile manufacturer should be liable for cyber vulnerabilities in its connected cars. Although Fiat argued that none of plaintiffs' vehicles had actually been hacked, the

[174] *Miller v. Southwest Airlines Co.*, 926 F.3d 898 (7th Cir. 2019).
[175] *Wainblat v. Comcast Cable Commc'ns, LLC*, 2019 U.S. Dist. LEXIS 190650 (D. Mass. Nov. 4, 2019).
[176] *See* Donald Frederico, *Google, Cookies, and Cy-Pres-Only Settlements*, Nat'l L. Rev. (Aug. 8, 2019), https://www.natlawreview.com/article/google-cookies-and-cy-pres-only-settlements.
[177] *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 934 F.3d 316 (3d Cir. 2019).
[178] *Frank v. Gaos*, 139 S. Ct. 1041 (2019).
[179] Ben Kochman, *High Court Boots Google Privacy Deal For Standing Issues*, Law360 (Mar. 20, 2019), https://www.law360.com/articles/1130806/high-court-boots-google-privacy-deal-for-standing-issues.
[180] *See, e.g., Brodsky v. Apple, Inc.*, 2019 U.S. Dist. LEXIS 148808 (N.D. Cal. Aug. 30, 2019) (granting motion to dismiss in case alleging that two factor authentication was a product defect); *Williams-Diggins v. Health*, 2018 U.S. Dist. LEXIS 206195 (N.D. Ohio Dec. 6, 2018) (holding 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).

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 could have been a viable theory.[181] When the plaintiffs sought class certification, the court granted certification on the smaller state subclasses while denying certification on the larger national classes.[182]

However, more product liability cases suggest that plaintiffs will likely have to demonstrate foreseeability in order to convince courts that their claims are actually viable. In *Beyer v. Symantec*, for example, plaintiffs alleged that they overpaid for the software due to security vulnerabilities.[183] In granting Symantec's motion to dismiss on Article III grounds, the court rejected the overpayment theory by citing to *Cahen v. Toyota Motor*[184] for plaintiffs' failure to allege tangible harm. In allowing plaintiffs an opportunity to amend, the court allowed for "limited and focused" discovery on (1) source code that would show connections between the vulnerabilities and malfunctions, if any, and (2) suspected and known incidents of third-party exploitation of the vulnerability.[185]

And in *Williams v. Apple*, where plaintiffs alleged that Apple's operating system had a defect that allowed Apple and unknown defendants to listen into conversations, plaintiffs stated causes of action for product liability, breach of implied warranties, and unjust enrichment. In granting the motion to dismiss, the court pointed out that products liability requires foreseeability and knowledge, which plaintiffs could not just allege conclusorily. The breach of warranty claims failed as plaintiffs did not allege when such promises were made, just as they had failed to allege actual misrepresentations.[186]

2. False Claims Act Claims for Failure to Secure

Two 2019 cases demonstrate that government vendors and suppliers may also be subject to False Claims Act (FCA) claims, when their products or services suffer from cybersecurity or privacy vulnerabilities:

- A California federal court allowed a relator's False Claims Act suit against two federal contractors to proceed beyond motions to dismiss, where the relator's allegations centered on purported noncompliance with federal cybersecurity requirements. While defendant contractors alleged that the government had some knowledge of the noncompliance, the court found it probative that defendants "did not fully disclose the extent of AR's noncompliance with relevant regulations," thereby implying that contractors have broader disclosure obligations.[187]
- In July 2019, the federal and several state governments unsealed a $8.6 million deal between them and Cisco Systems for Cisco's alleged sale of products with significant security flaws, even after the relator reported the flaws to Cisco.[188]

Thus, in addition to general product liability claims, companies providing products and services to government entities should be mindful of the prospect of FCA claims as well.

D. SECURITIES LITIGATION

Until 2017, plaintiffs alleging loss to the value of their securities and stakeholder interests from privacy events had been relatively unsuccessful in securities class actions.[189] However, when plaintiffs in the Yahoo! breach derivative action reportedly obtained an $80 million settlement in early 2018, many experts feared that the "first major recovery" in a privacy-based securities class action would precipitate similar, large settlements in other cases.[190]

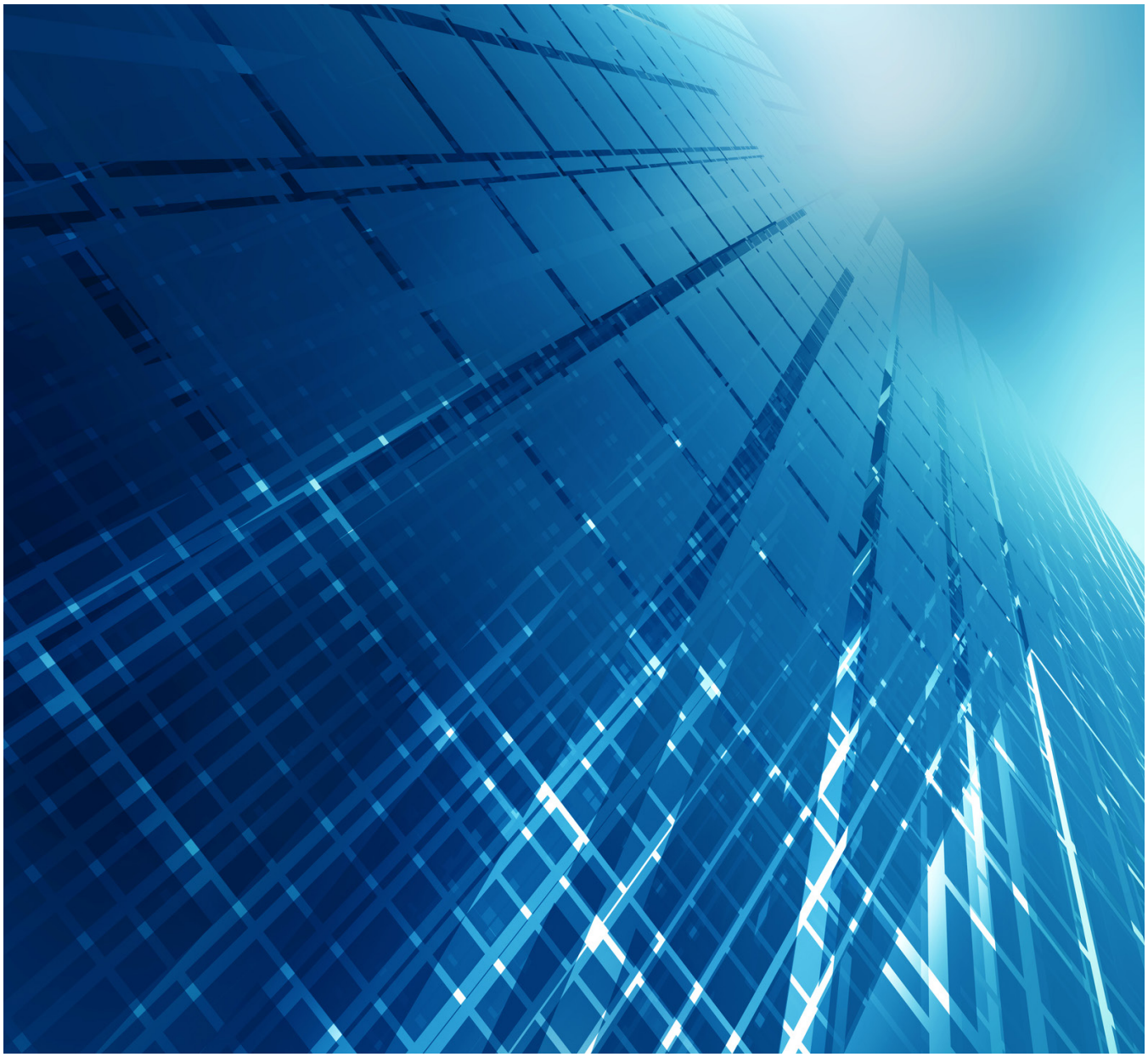
Such a rain of securities litigation never occurred. Instead, recent litigation suggests that plaintiffs still face substantial challenges in most scenarios, other than where privacy issues are actually known and intentionally withheld including:

