Trends in Privacy and Data Security: 2018

by Jeffrey D. Neuburger and Jonathan P. Mollod, Proskauer Rose LLP, with Practical Law Data Privacy Advisor

Published on 15 Feb 2019 • USA (National/Federal)

An Article addressing key privacy and data security developments in 2018 and likely trends for 2019, including federal and state regulation and enforcement. This Article also discusses private litigation related to data breaches, biometrics, and other privacy-related causes, recent changes in state data breach notification and other privacy and data security laws, and developments in industry self-regulation and international data protection laws and enforcement.

Organizations must keep up with the dynamic legal obligations governing privacy and data security, understand how they apply, improve their cyber intelligence, and manage their compliance to minimize risks. This Article reviews important privacy and data security developments in 2018 and highlights key issues for the year ahead. Specifically, it addresses recent:

- Federal and state regulations and enforcement actions.
- Private litigation.
- Federal and state legislation.
- Industry self-regulation and standards.
- International developments likely to affect US companies.
- Trends likely to gain more prominence in 2019.

States routinely pass privacy and data security-related legislation. However, a comprehensive review of state laws in this area, including laws concerning specific industry sectors or areas of law, such as employment law, data disposal, and general consumer protection, are beyond this Article's scope. For some notable state law updates, see Federal and State Legislation.

For more on the current patchwork of federal and state laws regulating privacy and data security, see Practice Note, US Privacy and Data Security Law: Overview.

Federal Regulation and Enforcement

Several federal agencies issued guidance and took privacy and data security enforcement actions in 2018, including:

- The **Federal Trade Commission** (FTC) (see FTC).
- The **Department of Health and Human Services** (HHS) (see HHS).
- The **Securities and Exchange Commission** (see SEC).
- Various other agencies (see Other Federal Regulatory Developments).

FTC

The FTC is the primary federal agency regulating general consumer privacy and data security. It derives its authority to protect consumers from unfair or deceptive trade practices from **Section 5 of the Federal Trade Commission Act** (FTC Act) (15 U.S.C. § 45).

For more on the FTC's authority and standards, see Practice Notes, US Privacy and Data Security Law: Overview: FTC Act and FTC Data Security Standards and Enforcement.

FTC Guidance

In 2018, the FTC blogged to explain its existing guidance in several areas, including small business cybersecurity, using VPN apps, children's online safety for parents, and data retention limits under the Children's Online Privacy Protection Act (COPPA). The FTC also released notable guidance on:

- **Connected cars.** The FTC staff released its The Connected Cars Workshop: The Federal Trade Commission Staff Perspective, which includes best practices for addressing privacy and data security risks, such as information sharing, network design, risk assessment and mitigation, and industry self-regulation.

- **Children's privacy practices.** In August, the FTC approved modifications to the Entertainment Software Rating Board (ESRB)'s COPPA safe harbor program. The ESRB is a self-regulatory organization for the video game industry. For more details, see Legal Update, FTC Okays Video Game Industry's Changes to COPPA Safe Harbor Program.

- **Mobile device security.** The FTC issued a report making several recommendations to industry for expediting the mobile device security update process, including:
    - improving consumer education;
    - implementing minimum guaranteed security support periods; and
    - streamlining the update process.

    (FTC: FTC Recommends Steps to Improve Mobile Device Security Update Practices.)

- **Informational injuries.** The FTC Information Injury Workshop: BE and BCP Staff Perspective recounts key perspectives discussed on informational injuries consumers suffer from privacy and data security incidents, such as medical identity theft, doxing, and disclosure of private information.

FTC Enforcement Activity

The FTC's privacy and data security enforcement actions provide guidance in the absence of comprehensive federal privacy and data security regulations. For example, key 2018 actions demonstrate that companies should:

- **Ensure that privacy and data security practices match promises.** A mobile phone manufacturer agreed to settle charges that it allowed a third-party service provider to collect users' text message content and geolocation data without their consent, despite promises that it intended to keep that information private (*In re Blu Prods., Inc.*, 2018 WL 4350018 (F.T.C. Sept. 6, 2018)).

- **Disclose consumer data breaches according to applicable law.** Uber Technologies, Inc. agreed to an expanded settlement relating to a 2014 data breach of driver data after the FTC discovered that the company had failed to disclose a later breach to consumers (*In re Uber Techs., Inc.*, 2018 WL 5631072 (F.T.C. Oct. 25, 2018)).

- **Adequately disclose privacy controls.** Mobile payment service Venmo settled FTC charges alleging that the company misled consumers about its app's privacy controls, failing to adequately explain the multiple user steps required (*In re PayPal, Inc.*, 2018 WL 2716645 (F.T.C. May 23, 2018)).

- **Protect children by complying with COPPA obligations.** For example, The FTC reached settlements with:
  - an electronic toy manufacturer, which agreed to pay $650,000 to settle charges that its app violated COPPA when it collected children's personal information without providing notice to parents and obtaining their consent (for more details, see Legal Update, FTC Settles COPPA Suit with Toy Maker); and
  - a web-based talent search company, which agreed to pay $235,000 relating to its alleged collection of user' personal information during registration, including those under age 13, without first obtaining parental consent (*United States v. Prime Sites, Inc.*, 2018 WL 834606 (D. Nev. Feb. 12, 2018)).