- Disclosures about ongoing privacy events – *In PayPal Securities Litigation,* plaintiff shareholders alleged that 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 twice dismissing the case, the court held 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,[191] the court ultimately dismissed the case with prejudice, noting that the plaintiffs had great difficulty demonstrating scienter.[192] PayPal demonstrates that where an organization is still navigating a breach event, it is difficult to contend that ongoing disclosures evidence an intent to hide the truth, when the disclosures themselves contradict any such intent. Likewise, plaintiffs who similarly sued Facebook for the ongoing privacy events relating to Cambridge Analytica had substantial difficulty demonstrating scientier and falsity for statements made regarding the ongoing investigation.[193]

[181] *Flynn v. FCA US LLC*, 2017 U.S. Dist. LEXIS 133365 (S.D. Ill. Aug. 21, 2017).
[182] *Flynn v. FCA US LLC*, 327 F.R.D. 206 (S.D. Ill. 2018).
[183] *Beyer v. Symantec Corp.*, 2019 U.S. Dist. LEXIS 30625, at *3 (N.D. Cal. Feb. 26, 2019).
[184] *Cahen v. Toyota Motor Corp.*, 717 F. App'x 720 (9th Cir. 2017).
[185] *Beyer*, 2019 U.S. Dist. LEXIS 30625 at *18.
[186] *Williams v. Apple, Inc.*, 2019 U.S. Dist. LEXIS 78772 (S.D. Tex. May 9, 2019).
[187] *United States ex. rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240, 1246 (E.D. Cal. 2019).
[188] Alexis Ronickher, *Cisco FCA Deal Shows Viability Of Cybersecurity Qui Tams*, Law360 (Aug. 5, 2019), https://www.law360.com/articles/1184931.
[189] *See, e.g.*, Order, *Davis v. Steinhafel*, No. 14-203, ECF 88 (D. Minn. July 7, 2016) (dismissing claims against board of directors of Target Corporation).
[190] 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/.
[191] *Sgarlata v. PayPal Holdings, Inc.* (*In re PayPal Holdings Inc. Sec. Litig.*), 2018 U.S. Dist. LEXIS 210564 (N.D. Cal. Dec. 13, 2018).
[192] *Sgarlata v. PayPal Holdings, Inc.* (*In re PayPal Holdings Inc. Sec. Litig.*), 2019 U.S. Dist. LEXIS 160126 (N.D. Cal. Sept. 18, 2019).
[193] *In re Facebook, Inc. Sec. Litig.*, 405 F. Supp. 3d 809 (N.D. Cal. 2019) (motion to dismiss granted with leave to amend).

- Failure to disclose about unexpected events – In *Kim v. Advanced Micro Devices*, plaintiffs were not able to successfully convince a court that AMD's general statements about cyber events and vulnerabilities in its security filings were material misstatements about the likelihood of a microchip vulnerability such as Spectre appearing. In granting AMD's motion to dismiss, the court noted that there were no allegations that AMD ever suspected the Spectre vulnerability before it was announced, and that plaintiffs did not allege that anyone actually successfully exploited Spectre.[194]

- Failure to disclose about known events – The above cases should be compared to In *re Equifax Inc. Securities Litig*. There, the court refused to dismiss plaintiff's claims against the former CEO and the company itself, finding that certain statements by the company regarding compliance with data protection laws were actionable and that plaintiff pleaded detailed allegations demonstrating Equifax's systems were "grossly deficient and outdated, below industry standards, and vulnerable to attack." The court limited the scope of allegedly false or misleading statements that could be actionable, however, holding that (1) "Defendants were under no duty to disclose the existence of the Data Breach before they knew it had occurred"; (2) the mere "occurrence of the Data Breach did not itself make [certain] prior statements false or misleading"; (3) Defendants' warnings that "Equifax could be vulnerable to a data breach" were not misleading; and (4) Defendants' representations about certain internal control in place at Equifax were not false or misleading.[195]



[194] *Kim v. Advanced Micro Devices, Inc.*, 2019 U.S. Dist. LEXIS 87287 (N.D. Cal. May 23, 2019).
[195] *In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189 (N.D. Ga. 2019).

IV. DEVELOPMENTS IN REGULATORY ENFORCEMENT

Perhaps due in part to the international privacy law environment, regulators are taking increasingly aggressive postures on privacy. With the exception of large incidents, the Department of Health and Human Services (HHS) and its Office of Civil Rights (OCR) have tended to impose proportionally higher fines per consumer record than the Federal Trade Commission (FTC) and State Attorneys General (AGs), although the FTC and AGs continue to be very active.

A. ENFORCEMENT EFFORTS INVOLVING DATA INCIDENTS AND MISUSE

In January 2019, a large retailer reached a settlement with 43 states and the District of Columbia, agreeing to pay $1.5 million to resolve an investigation into a 2013 data breach that affected approximately 370,000 credit cards. The retailer agreed to update its credit card processing software and utilize additional technologies to protect customers' data.[196]

In January 2019, a large American power company agreed to pay $10 million to settle allegations that it put the U.S. electric grid at high risk of attack for more than five years by failing to meet federal cybersecurity standards. A report issued by the North American Electric Reliability Corp. cited the company's violations and lack of managerial oversight as reasons for the settlement.[197]

In June 2019, the New York Attorney General's Office reached an agreement with a sock startup that allegedly waited more than three years to provide notice to nearly 40,000 consumers of a payment card breach. The startup agreed to pay $65,000 in penalties and implement various data security policies.[198]

In June 2019, the FTC reached a settlement with an auto dealer software provider over data security allegations, wherein the company agreed to take steps to better protect the data it collects. In its complaint, the FTC alleged that the company failed to implement security measures to protect personal data stored on its network and that such failure led to a 2016 breach where a hacker gained access to the unencrypted personal information of approximately 12.6 million consumers stored by the company's customers (more than 69,000 individuals had their SSNs, driver's license numbers and birth dates, as well as wage and financial information downloaded). The settlement is notable because the company does not market or sell products directly to consumers, but rather, only to businesses. Nonetheless, the FTC still alleged that the software developer was covered by the Gramm-Leach Bliley Act (GLBA), due to its association with its customers, which were GLBA-covered entities.[199]