- **Maintain reasonable procedures to ensure accuracy in consumer reports.** A property management company agreed to pay $3 million and settle charges that it purportedly failed to take reasonable steps to ensure the accuracy of tenant screening information in violation of the **Fair Credit Reporting Act** (FCRA) (Stipulated Order for Permanent Injunction & Civil Penalty Judgment, FTC v. RealPage, Inc., No. 18-02737 (N.D. Tex. Oct. 16, 2018)).

- **Make accurate representations about their cross-border data transfer practices.** The FTC settled charges with several companies alleging they misled consumers about their participation in cross-border data transfer programs, including the **EU-US Privacy Shield** and the Swiss-US Privacy Shield (*In re ReadyTech Corp.*, 2018 WL 5631091 (F.T.C. Oct. 17, 2018); *In re IDmission LLC*, 2018 WL 6192199 (F.T.C. Nov. 15, 2018); *In re mResource LLC*, 2018 WL 6078357 (F.T.C. Nov. 15, 2018); *In re SmartStart Emp. Screening*, Inc., 2018 WL 6078361 (F.T.C. Nov. 15, 2018); *In re VenPath, Inc.*, 2018 WL 6078359 (F.T.C. Nov. 15, 2018)).

Limitations on FTC Authority

In 2018, some companies facing enforcement actions continued to challenge the FTC's authority and interpretation of consumer harm with mixed results. For example:

- The US Court of Appeals for the Eleventh Circuit vacated an FTC order directing now-defunct LabMD, Inc. to overhaul and replace its data security program (*LabMD, Inc. v. FTC*, 894 F.3d 1221 (11th Cir. 2018)). The Eleventh Circuit found the cease and desist order unenforceable because it did not direct LabMD to cease committing a specific unfair act or practice within the meaning of Section 5(a) of the FTC Act (15 U.S.C. § 45(a)). Going forward, the FTC is likely to be more specific about not only a respondent's data security or privacy shortcomings, but also what procedures companies must enact as part of a comprehensive privacy or security program. For more details, see Legal Update, FTC Cannot Require Labmd to Overhaul Its Data Security Program: Eleventh Circuit.

- The US Court of Appeals for the Ninth Circuit ruled that telecommunications carriers are only immune from FTC regulation of unfair and deceptive practices to the extent that they are engaging in common-carrier services, leaving internet and other information service providers subject to FTC enforcement (FTC v. AT&T Mobility LLC, 883 F.3d 848 (9th Cir. 2018)).

HHS

HHS's Office for Civil Rights (OCR) provides guidance and takes enforcement actions under the **Health Insurance Portability and Accountability Act of 1996** (HIPAA) and related regulations. For more information on HIPAA compliance and enforcement, see HIPAA and Health Information Privacy Compliance Toolkit.

HHS Guidance

In 2018, HHS issued regulations updating for inflation the amounts for HIPAA civil penalties and provided notable guidance on:

- HIPAA authorizations for using and disclosing **protected health information** (PHI) for research purposes (see Legal Update, HHS Addresses Authorizations of Uses and Disclosures of PHI for Research).
- Vulnerabilities in computer chips that may pose threats (see Legal Update, HHS Addresses Risks to PHI Involving Computer Processor Chips).
- Electronic device and media disposal (see Legal Update, HHS Addresses Disposing of Electronic Devices and Media under HIPAA).

HHS also issued, in late December, a four-volume set of voluntary cybersecurity practices. The publications are the result of a Cybersecurity Act of 2015 mandate and public-private partnership.

HHS Enforcement Activity

OCR settled several notable HIPAA enforcement actions in 2018, highlighting that companies should:

- **Implement appropriate measures for detecting network intrusions**. Health insurer Anthem, Inc. agreed to a record $16 million settlement relating to a series of cyberattacks, beginning with a phishing email to an employee and exposing some 79 million people's PHI (see Legal Update, Anthem's $16 Million HIPAA Settlement Is Largest in History).
- **Review media, filming, and public communications policies.** For example:
  - Allergy Associates of Hartford, P.C. agreed to a $125,000 settlement regarding impermissible PHI disclosures made during a doctor's media interview (see Legal Update, Health Provider Must Pay HHS $125,000 for Disclosing PHI to the Press); and
  - Boston Medical Center, Brigham and Women's Hospital, and Massachusetts General Hospital, together paid $999,999 to settle alleged HIPAA violations when they allowed on premises filming for a television series allegedly without sufficient patient authorization (see Legal Update, Television Crew's Filming of Hospital Patients Results in HIPAA Settlements Totaling Nearly $1 Million).
- **Conduct a thorough risk analysis and implement effective safeguards.** Specifically:
  - Fresenius Medical Care North America agreed to pay $3.5 million related to multiple data breaches related to alleged failures to adequately safeguard hardware and electronic media that contained PHI (see Legal Update, Five Breaches Result in $3.5 Million HIPAA Settlement);

- an administrative law judge required the University of Texas MD Anderson Cancer Center to pay $4.3 million in civil penalties following data breaches involving an unencrypted laptop and loss of unencrypted thumb drives (see Legal Update, Failure to Encrypt Leads to $4.3 Million in HIPAA Civil Money Penalties); and

- Pagosa Springs Medical Center in Colorado agreed to pay $111,400 to resolve a complaint alleging that the hospital failed to terminate a former employee's access to protected health information. Under a two-year corrective action plan, the hospital agreed, among other things, to update policies and procedures and train its workforce.