In one of the most closely watched enforcement actions involving IoT, the FTC in July 2019 settled with a connected home devices manufacturer, its allegations involving security flaws with the manufacturer's connected cameras. The FTC alleged that the security flaws allowed hackers to possibly access the cameras' live video and audio feeds. Although no money was exchanged, the manufacturer agreed to "implement a comprehensive software security program, including specific steps to ensure that its Internet-connected cameras and routers are secure. This includes implementing security planning, threat modeling, testing for vulnerabilities before releasing products, ongoing monitoring to address security flaws, and automatic firmware updates, as well as accepting vulnerability reports from security researchers."[200]

Almost concurrently, in late July 2019, the FTC announced two of its largest settlements in history. Its first settlement with Equifax had the credit reporting agency paying $575 million to the FTC, Consumer Financial Protection Bureau (CFPB), and 50 states and territories, which alleged that Equifax failed to take reasonable steps to secure its network, leading to a data breach in 2017 that allegedly affected 147 million people.[201] In addition, to resolve civil claims filed by consumers across multiple states, Equifax agreed to pay additional amounts up to a total of $700 million, which is inclusive of $575 million to authorities.[202] The settlement was amongst the first of its kind to package both the civil and regulatory actions into one settlement.

[196] *AG Paxton Announces $1.5 Million Settlement with Neiman Marcus over Data Breach*, Office of Tex. Att'y Gen. Ken Paxton (Jan. 8, 2019), https://www.texasattorneygeneral.gov/news/releases/ag-paxton-announces-15-million-settlement-neiman-marcus-over-data-breach.

[197] Alison Noon, *Power Co. Fined Record $10M for 127 Cybersecurity Lapses*, Law360 (Jan. 31, 2019), https://www.law360.com/articles/1124166/power-co-fined-record-10m-for-127-cybersecurity-lapses.

[198] *Attorney General James Announces $65,000 Settlement With Online Retailer Bombas LLC Over Consumer Data Breach*, Office of N.Y. Att'y. Gen. Letitia James (June 6, 2019), https://ag.ny.gov/press-release/attorney-general-james-announces-65000-settlement-online-retailer-bombas-llc-over.

[199] *Auto Dealer Software Provider Settles FTC Data Security Allegations*, Fed. Trade Comm'n (June 12, 2019), https://www.ftc.gov/news-events/press-releases/2019/06/auto-dealer-software-provider-settles-ftc-data-security.

[200] *D-Link Agrees to Make Security Enhancements to Settle FTC Litigation*, Fed. Trade Comm'n (July 2, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/d-link-agrees-make-security-enhancements-settle-ftc-litigation.

[201] *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, Fed. Trade Comm'n (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

[202] Ben Kochman, *Equifax To Pay Up To $700M To Settle Data Breach Probes*, Law360 (July 22, 2019), https://www.law360.com/articles/1180467/equifax-to-pay-up-to-700m-to-settle-data-breach-probes.

Shortly thereafter, the FTC and Department of Justice (DOJ) announced another of their largest settlements in history ($5 billion) with a large social media company. The FTC alleged that the company violated a prior consent decree relating to users' abilities to control their information and allowed at least one third-party application developer to circumvent the company's access controls. The FTC and DOJ required that the company submit to new requirements and give users more control over their information and privacy.[203]

In August 2019, the FTC entered into a consent decree with an email management service, requiring it to delete data previously collected from users, and restructuring how and what it collects. The FTC alleged that it had received complaints about how the company was collecting transactional data in user emails, although the company's marketing campaigns had promised consumers privacy and confidentiality. The FTC did not opine on whether the company's use of data was inconsistent with its user terms or privacy policy, but the FTC also issued no monetary penalties.[204]

In November 2019, the FTC settled with an application developer that provides back-end operation services to multi-level marketers, ranging from compensation, inventory, orders, accounting, training, data security, and website hosting services. The FTC alleged that the developer stored sensitive consumer personal information without implementing reasonable cybersecurity safeguards. As a result of the respondent's alleged failure to implement low-cost readily available protections, the FTC alleged that a hacker was able to infiltrate the company's servers and access about one million consumer records. As part of the settlement, the developer is required to implement substantially improved cybersecurity measures and be subject to third-party assessments every two years.[205]

In December 2019, the FTC granted final approval of a settlement with the former CEO of Cambridge Analytica and an affiliated application developer, while the company itself filed for bankruptcy. The respondents are prohibited from making false or deceptive statements regarding the extent to which they collect, use, share, or sell personal information, as well as the purposes for which they collect, use, share, or sell such information. In addition, they are required to delete or destroy any personal information collected from consumers via the company's GSRApp and any related work product that originated from the data.[206]

B. INCREASED EFFORTS ON COPPA ENFORCEMENT

In February 2019, the FTC obtained a $5.7 million consent decree against a video social networking application, in connection with allegations that the application collected personal information from children in contravention of the Children's Online Privacy Protection Act (COPPA). In addition to the civil penalty, the settlement also required the app to comply with COPPA and take offline all videos made by children under the age of 13.[207]

In April 2019, the operators of a dress-up games website and an online rewards website each separately agreed to settle FTC allegations that they failed to reasonably secure consumer data, which resulted in breaches of both websites. The dress-up games website faced additional alleged violations under COPPA and as part of its proposed settlement, the company agreed to pay $35,000 in civil penalties, is prohibited from violating COPPA, and must implement a comprehensive data security program. The online rewards website is prohibited from making misrepresentations regarding its privacy and data security practices, must implement a comprehensive information security program, and must obtain independent biennial assessments of its program.[208]

[203] *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, Fed. Trade Comm'n (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions; *Facebook Agrees to Pay $5 Billion and Implement Robust New Protections of User Information in Settlement of Data-Privacy Claims*, Dep't of Justice (July 24, 2019), https://www.justice.gov/opa/pr/facebook-agrees-pay-5-billion-and-implement-robust-new-protections-user-information.

[204] *Operator of Email Management Service Settles FTC Allegations that it Deceived Consumers About How it Accesses and Uses Emails*, Fed. Trade Comm'n (Aug. 8, 2019), https://www.ftc.gov/news-events/press-releases/2019/08/operator-email-management-service-settles-ftc-allegations-it.

[205] *Utah Company Settles FTC Allegations it Failed to Safeguard Consumer Data*, Fed. Trade Comm'n (Nov. 12, 2019), https://www.ftc.gov/news-events/press-releases/2019/11/utah-company-settles-ftc-allegations-it-failed-safeguard-consumer.

[206] *FTC Grants Final Approval to Settlement with Former Cambridge Analytica CEO, App Developer over Allegations they Deceived Consumers over Collection of Facebook Data*, Fed. Trade Comm'n (Dec. 18, 2019), https://www.ftc.gov/news-events/press-releases/2019/12/ftc-grants-final-approval-settlement-former-cambridge-analytica.

[207] *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations that it Violated Children's Privacy Law*, Fed. Trade Comm'n (Feb. 27, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc.

[208] *FTC Alleges Operators of Two Commercial Websites Failed to Protect Consumers' Data*, Fed. Trade Comm'n (Apr. 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/04/ftc-alleges-operators-two-commercial-websites-failed-protect.