- **Follow proper data disposal procedures.** The court-appointed receiver for defunct Filefax, Inc. agreed to pay $100,000 to settle allegations that the company inappropriately disposed of PHI (see Legal Update, Receiver for Out-Of-Business HIPAA BA Reaches $100,000 Settlement with HHS).

SEC

The SEC issues guidance and takes cybersecurity-related enforcement actions against broker-dealers and publicly traded companies. Notable 2018 guidance and resources include:

- The Commission Statement and Guidance on Public Company Cybersecurity Disclosures, which builds on the SEC's 2011 guidance and emphasizes that cybersecurity disclosures should:
  - be specific and tailored, avoiding generic or boilerplate language; but
  - not be so specific to provide a roadmap for cyberattackers.

  (See Legal Update, SEC Announces New Cybersecurity Disclosure Guidance.)

- An investigative report in which the SEC cautioned public companies to:
  - adapt internal accounting controls to the current risk environment, including risks arising from cyber-related frauds, such as business email compromise attacks; and
  - assess and adjust their policies and procedures accordingly

  (See Legal Update, SEC Issues Investigative Report: Reassess Internal Accounting Controls in Light of Cyber Threats.)

On the enforcement side, in 2018, the SEC announced resolution of several cybersecurity-related actions, including:

- The entity formerly known as Yahoo! agreed to pay a $35 million to settle charges that it failed to disclose its 2014 mega-breach in quarterly and annual reports, misleading investors for two years (In re Altaba, Inc., 2018 WL 1919547 (S.E.C. Apr. 24, 2018); see Legal Update, SEC Settles with Yahoo for $35 Million over Failure to Disclose 2014 Data Breach).

- Broker-dealer and investment adviser Voya Financial Advisors, Inc. agreed to pay $1 million to settle charges that it violated the Safeguards Rule following an April 2016 cyberattack that compromised 5,600 customers' personal information (*In re Voya Fin. Advisors, Inc.*, 2018 WL 4627393 (S.E.C. Sept. 26, 2018); see Legal Update, Voya Pays $1 Million to Settle SEC's Charges under Red Flags and Safeguards Rules).

- The SEC charged two Equifax officials with insider trading before a 2017 announcement of the company's massive data breach (Criminal Information, SEC v. Bonthu, 2018 WL 3407781 (N.D. Ga. June 28, 2018); Complaint, SEC v. Ying, 2018 WL 1321979 (N.D. Ga. Mar. 14, 2018)). A Georgia district judge refused to dismiss a parallel federal criminal action, finding that the government sufficiently advanced insider trading allegations (*United States v. Ying*, 2018 WL 6322308 (N.D. Ga. Dec. 4, 2018)).

Other Federal Regulatory Developments

Other key federal agencies active in privacy and data security for 2018 include:

- The National Institute of Standards and Technology (NIST), which:
  - released version 1.1 of its Cybersecurity Framework, including updates on addressing authentication and identity, self-assessing cybersecurity risk, and managing supply chain risks (see Legal Update, NIST Releases New Version of Cybersecurity Framework);
  - published a guide on protecting electronic health records stored on smartphones and tablets (see Legal Update, NIST Releases Guidelines for Securing Electronic Health Information on Mobile Devices);
  - released and sought comments on various cybersecurity technical and risk management standards through its Computer Security Resource Center; and
  - launched the NIST Privacy Framework initiative to develop a voluntary method for organizations to more effectively manage privacy risks.

- The **Commodity Futures Trading Commission** (CFTC), which announced:
  - its first cybersecurity-related settlement, with a registered futures commission merchant agreeing to pay $100,000 relating to its alleged failure to supervise its information technology provider, necessarily highlighting the importance of vendor management and monitoring cybersecurity incidents in the industry (see Legal Update, CFTC Settles Cybersecurity Action for Failure to Supervise IT Provider); and
  - a proposed rule to provide an exception to the annual privacy notice requirements under the Gramm-Leach-Bliley Act and align with similar requirements from other agencies (see Legal Update, CFTC Proposes Exception to GLBA Annual Privacy Notice Requirement).

- The **Consumer Financial Protection Bureau** (CFPB), which issued:

- a final rule exempting some financial institutions from providing annual customer privacy notices under the Gramm-Leach-Bliley Act (GLBA) (see Legal Update, CFPB Final Rule Codifies Exemption to GLBA Annual Privacy Notice Requirement); and

- an interim final rule updating the agency's model FCRA summary of rights forms, including notification of consumers' national security freeze right (see Legal Update, CFPB Publishes Interim Final Rule Amending the FCRA Summary of Rights Model Forms).

- The **Federal Communications Commission** (FCC), which:

  - sought further comment on what constitutes an automatic telephone dialing system (ATDS) under the Telephone Consumer Protection Act of 1991 (TCPA), following conflicting federal appeals court decisions (*Consumer & Governmental Affairs Bureau Seeks Comment on Interpretation of the TCPA in Light of the D.C. Cir.'s ACA Int'l Decision*, 2018 WL 2253215 (F.C.C. May 14, 2018); see TCPA Cases); and

  - ruled that SMS and MMS services are "information services," not "telecommunications services" under the Communications Act, clarifying that wireless providers may continue their efforts to stop unwanted text messaging using robotext-blocking and other anti-spam measures (*In re Petitions for Declaratory Ruling on Regulatory Status of Wireless Messaging Service*, 2018 WL 6590245 (F.C.C. December 13, 2018)).

- The **Food and Drug Administration** (FDA), which:

  - released draft guidance on cybersecurity considerations for designing and developing medical devices and preparing them for market (see FDA: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices); and

  - announced increased cooperation with the **Department of Homeland Security** (DHS) on medical device cybersecurity, including greater information sharing about device vulnerabilities and threats (see FDA: FDA and DHS increase coordination of responses to medical device cybersecurity threats under new partnership; a part of the two agencies' broader effort to protect patient safety).

- The Department of Commerce, which:

  - with DHS, offered joint guidance on reducing threats from botnets and distributed attacks (see US Department of Commerce: Report to the President on Enhancing Resilience Against Botnets);

  - explained the measures the US has taken to implement and enforce the EU-US and Swiss-US Privacy Shield Frameworks (see US Department of Commerce: U.S. Implementation, Oversight and Enforcement of the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks); and

  - through its National Telecommunications and Information Administration (NTIA), solicited comments on approaches to consumer data privacy that support innovation (see NTIA: NTIA Releases Comments on a Proposed Approach to Protecting Consumer Privacy).

- The White House, which unveiled the National Cyber Strategy, listing multiple goals to protect the nation's critical infrastructure and digital commerce in the face of new threats (see White House: President Trump Unveils America's First Cybersecurity Strategy in 15 Years).

State Regulation and Enforcement

Key 2018 developments at the state level include:

- Cybersecurity regulations for state-regulated financial services organizations. Most notably, the New York State Department of Financial Services (NYDFS):
    - continued implementing its nation-leading cybersecurity regulations for banks and other financial institutions, requiring the first round of annual compliance certifications in February 2018 (23 NYCRR 500.0 through 500.23); and
    - expanded the scope of its regulations to include credit reporting agencies (23 NYCRR 201.00 through 201.09).

  For details on NYDFS cybersecurity obligations, see Practice Note, The NYDFS Cybersecurity Regulations.
- A growing number of single-state enforcement actions (see Single-State Enforcement Actions).
- Several high-profile multi-state and joint FTC actions (see Multi-State Enforcement Actions).

Single-State Enforcement Actions

State attorneys general and other agencies pursued privacy and data security enforcement actions in 2018, including those in:

- California, where the state's Department of Public Health announced penalties against multiple hospitals and medical providers relating to inadvertent PHI disclosures (see California Department of Public Health: Breach of Confidential Patient Medical Information: Penalties Issued).
- Massachusetts, which settled with:
    - UMass Memorial Medical Group, Inc. for $230,000 and an agreement to improve security practices regarding employee data access following two data breaches (see Massachusetts Office of the AG: UMass Memorial Health Care Entities to Pay $230,000 to Resolve AG's Lawsuit Over Data Breaches); and
    - Yapstone Holdings, Inc. for $155,000 and an agreement to update security policies following the payment processor's alleged website error that exposed residents' personal information (see Massachusetts Office of the AG: Payment Processor to Pay $155,000 Over Data Breach Affecting Thousands of Massachusetts Residents).
- New Jersey, which settled with:

- ATA Consulting LLC, a defunct medical services vendor, for $200,000 following a 2016 server misconfiguration that exposed PHI online and Virtua Medical Group, P.A., which agreed to pay almost $418,000 and enhance its data security practices, relating to the same data breach (see New Jersey Office of the AG: Defunct Georgia Vendor Responsible for Exposing Virtua Medical Group Patient Files Online Agrees to $200,000 Settlement and Virtua Medical Group Agrees to Pay Nearly $418,000, Tighten Data Security to Settle Allegations of Privacy Lapses Concerning Medical Treatment Files of Patients);

- Unixiz, Inc., which agreed to shut down its teen social website, pay a $98,000 fine, and comply with applicable laws on its other sites to resolve allegations related to COPPA violations and a 2016 data breach (see New Jersey Office of the AG: Operator of Teen Social Website Breached by Hacker Agrees to Close Site and Reform Practices to Settle Allegations it Violated Children's Online Privacy Protection Act);

- Meitu, Inc., which agreed to pay $100,000 and alter its practices to settle charges that the Chinese software company violated COPPA (see New Jersey Office of the AG: NJ Division of Consumer Affairs Announces $100,000 Settlement with App Developer Resolving Investigation Into Alleged Violations of Children's Online Privacy Law); and

- Lightyear Dealer Technologies, which agreed to pay $80,000 and institute comprehensive data security changes after a security researcher accessed an unencrypted database with a dealership's customers' personal information (see New Jersey Office of the AG: Software Developer Agrees to Implement Security Protocols to Settle Investigation into Data Breach Exposing Personal Information of Auto Dealership Customers Nationwide, Including Thousands in NJ).