In May 2019, three dating apps were removed from the online stores after the FTC alleged that children as young as 12 were accessing the apps. The FTC alleged that while the apps' privacy policies claimed to prohibit users under the age of 13, the apps failed to prevent users under 13 from being contacted by other app users. Additionally, the FTC alleged that the company operating the three apps was aware that children under 13 were using the apps and thus, were obligated to comply with COPPA, which it allegedly failed to do.[209]

In September 2019, the FTC and the New York AG entered into a $170 million settlement with Google over how YouTube allegedly treats children's privacy. The FTC alleged that Google inadequately protected children who used its video-streaming service, and that it had actual knowledge of children's information being impermissibly collected in contravention of COPPA. As part of the settlement, Google and YouTube will develop, implement, and maintain a system that permits channel owners to identify their child-directed content on the YouTube platform to ensure that it complies with COPPA.[210] Following the settlement, secondary authorities opined that "YouTube creators may also be held liable for COPPA violations, following [the] FTC settlement."[211]

In October 2019, the FTC entered into a consent decree with the developer of a "stalking app," which allegedly enabled purchasers of the application to secretly monitor the mobile devices upon which they were installed. The FTC alleged that the developer failed to ensure that the apps would be used for lawful and legitimate purposes, did not secure personal information collected from children and others, and misrepresented the extent to which that information would be kept confidential – all allegedly in violation of Section 5 of the FTC Act as well as COPPA. Under the terms of the settlement, the developer may not require that purchasers jailbreak the mobile devices where the applications would be installed, may not hide the application icon on the home screen upon installation, and must obtain an express attestation from the purchaser that the applications would be used for lawful purposes. In addition, the purchase, installation, and use of the application must comply with the parental verification requirements of COPPA.[212]

In December 2019, the Pennsylvania AG settled a data breach case with two travel fare aggregators, involving approximately 21,000 Pennsylvania residents and 880,000 payment cards globally. The AG reported that a hacker had circumvented cybersecurity detection and targeted payments cards. One company was allegedly notified by a business partner of the compromise. As part of the consent decree, the two aggregators agreed to pay $110,000 and strengthen their security practices going forward.[213]

C. ENFORCEMENT EFFORTS INVOLVING MEDICAL INFORMATION

Medical data continues to yield some of the largest regulatory payouts per consumer record. In January 2019, a large health insurance company settled with the California AG's Office regarding allegations that the company violated state privacy laws when it mailed letters with envelope windows that revealed the recipient was taking HIV-related medication. Nearly 2,000 Californians were affected. The company agreed to pay almost $1 million to take steps toward protecting customer medical information and to complete an annual privacy risk assessment for the next three years.[214]

In May 2019, a Tennessee diagnostic medical imaging services company agreed to settle potential HIPAA violations by paying $3 million to the HHS OCR and adopting a corrective action plan. In 2014, the company learned that one of its FTP servers allowed uncontrolled access to its patients' protected health information ("PHI") and that such PHI was visible on the internet for a period of time. More than 300,000 patients were affected. The OCR's investigation found that the company did not thoroughly investigate the incident in a timely manner, did not notify impacted patients in a timely manner, and did not have adequate measures in place to protect PHI.[215]

In May 2019, an Indiana medical records services company agreed to settle potential HIPAA violations by paying $100,000 to the OCR and adopting a corrective action plan. In 2015, the company filed a breach report with the OCR stating that hackers accessed the electronic protected health information ("ePHI") of approximately 3.5 million people. The OCR's investigation revealed that the company did not conduct a comprehensive risk analysis prior to the breach.[216]

In May 2019, the United States Attorney's Office for the District of Kansas announced that a Kansas hospital agreed to pay $250,000 to settle claims that it violated the False Claims Act. The government alleged that the hospital submitted false claims to the Medicare and Medicaid Programs pursuant to the Electronic Health Records Incentive Program.[217]

---

[209] *App Stores Remove Three Dating Apps After FTC Warns Operator About Potential COPPA, FTC Act Violations*, Fed. Trade Comm'n (May 6, 2019), https://www.ftc.gov/news-events/press-releases/2019/05/app-stores-remove-three-dating-apps-after-ftc-warns-operator.

[210] *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, Fed. Trade Comm'n (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

[211] Sarah Perez, *YouTube creators may also be held liable for COPPA violations, following FTC settlement*, TechCrunch (Sept. 4, 2019), https://techcrunch.com/2019/09/04/youtube-creators-may-also-be-held-liable-for-coppa-violations-following-ftc-settlement/.

[212] *FTC Brings First Case Against Developers of "Stalking" Apps*, Fed. Trade Comm'n (Oct. 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/10/ftc-brings-first-case-against-developers-stalking-apps.

[213] *AG Shapiro Announces Settlement with Orbitz and Expedia in Data Breach Affecting Pennsylvania Consumers*, Office of PA. Att'y Gen. Josh Shapiro (Dec. 13, 2019), https://www.attorneygeneral.gov/taking-action/press-releases/ag-shapiro-announces-settlement-with-orbitz-and-expedia-in-data-breach-affecting-pennsylvania-consumers/.

[214] Kaitlyn Burton, *Aetna To Pay Nearly $1M To End HIV Info Row In Calif.*, Law360 (Jan. 31, 2019), https://www.law360.com/articles/1123973.

[215] *Tennessee Diagnostic Medical Imaging Services Company Pays $3,000,000 to Settle Breach Exposing Over 300,000 Patients' Protected Health Information*, Dep't of Health & Hum. Servs. (May 6, 2019), https://www.hhs.gov/about/news/2019/05/06/tennessee-diagnostic-medical-imaging-services-company-pays-3000000-settle-breach.html.

[216] *Indiana Medical Records Service Pays $100,000 to Settle HIPAA Breach*, Dep't of Health & Hum. Servs. (May 23, 2019), https://www.hhs.gov/about/news/2019/05/23/indiana-medical-records-service-pays-100000-to-settle-hipaa-breach.html.

[217] *Kansas Hospital Agrees to Pay $250,000 To Settle False Claims Act Allegations*, Dep't of Justice, U.S. Att'y's Office, D. Kans. (May 31, 2019), https://www.justice.gov/usao-ks/pr/kansas-hospital-agrees-pay-250000-settle-false-claims-act-allegations.

In May 2019, a medical software provider agreed to pay $900,000 to more than a dozen state attorneys general and take corrective actions to resolve alleged state law and HIPAA violations in relation to a 2015 data breach wherein hackers stole the ePHI of more than 3.9 million individuals. The ePHI included names, SSNs, lab results, diagnoses, and health insurance policy information. This is the first multistate lawsuit involving a HIPAA-related data breach.[218]

In July 2019, a coalition of state AGs and a large health insurance company agreed to a $10 million settlement for a data breach that allegedly exposed the data of 10.4 million consumers nationwide. The regulators alleged that the vulnerability that had led to the breach that was exposed for almost a year.[219]

In August 2019, an electronic health records company settled with the DOJ over allegations of kickbacks in addition to HIPAA violations. The company paid a total of $145 million to the DOJ.[220]

In October 2019, the HHS imposed one of its largest fines on record proportional to the number of patients at issue. The HHS reported that Jackson Health Systems failed to implement reasonable security measures and timely notify the HHS of security incidents, with fewer than 26,000 patients at issue over four years. However, the HHS imposed a $2.15 million fine.[221] The fine marked the beginning of a number of aggressive settlements by the HHS through the end of 2019.