- New York, which settled with:

  - Oath, Inc. (formerly AOL) for $4.95 million, the largest penalty in a COPPA enforcement action, regarding billions of ad auctions on websites directed to children under age 13 (see Legal Update, NY Attorney General Announces $4.95 Million COPPA Penalty);

  - Aetna Inc. for $1.15 million following claims that the health insurer revealed the HIV status of thousands of members. Other states reached separate settlements relating to the incident and the health insurer paid $17 million to settle a class action lawsuit. (See NY Office of the AG: A.G. Schneiderman Announces Settlement With Aetna Over Privacy Breach Of New York Members' HIV Status*; Beckett v. Aetna, Inc.*, 2018 WL 2089301 (E.D. Pa. Jan. 16, 2018).);

  - EmblemHealth for $575,000 following an error that included policyholders' Social Security numbers on mailing labels, allegedly in violation of HIPAA and state law (see NY Office of the AG, A.G. Schneiderman Announces $575,000 Settlement With EmblemHealth After Data Breach Exposed Over 80,000 Social Security Numbers); and

  - Equifax Consumer Services LLC, Priceline.com LLC, and other companies for operating mobile apps that allegedly failed to address known cyber vulnerabilities (see Legal Update, New York AG Settles Charges against Five Companies for Mobile Application Security Failures).

Multi-State Enforcement Actions

The trend of multi-state and federal-state cooperation in privacy enforcement continued in 2018. For example:

- Uber Technologies, Inc. settled with 50 states and the District of Columbia for $148 million relating to the company's failure to promptly report a 2016 data breach affecting users and drivers. The settlement required Uber to strengthen its corporate governance and security practices and comply with data breach notification laws. (See Legal Update, Uber Agrees to $148 Million Data Breach Settlement with State Attorneys General.)

- Equifax, Inc. agreed to a consent order with the NYDFS and seven other state bank regulators to take corrective actions in the wake of its massive 2017 data breach (see NYDFS: DFS Takes Additional Action to Hold Equifax Accountable for Massive 2017 Data Breach).

Private Litigation

Standing remained a key issue for privacy-related litigation in 2018, especially in actions alleging procedural violations of the FCRA and the Fair and Accurate Credit Transactions Act of 2003 (FACTA) (for example, see *Bassett v. ABM Parking Servs., Inc.*, 883 F. 3d 776 (9th Cir. 2018) (denying standing for bare procedural FACTA violation); *Auer v. Trans Union, LLC*, 902 F. 3d 873 (8th Cir. 2018) (denying standard for alleged FCRA procedural violation); *Muransky v. Godiva Chocolatier, Inc.*, 905 F.3d 1200 (11th Cir. 2018) (conferring standing where printing full credit card numbers exposed plaintiffs to increased risk)).

Other highlights for 2018 include:

- US Supreme Court rulings on privacy-related issues (see Privacy-Related Supreme Court Actions).

- Data breach-related actions (see Data Breach Litigation).

- Biometrics actions (see Biometrics Privacy Litigation).

- TCPA actions (see TCPA Cases).

- Other privacy-related actions (see Other Notable Cases).

Privacy-Related Supreme Court Actions

In 2018, the Supreme Court took noteworthy privacy-related actions. For example, the Supreme Court:

- Issued an opinion in *Carpenter v. United States*, in which it:
    - declined to extend the third-party doctrine to the government's collection of cell-site location information; and
    - deemed the collection a Fourth Amendment search.

  (138 S. Ct. 2206 (2018).)

- Declined to review a decision that invalidated the FCC's 2006 Solicited Fax Rule, which required opt-out notices on solicited fax advertisements (*Bais Yaakov of Spring Valley v. FCC*, 852 F.3d 1078 (D.C. Cir. 2017), cert. denied sub nom. *Bais Yaakov of Spring Valley v. FCC*, 138 S. Ct. 1043 (2018); see Legal Update, Updated: Supreme Court Declines to Review D.C. Circuit's Decision Overturning FCC's Solicited Fax Rule).

- Heard arguments regarding an $8.5 million *cy pres* settlement in a privacy-related class action against Google. The Supreme Court requested supplemental briefing on Article III standing, signaling a potential impact on future privacy litigation (2018 WL 5722840 (U.S. Oct. 31, 2018); 139 S. Ct. 475 (2018) (Supreme Court ordered supplemental briefing)).

Data Breach Litigation

Standing also remained a key issue in 2018 for data breach actions in federal courts. Circuit courts ruled differently, considering factors, such as:

- The type and sophistication of the data intrusion.
- The sensitivity of the stolen personal information.
- The amount of time elapsed without evidence of data misuse.
- Whether litigants incurred costs to mitigate fraud or identity theft risks.

For example:

- The Ninth Circuit held that plaintiffs sufficiently alleged an injury based on a substantial fraud or identity theft risk, because:
    - another set of plaintiffs that already showed they had standing had faced incidents of identity theft; and
    - the risk of future harm they faced was fairly traceable to the challenged conduct.

    (*In re Zappos.com, Inc.,* 888 F.3d 1020 (9th Cir. 2018).)

- The US Circuit Court of Appeals for the Fourth Circuit held that plaintiffs had suffered a non-speculative injury-in-fact where a data breach:
    - allowed fraudsters to open or attempt to open credit card accounts using plaintiffs' personal information;
    - reduced individuals' credit scores; and
    - required individuals to spend time and resources to repair their credit.

(*Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018).)

- The US Court of Appeals for the Seventh Circuit held that consumers had standing based on payments for credit monitoring and unavailability of funds from affected accounts (*Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826 (7th Cir. 2018); but see *Cmty. Bank of Trenton v. Schnuck Mkts., Inc.*, 887 F.3d 803 (7th Cir. 2018) (applicable state tort law did not offer a remedy to banks against a retail merchant who suffered a data breach, beyond contractual remedies)).

With the continued uncertainty of litigation, 2018 also saw notable data breach-related settlement activities, including those regarding:

- Vizio, Inc., which agreed in a proposed settlement to pay $17 million and improve its privacy practices to resolve litigation surrounding smart TVs that allegedly tracked users' viewing data without consent (*In re Vizio, Inc. Consumer Privacy Litig.*, No. 16-ML-02693 (C.D. Cal. Oct. 4, 2018)).

- Yahoo! Inc., which agreed in a proposed settlement to pay $50 million and provide two years of credit monitoring services following multiple large-scale cyberattacks (*In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752 (N.D. Cal. Oct. 22, 2018)). However, in early 2019, the court rejected this initial settlement, holding the settlement's disclosures inadequate and expressing concerns regarding legal fees (2019 WL 387322 (N.D. Cal. Jan. 30, 2019)).

- Lenovo Inc. and Superfish, Inc., which agreed to pay a total of $8.5 million to settle claims that some laptops had risky adware installed without consumers' knowledge (*In re Lenovo Adware Litig.*, 2018 WL 6099948 (N.D. Cal. Nov. 21, 2018)).

- Anthem, Inc., which saw its $115 million settlement with consumers finalized, following a 2015 data breach involving nearly 80 million records (*In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617 (N.D. Cal. Aug. 16, 2018)).

For more details on data breach litigation issues, including applicable law and recovery theories, the roles of harm and standing, class certification, and settlement considerations, see Practice Note, Key Issues in Consumer Data Breach Litigation.

Shareholder Actions

Shareholder actions against companies that suffer high-profile data breaches or announce data security vulnerabilities appeared increasingly common, with mixed results. For example:

- *Sgarlata v. PayPal Holdings Inc.*, 2018 WL 6592771 (N.D. Cal. Dec. 13, 2018) (dismissing shareholder suit alleging misleading statements relating to a newly acquired subsidiary's cyber incident).

- *In re Intel Corp. Securities Litig.*, 2018 WL 2412111 (N.D. Cal. May 29, 2018) (consolidating shareholder suit regarding vulnerabilities discovered in Intel processors).

- *In re Yahoo! Inc. Securities Litig.*, 2018 WL 4283377 (N.D. Cal. Sept. 7, 2018) (issuing final approval of $80 million settlement following large-scale cyberattacks).

- Complaint, *In re Facebook, Inc. Shareholder Derivative Privacy Litig.*, No. 18-1792 (N.D. Cal. July 2, 2018) (consolidating shareholder suit regarding Cambridge Analytica data leak).

For a discussion on shareholder derivative and securities fraud class actions brought after data breaches and the obstacles plaintiffs face, see Article, Shareholder Derivative and Securities Fraud Litigation After Data Breaches.

Biometrics Privacy Litigation

Litigation under Illinois's Biometric Information Privacy Act (BIPA) against employers, businesses, social media sites, and other mobile platforms remained robust in 2018 (740 ILCS 14/1). In January 2019, the Illinois Supreme Court issued an opinion in *Rosenbach v. Six Flags Entertainment Corp.*, holding that BIPA does not require individuals to suffer actual injury beyond a statutory violation to sustain a private action (2019 WL 323902 (Ill. Jan. 25, 2019)). This ruling is undoubtedly likely to:

- Increase the breadth and number of suits filed.
- Change the risk analysis and settlement approach for targeted organizations.

Organizations with connections to Illinois should carefully consider their privacy practices related to collecting and using biometrics information.

For more details on BIPA and emerging issues in biometrics law and litigation, see Practice Note, Biometrics Litigation: An Evolving Landscape.