In November 2019, the HHS continued its trend towards increasingly aggressive enforcement efforts by fining the University of Rochester Medical Center $3 million. The HHS alleged that the medical center had failed to encrypt and secure mobile devices, which resulted in breach reports with the OCR in 2013 and 2017. The total number of patients at risk from the incidents was not disclosed.[222]

Almost concurrently, the HHS imposed a $1.6 million penalty against the Texas Health and Human Services Commission, a public entity, for exposing an unknown number of patient records when migrating certain records from a private server to a public server. The commission apparently discovered the incident in 2015, then reported that only 6,617 patient records were viewable publicly over the internet.[223]

Then in December 2019, the HHS fined Sentara Hospitals $2.15 million for inaccurately reporting an incident where it accidentally disclosed the names, account numbers, and dates of services for 577 patients by mailing notices to the wrong addresses. The HHS apparently took issue with Sentara's interpretation of the incident, which minimized the significance of the data set disclosed.[224]

Lastly, organizations should be mindful that the HHS has begun imposing fines for patients being denied access to their health records, including for being charged unreasonable fees,[225] and for being given records in a "readily producible format" of the patient's choice.[226]

D. OTHER NOTABLE ENFORCEMENT EFFORTS

In March 2019, the U.S. Department of Housing and Urban Development (HUD) issued a public statement regarding its renewal of charges against a large social media network for allegedly allowing advertisers of housing and housing-related services to target specific demographic groups, allegedly in violation of the Fair Housing Act. The press release shortly followed a civil settlement between the company and numerous civil liberty groups on similar charges. The settlement is part of a new debate regarding whether third-party targeted advertising affecting protected classes under anti-discrimination laws can create legal liability for technology platforms.[227]

The FTC continues to enforce against misrepresentations of compliance with various privacy programs including the EU-U.S. Privacy Shield program. In June 2019, the FTC announced that more than a dozen such companies have been warned for falsely claiming participation in international privacy agreements.[228] As such, companies should ensure their websites, privacy policies, public documents, and statements accurately reflect their current data privacy practices.

---

[218] *Attorney General Josh Stein Reaches $900,000 Multistate Settlement with Medical Informatics Engineering over Data Breach*, Office of N.C. Att'y Gen. Josh Shapiro (May 23, 2019), https://ncdoj.gov/attorney-general-josh-stein-reaches-900000-multi/.

[219] *Attorney General Ferguson's Investigation into Premera Data Breach Results in Permera Paying $10 Million over Failure to Protect Sensitive Information*, Office of Wash. Att'y Gen. Bob Ferguson (July 11, 2019), https://www.atg.wa.gov/news/news-releases/attorney-general-ferguson-s-investigation-premera-data-breach-results-premera; *Attorney General Reaches Settlement with Premera over Data Breach*, Alaska Dep't of Law (July 11, 2019), http://www.law.state.ak.us/press/releases/2019/071119-Premera.html.

[220] Hailey Konnath, *Allscripts to Pay $145M After DOJ Looks At Kickbacks, HIPAA*, Law360 (Aug. 8, 2019), https://www.law360.com/articles/1186941/allscripts-to-pay-145m-after-doj-looks-at-kickbacks-hipaa.

[221] *OCR Imposes a $2.15 Million Civil Money Penalty against Jackson Health System For HIPAA Violations*, Dep't of Health & Hum. Servs. (Oct. 23, 2019), https://www.hhs.gov/about/news/2019/10/23/ocr-imposes-a-2.15-million-civil-money-penalty-against-jhs-for-hipaa-violations.html.

[222] *Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA Settlement*, Dep't of Health & Hum. Servs. (Nov. 5, 2019), https://www.hhs.gov/about/news/2019/11/05/failure-to-encrypt-mobile-devices-leads-to-3-million-dollar-hipaa-settlement.html.

[223] *OCR Imposes a $1.6 Million Civil Money Penalty against Texas Health and Human Services Commission For HIPAA Violations*, Dep't of Health & Hum. Servs. (Nov. 7, 2019), https://www.hhs.gov/about/news/2019/11/07/ocr-imposes-a-1.6-million-dollar-civil-money-penalty-against-tx-hhsc-for-hipaa-violations.html.

[224] *OCR Secures $2.175 Million HIPAA Settlement after Hospitals Failed to Properly Notify HHS of a Breach of Unsecured Protected Health Information*, Dep't of Health & Hum. Servs. (Nov. 27, 2019), https://www.hhs.gov/about/news/2019/11/27/ocr-secures-2.175-million-dollars-hipaa-settlement-breach-notification-and-privacy-rules.html.

[225] OCR Settles First Case in HIPAA Right of Access Initiative, Dep't of Health & Hum. Servs. (Sept. 9, 2019), https://www.hhs.gov/about/news/2019/09/09/ocr-settles-first-case-hipaa-right-access-initiative.html; *OCR Settles Second Case In HIPAA Right of Access Initiative*, Dep't of Health & Hum. Servs. (Dec. 12, 2019), https://www.hhs.gov/about/news/2019/12/12/ocr-settles-second-case-in-hipaa-right-of-access-initiative.html.

[226] Dep't of Health & Hum. Servs., *OCR Settles Second Case In HIPAA Right of Access Initiative, supra* note 225.