Increasingly popular genetic testing companies have also come under scrutiny for sharing anonymized data with researchers and have faced other potential compliance issues with various state genetic privacy laws. The Ninth Circuit denied class action status for a privacy suit alleging that a testing company disclosed customer DNA results without informed written consent purportedly in violation of the Alaska Genetic Privacy Act (Alaska Stat. Ann. § 18.13.010(a)(1); *Cole v. Gene by Gene, Ltd*, 735 Fed. Appx. 368 (9th Cir. 2018)).

TCPA Cases

The TCPA regulates how businesses can:

- Use ATDSs or artificial prerecorded voice technology to contact consumers by telephone.
- Send fax advertisements.

For details on the TCPA and compliance obligations, see Practice Note, TCPA Litigation: Key Issues and Considerations.

TCPA litigation continued apace in 2018. Some ongoing issues with notable developments include:

- **The definition of an autodialer.** Federal appeals courts remain split regarding what is an ATDS, including whether a device qualifies if it only stores numbers for autodialing or if it must generate random or sequential numbers (*Marks v.*

Crunch San Diego, LLC, 904 F.3d 1041 (9th Cir. 2018) (stating that an ATDS is "not limited to devices with the capacity to call numbers produced by a 'random or sequential number generator,' but also includes devices with the capacity to dial stored numbers automatically"); compare *King v. Time Warner Cable Inc.*, 894 F.3d 473 (2d Cir. 2018) (holding that "capacity" in the TCPA's ATDS definition should be interpreted to refer to a device's current functions, absent modifications); *Dominguez v. Yahoo, Inc.*, 894 F.3d 116 (3d Cir. 2018) (holding that TCPA plaintiff must demonstrate that defendant's equipment "had the present capacity to function as an autodialer")). In early 2019, the *Marks* defendants petitioned the Supreme Court to address the ATDS issue (Petition for Writ of Certiorari, *Crunch San Diego, LLC v. Marks*, No. 18-995, 2019 WL 411371 (U.S. Jan. 28, 2019).).

- **The FCC's rulemaking authority.** In *ACA International v. FCC*, the US Court of Appeals for the D.C. Circuit issued a ruling that partly narrowed and partly upheld a 2015 FCC order, which had sought to clarify how the TCPA applied to robocalls and texts. The D.C. Circuit:
  - upheld the FCC's approach to revoking consent, allowing a party to express a desire to receive no further messages from the caller using any reasonable means;
  - sustained the scope of the agency's exemption for time-sensitive healthcare calls;
  - struck down the FCC's "unreasonably expansive interpretation" of what constitutes an ATDS, saying it sweeps in devices like conventional smartphones; and
  - vacated the FCC's prior approach to handling calls to recycled numbers, finding the one-call safe harbor was arbitrary and capricious.

  Notably, on the latter two issues, the D.C. Circuit did not replace the FCC's interpretation with its own, leaving courts to consider this issue anew and the FCC to initiate new proceedings to resolve the issues. (885 F.3d 687 (D.C. Cir. 2018); see Legal Update, DC Court of Appeals Partially Upholds and Partially Sets Aside FCC's 2015 Declaratory Ruling and Order on TCPA and Other Federal Regulatory Developments).

- **The ability to revoke consent.** Declining to adopt precedent from the US Circuit Court of Appeals for the Second Circuit, an Ohio district court ruled that a consumer can unilaterally revoke consent to receive robocalls even when consent was formed as part of a bargained-for exchange. (*Rodriguez v. Premier Bankcard, LLC*, 2018 WL 4184742 (N.D. Ohio Aug. 21, 2018); see Legal Update, District Court Disagrees with Second Circuit and Holds That Consent to Receive Robocalls in Bargained-For Agreements May Be Unilaterally Revoked under the TCPA).

Other Notable Cases

Other notable privacy and data security-related decisions and settlements in 2018 included those addressing:

- **Computer Fraud and Abuse Act (CFAA) damages.** The Second Circuit affirmed the CFAA conviction of an Italian citizen as the perpetrator of various cyberattacks and a click-fraud scheme, rejecting the constitutional challenge to the statute and the defendant's challenge to the admission of screenshots from the Internet Archive, known colloquially as the "Wayback Machine" (*United States v. Gasperini*, 894 F.3d 482 (2d Cir. 2018)).

- **Cyberinsurance coverage for spoofed emails.** Litigation has continued regarding whether various commercial insurance policies cover email "spoofing" as a data security incident. Spoofing generally refers to the practice of disguising an email sender's real identity. For example:
    - the Second Circuit found that a computer fraud provision covered an incident where the spoofed email fraudulently directed employees to transfer funds (Medidata Sols. Inc. v. Fed. Ins. Co., 729 Fed. Appx. 117 (2d Cir. 2018)); and
    - the US Circuit Court of Appeals for the Sixth Circuit similarly found that a policy covered loss from a spoofing incident as "computer fraud" (*Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 895 F.3d 455 (6th Cir. 2018)).

- **Data collection by smart meters.** The Seventh Circuit held that a public utility's collection of smart meter data at 15-minute intervals constitutes a "reasonable" search, given:
    - the government's interest in improving energy efficiency; and
    - the search is unrelated to law enforcement and minimally intrusive.