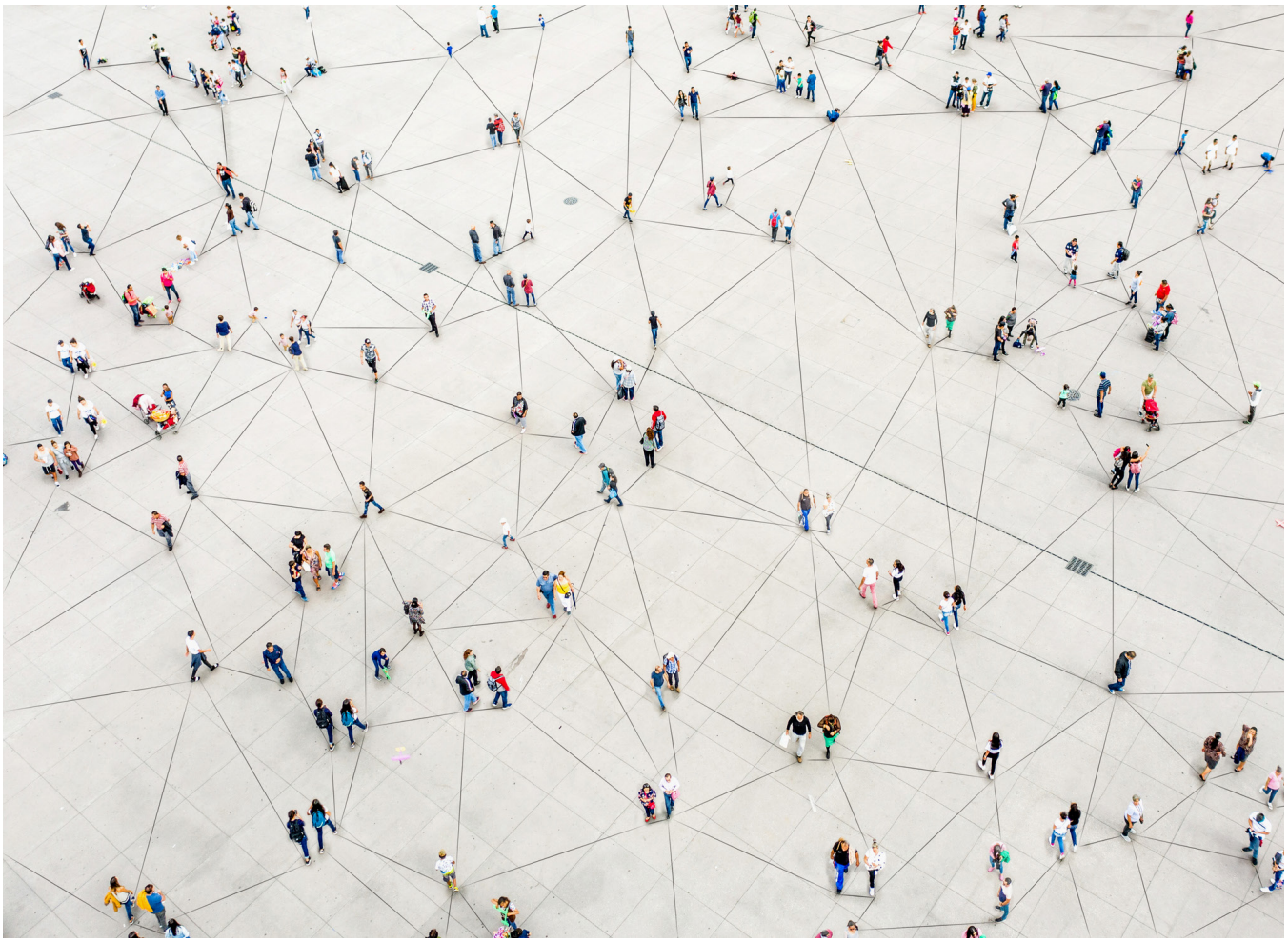
[227] *HUD Files Housing Discrimination Complaint Against Facebook*, Dep't of Hous. & Urban Dev. (Aug. 17, 2018), https://www.hud.gov/press/press_releases_media_advisories/HUD_No_18_085.

[228] *FTC Takes Action against Companies Falsely Claiming Compliance with the EU-U.S. Privacy Shield, Other International Privacy Agreements*, Fed. Trade Comm'n (June 14, 2019), https://www.ftc.gov/news-events/press-releases/2019/06/ftc-takes-action-against-companies-falsely-claiming-compliance-eu.

By the year's end, the FTC settled with 10 companies that had allegedly falsely represented that they were certified under the EU-U.S. Privacy Shield program. The FTC noted that although these companies claimed self-certification under the Privacy Shield for transatlantic data transfers, they did not actually meet the requirements under the program, or complete the steps necessary to participate.[229] Notably, the FTC pursued suit against those that did not settle with the FTC despite its earlier warnings.[230]

Importantly, the Consumer Financial Protection Bureau (CFPB) ended the year with one of the largest privacy settlements per consumer against the background check company Sterling Infosystems. The CFPB alleged that Sterling violated the Fair Credit Reporting Act (FCRA) by failing to adopt reasonable policies that would ensure the accuracy of its reporting information. Notably, the CFPB alleged that Sterling maintained a dispute resolution department that was extremely slow in responding to disputes from job applicants, lacked procedures which would rigorously segregate different records, and maintained very old criminal records. Approximately 7,100 consumer records were at issue, such that the fine was over $1,000 per consumer.[231]

In a joint press conference, the U.S. Department of Commerce and the European Commission announced that the Privacy Shield program passed its third annual review by the EU. Approximately 5,000 U.S. companies have signed up for the program to date.[232]



[229] *Five Companies Settle FTC Allegations that they Falsely Claimed Participation in the EU-U.S. Privacy Shield*, Fed. Trade Comm'n (Sept. 3, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/five-companies-settle-ftc-allegations-they-falsely-claimed; *California Company Settles FTC Allegations that it Falsely Claimed Participation in EU-U.S. Privacy Shield*, Fed. Trade Comm'n (Nov. 19, 2019), https://www.ftc.gov/news-events/press-releases/2019/11/california-company-settles-ftc-allegations-it-falsely-claimed; *FTC Announces Settlements with Four Companies Related to Allegations they Deceived Consumers over Participation in the EU-U.S. Privacy Shield*, Fed. Trade Comm'n (Dec. 3, 2019), https://www.ftc.gov/news-events/press-releases/2019/12/ftc-announces-settlements-four-companies-related-allegations-they.

[230] *See, e.g., FTC Charges Nevada Company with Falsely Claiming Participation in the EU-U.S. Privacy Shield*, Fed. Trade Comm'n (Nov. 7, 2019), https://www.ftc.gov/news-events/press-releases/2019/11/ftc-charges-nevada-company-falsely-claiming-participation-eu-us.

[231] Jack Queen, *CFPB Strikes $8.5M Deal Over Inaccurate Background Checks*, Law360 (Nov. 22, 2019), https://www.law360.com/cybersecurity-privacy/articles/1222775/.

[232] Natasha Lomas, *EU-US Privacy Shield passes third Commission 'health check' – but litigation looms*, TechCrunch (Oct. 23, 2019), https://techcrunch.com/2019/10/23/eu-us-privacy-shield-passes-third-commission-health-check-but-litigation-looms/.

IV. INTERNATIONAL DEVELOPMENTS IN EUROPE AND ASIA

A. THE EU AND THE UK

The European Union's General Data Protection Regulation (GDPR) went into effect in 2018. While some private organizations and national data protection authorities (DPAs) struggled to get acquainted during their first year, courts and regulators have begun issuing important precedents.

In the context of data breaches, UK regulators announced in 2019 their intent to impose two significant fines:

- The United Kingdom's Information Commissioner's Office (ICO) announced its intention to fine British Airways £183.39 million for the data breach announced in September 2018, allegedly affecting approximately 500,000 customers since June 2018. The ICO stated that it made its findings as lead supervisory authority on behalf of other EU DPAs.[233] British Airways now has the opportunity to make representations to the ICO as to the proposed findings and sanction.

- Nearly concurrently, the ICO also announced its intention to impose a £99 million fine on Marriott International for the approximately 30 million EU residents' information at issue in the data breach reported in November 2018.[234] Like British Airways, Marriott also has an opportunity to make representations to the ICO.

Due to the advent of the IoT, the EU also passed the EU Cybersecurity Act, effective June 27, 2019, which strengthened the existing mandate of the European Union Agency for Cybersecurity (ENISA) to support EU member states with tackling cybersecurity threats. ENISA will put in place certification schemes for specific connected products, and the European Commission will be able to request certification schemes for specific products and services. The law will create a voluntary certification framework for digital products and services for consumers and for services that underpin critical infrastructures.[235]

In the context of data use, the European DPAs have become increasingly focused on the adtech industry, and made several important intent-to-enforce announcements in 2019:

- In January 2019, France's DPA, the Commission Nationale de l'Informatique et des Libertés (CNIL), announced an intent to fine Google €50 million for Google's failure to fully disclose how data subjects have their personal information collected. It appears that several privacy advocacy groups complained to the CNIL, which then took action.[236]

- In March 2019, the Dutch DPA stated that where consent for cookies is a required condition of accessing a website (a "cookie wall"), such consent is not voluntary and therefore is not valid consent under the GDPR. Industry advocates countered that websites belong to the website owners, and websites do not have to allow any visitors.[237] But the higher courts may not agree: in a separate case in October 2019, the European Court of Justice (ECJ) issued a preliminary ruling in a case against a German online gaming company called Planet49, finding that a pre-checked box authorizing the use of cookies while users visited a website cannot be considered valid consent.[238]

- In June 2019, the ICO announced in a special report that it was investigating the adtech industry and its "real-time bidding (RTB)" systems. The ICO stated in the report that RTB might violate the consent and automated processing requirements of the GDPR, especially if the processing involves special categories of data. The ICO stated that it still has significant concerns around several aspects of adtech, and threatened enforcement in December 2019, with a further update expected in early 2020.[239]

- In June 2019, the CNIL announced that it would publish new guidelines specifically relating to targeted advertising in 2019 and 2020, finding problems with third-party cookies and tracking technologies, and noting again the need for consumer "opt-ins" when websites allow third parties to track users. The CNIL had announced in December 2018 its intent to take action against websites that fail to so do by June 2019.[240]

[233] *Intention to Fine British Airways £183.39m Under GDPR For Data Breach,* Info. Comm'r's Office (Jul. 8, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/.

[234] *Intention to Fine Marriott International, Inc. More than £99m Under GDPR for Data Breach,* Info. Comm'r's Office (July 9, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

[235] Sara Merken, *EU Cybersecurity Law Aims to Fortify Connected Devices*, Bloomberg Law (June 26, 2019), https://news.bloomberglaw.com/privacy-and-data-security/eu-cybersecurity-law-aims-to-fortify-connected-devices.

[236] Tony Romm, *France Fines Google Nearly $57 Million for First Major Violation of New European Privacy Regime*, Wash. Post (Jan. 21, 2019), https://www.washingtonpost.com/world/europe/france-fines-google-nearly-57-million-for-first-major-violation-of-new-european-privacy-regime/2019/01/21/89e7ee08-1d8f-11e9-a759-2b8541bbbe20_story.html.

[237] Natasha Lomas, *Cookie Walls Don't Comply with GDPR, Says Dutch DPA*, TechCrunch (Mar. 8, 2019), https://techcrunch.com/2019/03/08/cookie-walls-dont-comply-with-gdpr-says-dutch-dpa/.

[238] Ben Kochman, *EU Cookie Ruling Tightens Leash On Ad Tech Staple*, Law360 (Oct. 9, 2019), https://www.law360.com/articles/1207005/eu-cookie-ruling-tightens-leash-on-ad-tech-staple.

[239] *Update Report into Adtech and Real Time Bidding,* Info. Comm'r's Office (June 20, 2019), https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

[240] Hunton Andrews Kurth LLP, *CNIL Publishes Guidance On Data Sharing With Business Partners or Brokers*, Lexology (Jan. 2, 2019), https://www.lexology.com/library/detail.aspx?g=b6c6423a-6d9a-40a8-b92a-824d475dab6b.

- The ECJ held in July 2019 that websites that embed third-party social media buttons can be liable for privacy violations by those third parties.[241] This was consistent with (although not based on) the guidelines published by the CNIL in June 2019 and other DPAs relating to cookies and tracking.

- In October 2019, the ECJ handed down a pair of potentially conflicting rulings. In a move limiting the territorial ambit of GDPR, the ECJ ruled that Google did not need to comply with a "request to be forgotten" globally (i.e. it only needs to remove links from its search results in the EU but not elsewhere).[242] But in a separate judgment, the ECJ held that the national courts of individual member states were able to order Facebook to remove defamatory or otherwise illegal statements globally.[243]

Critically, it appears that most EU to U.S. transfer mechanisms will survive the challenges mounted by European advocacy groups. In October 2019, the U.S. Department of Commerce and the European Commission jointly announced that the Privacy Shield program had passed its third annual review.[244] In addition, the European Data Protection Board issued a draft opinion finding ExxonMobil's binding corporate rules (BCRs) to be compliant with the GDPR,[245] alleviating previous fears that European courts may invalidate at least some of the current EU to U.S. transfer mechanisms, creating potential problems for the others as well.

Importantly, one of the biggest developments that will likely affect GDPR compliance is the EU's recent promulgation of class action rules for privacy class actions. In 2019, the English Court of Appeal overturned an earlier decision of the High Court, thereby allowing claims to proceed against Google in the form of an opt-out class action (which is relatively unusual in England). The claims related to a feature which allowed Google to set cookies on mobile devices without the user's knowledge or consent.[246] The class action process is slowly growing from its infancy in the UK, but 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. But it should be noted that 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.[247] Much remains to be seen as to how these new rules will affect litigation trends in the EU.

The UK is due to leave the European Union on January 31, 2020. But GDPR will continue to apply in the UK until the end of the transition period following departure, which is expected to last until at least December 31, 2020. After such point, GDPR will cease to apply and the UK's Data Protection Act 2018 (already in force and designed to mirror all relevant provisions of GDPR) will be solely applicable. It remains to be seen how the EU will regard the UK's adequacy of its treatment of personal data as a non-EU country once GDPR ceases to apply in the UK.

B. CHINA

On April 10, 2019, China's Ministry of Public Security (CMPS) published its finalized Guideline for Internet Personal Information Security Protection (the "Guideline"). Although "voluntary," the Guideline sets forth the CMPS' prescribed best practices for cyber-

[241] Ben Kochman, *Facebook's 'Like' Button Makes Sites Liable, EU Court Finds*, Law360 (July 29, 2019), https://www.law360.com/articles/1182789/facebook-s-like-button-makes-sites-liable-eu-court-finds.

[242] Ben Kochman, *Google Must Only Apply 'Right to Be Forgotten' In EU*, Law360 (Sept. 24, 2019), https://www.law360.com/articles/1202254/google-must-only-apply-right-to-be-forgotten-in-eu.

[243] Ben Kochman, *EU Court Says Facebook Takedown Orders Apply Globally*, Law360 (Oct. 3, 2019), https://www.law360.com/articles/1205662/eu-court-says-facebook-takedown-orders-apply-globally.

[244] Lomas, *EU-US Privacy Shield Passes Third Commission "Health Check"– But Litigation Looms, supra* note 232.

[245] *EDPB Releases Opinion On Belgian DPA's BCR Draft Decision*, Int'l Ass'n Privacy Profs. (Nov. 22, 2019), https://iapp.org/news/a/edpb-releases-opinion-on-belgian-dpas-bcr-draft-decision/.

[246] 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.

[247] 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.

security and privacy for "personal information holders and processors," which can potentially cover all entities engaged in services on the internet, private networks, and even offline systems.

In addition to establishing guidance regarding physical, administrative, and technical protections and controls, the Guideline sets forth the following:

- Certain Collections and Disclosures Prohibitions: Mass collection and public disclosure of sensitive information pertaining to the ethnicity, political views, and religious beliefs of Chinese citizens are prohibited. Public disclosure of personal psychological, biometric, and genetic information is also prohibited.

- Limitation of Automatic Processing: Automatic processing of personal information may be permitted so long as the other requirements of China's Cybersecurity Law[248] are met, but opt-out rights must be granted where the purpose is for marketing, personalization, targeting advertising, and filtering search results. Especially where the processing may have legal consequences on the individual (e.g., credit or legal administration), express user consent must be obtained.

- Forward-Looking Technology Requirements: The Guideline requires authentication and verification to protect the integrity and confidentiality of personal information, even for information collected by the IoT.

- National Security Exceptions: As with the Cybersecurity Law, the Guideline provides exceptions to consent requirements (i.e. where the personal information is for national security, national defense, public safety, public health, vital public interest, and crime investigation).

The Guideline also signals the CMPS' view on two potentially important points. First, China's Cybersecurity Law previously only imposed data localization and cross-border data-transfer requirements on "network operators," although what constituted a network operator could have been interpreted broadly. Under the Guideline, it appears that data localization and transfer restrictions will be imposed on all personal information holders and processors. Second, the Guideline prescribes limited guidance on the use of biometric information, which is likely due to the Chinese government's own pervasive use of biometric technologies.[249]

It will be important for U.S.-based companies to consider the guidance, as China is reportedly increasing its efforts to crack down on apps over privacy violations.[250]

Companies should also be aware that China's national law on encryption is effective January 1, 2020, interlaying with China's Cybersecurity Law, which requires the use of commercial encryption. Partially as a result of the current political environment, the new encryption law is refreshingly balanced on its face in how it purportedly treats both domestic and foreign commercial encryption technologies equally. Under the new law, most commercial encryption technologies are no longer considered "state secrets," and the establishment of a system of commercial encryption standards that can be internationalized is proposed. Of course, the Ministry of Commerce will still publish a list of commercial encryption that will be subject to export and import restrictions.[251]

C. 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)."[252]

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; and

7. Be accountable and be ready to provide demonstrate compliance.[253]

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 this release of guidelines lightly.

Indeed, in November 2019, the Canadian privacy commissioners found that data aggregator AIQ violated Canadian laws for its work in association with Cambridge Analytica. Most notably, the commissioner enumerated extra-territorial violations of the rights of U.S. citizens by AIQ. [254]

---

[248] *See* GT/T 35273-2017.

[249] Xiaoyan Zhang and Vincent J. Barbuto, *A Look at China's New Cybersecurity Guidance*, Law360 (June 18, 2019), https://www.law360.com/articles/1170321/a-look-at-china-s-new-cybersecurity-guidance.

[250] Lavender Au, *China Redoubling Crackdown on Apps over Privacy Violations*, Technode (Nov. 5, 2019), https://technode.com/2019/11/05/china-redoubling-crackdown-on-apps-over-privacy-violations/.

[251] Karen Ip et al., *China Cybersecurity and Data Protection: China publishes first law on encryption*, Lexology (Nov. 12, 2019), https://www.lexology.com/library/detail.aspx?g=53282dfc-c7f6-4cef-8de6-8f180fed8b31.

[252] Office of the Privacy Comm'r of Can., *Guidelines for Obtaining Meaningful Consent* (May 2018), https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

[253] *Id.*

[254] Ryan Chiavett, *OPC, OIPC Find AIQ Violated Federal, Provincial Privacy Laws*, Int'l Ass'n Privacy Profs. (Nov. 27, 2019), https://iapp.org/news/a/opc-oipc-find-aiq-violated-federal-provincial-privacy-laws/.

The following Boies Schiller Flexner lawyers assisted in the preparation of this client alert: Mark Mao, James Lee, Albert Giang, Matthew Getz, Michael Jacobs, Matthew Chou, Yanni Lin, Diana Liu, Gabriel Schlabach, and Stephen Wilson.

At Boies Schiller Flexner, we pride ourselves on creating solutions to complex legal issues that take into account not only the legal aspects of the particular matter, but also the implications for our client's business as a whole. Our data privacy team helps clients stay ahead of the curve by designing preventative strategies, including assessment designed to minimize risks created by data collection and third-party contracts, and by helping our clients mitigate risk through sound policies, procedures, incident response plans, and insurance coverage.

When privacy and security incidents do occur, we have assembled a team with years of experience in government and private practice, with crisis management skills and a sophisticated understanding of forensics and computer science, to help clients respond efficiently and effectively to regulatory and media inquiries, investigations, and litigation.

Given our capabilities and litigation experience, Boies Schiller Flexner lawyers are uniquely positioned to help clients resolve matters at the cutting edge of privacy and information security. For further information, please contact the Boies Schiller Flexner lawyer with whom you usually work or any of the following leaders and members of the Firm's Cybersecurity and Privacy and Crisis Management and Government Relations practice groups:

Mark Mao, San Francisco, mmao@bsfllp.com, 1-415-293-6800
Quyen Ta, San Francisco, qta@bsfllp.com, 1-415-293-6800
Meredith Dearborn, San Francisco, mdearborn@bsfllp.com, 1-415-293-6800

Albert Giang, Los Angeles, agiang@bsfllp.com, 1-213-629-9040
Michael Roth, Los Angeles, mroth@bsfllp.com, 1-213-629-9040
Chris Caldwell, Los Angeles, ccaldwell@bsfllp.com, 1-213-629-9040
Michael Schafler, Los Angeles, mschafler@bsfllp.com, 1-213-629-9040
Luan Tran, Los Angeles, ltran@bsfllp.com, 1-213-629-9040

Damien Marshall, New York, dmarshall@bsfllp.com, 1-212-446-2300
Andrew Michaelson, New York, amichaelson@bsfllp.com, 1-212-446-2300
Peter Skinner, New York, pskinner@bsfllp.com, 1-212-446-2300
Lee Wolosky, New York, lwolosky@bsfllp.com, 1-212-446-2300
John Zach, New York, jzach@bsfllp.com, 1-212-446-2300

Karen Dunn, Washington DC, kdunn@bsfllp.com, 1-202-237-2727
Robert Cooper, Washington DC, rcooper@bsfllp.com, 1-202-237-2727
Stacey Grigsby, Washington DC, sgrigsby@bsfllp.com, 1-202-237-2727

James Lee, Miami, jlee@bsfllp.com, 1-305-539-8400
Andrew Brenner, Miami, abrenner@bsfllp.com, 1-305-539-8400

Stuart Singer, Fort Lauderdale, ssinger@bsfllp.com, 1-954-356-0011
Jesse Panuccio, Fort Lauderdale/Washington DC, jpanuccio@bsfllp.com, 1-954-356-0011

Matthew Getz, London, mgetz@bsfllp.com, +44 203 908 0800