  (*Naperville Smart Meter Awareness v. City of Naperville*, 900 F. 3d 521 (7th Cir. 2018).)

- **Data security obligations and employee privacy.** The Pennsylvania Supreme Court ruled that a medical center had a legal duty to reasonably safeguard its employees' sensitive personal information stored on an internet-accessible computer system (*Dittman v. UPMC*, 196 A.3d 1036 (Pa. 2018)).

- **Privacy and online browsing.** Users that consented to Facebook's terms and policies, which included disclosures about tracking online browsing activity, do not have a viable claim against the company for tracking their visits to public healthcare-related sites, data which the court held also does not fall under HIPAA (*Smith v. Facebook, Inc.*, 745 Fed. Appx. 8 (9th Cir. 2018)).

Federal and State Legislation

Despite the lack of a viable comprehensive federal privacy bill, Congress did pass several privacy and data security-related laws in 2018, including:

- The Clarifying Lawful Overseas Use of Data (CLOUD) Act, which:
    - amends portions of the **Stored Communications Act** (SCA) to better reflect current service provider data storage practices;
    - requires US service providers that store data outside the US to respond to lawful requests for data under the SCA regardless of where it is stored;
    - creates a process for the US to enter into international agreements to support data requests; and

- provides service providers with a procedure to challenge certain requests, such as those that conflict with other countries' laws.

(Pub. L. 115-141; 18 U.S.C. §§ 2701 through 2713.)

- The NIST Small Business Cybersecurity Act, which requires NIST to consider small businesses when it develops voluntary, industry-led guidelines and procedures to reduce cyber risks to critical infrastructure (Pub. L. No. 115-236).

- The Cybersecurity and Infrastructure Security Agency Act of 2018, which established the Cybersecurity and Infrastructure Security Agency in DHS to lead the national effort against cybersecurity threats to critical infrastructure (Pub. L. No. 115-278).

State law proliferation increased given the lack of comprehensive federal privacy or data security legislation. Key activities included:

- California's establishing comprehensive consumer data protection rights (see California Consumer Privacy Act of 2018).

- The remaining holdouts enacting data breach notification laws (see State Data Breach Notification Laws).

- Several state-specific data security laws (see State Cybersecurity Laws).

- Other various but notable privacy-related statutes (see Other State Privacy Laws).

California Consumer Privacy Act of 2018

California passed and later clarified the California Consumer Privacy Act of 2018 (CCPA), a comprehensive data protection law that grants consumers rights to:

- Notice, before or at the point of collection, about what personal information categories the business collects and its intended use purposes. Businesses may not collect additional personal information categories or use collected personal information for unrelated purposes without providing the required notice.

- Opt-out of the sale of their personal information if the consumer is 16 years old or older.

- For minors, affirmatively opt-in to the sale of their personal information, by providing direct authorization if they are between 13 and 16 years old, or with parental or guardian consent if they are under 13.

- Not face discrimination for asserting their CCPA rights, although businesses may impose consumer payments and certain price or service differences directly related to the value of the consumer's data that do not result in unjust, unreasonable, coercive, or usurious financial incentive practices.

The CCPA broadly defines personal information and imposes specific obligations on covered businesses. The California Attorney General holds rulemaking authority and intends to enforce the CCPA and any related regulations beginning six months after publishing final regulations or July 1, 2020, whichever is earlier.

The CCPA permits a private right of action for unauthorized access, theft, or disclosure of personal information in certain situations, with some procedural restrictions. For more details on the CCPA, covered businesses, their obligations, and enforcement mechanisms, see Practice Note, Understanding the California Consumer Privacy Act (CCPA).

State Data Breach Notification Laws

The year brought data breach notification obligations to all 50 states when the last two holdouts, South Dakota and Alabama, enacted laws (see Legal Updates, Alabama Enacts Data Breach Notification Law and South Dakota Enacts Data Breach Notification Law).

Several other states amended their laws, generally extending them in one or more ways. For example:

- Arizona amended its law by:
    - expanding the definition of personal information; and
    - updating notification timing requirements.

    (A.R.S. § 18-545; see Legal Update, Arizona and Iowa Amend Data Breach Notification Laws.)
- Colorado enacted a data security law and amended its data disposal and breach notification law to:
    - expand the definition of personal information requiring notification to include biometric data, health insurance identification number, and medical information; and
    - require notice to the state attorney general if a breach affects more than 500 Colorado residents.

    (Colo. Rev. Stat. Ann. §§ 6-1-713, 6-1-713.5, and 6-1-716; see Legal Update, Colorado Amends Data Disposal and Breach Notification Laws, Enacts Data Security Law.)
- Connecticut amended its law to:
    - refine the definition of protected personal information to separate credit or debit cards from other financial account numbers; and
    - extend the minimum length of time that entities must offer free identify theft prevention services from 12 to 24 months.

    (Conn. Gen. Stat. Ann. § 36a-701b.)
- Louisiana amended its law to:

- expand the definition of personal information to include passport numbers and biometric data;
- require covered entities to implement reasonable security procedures;
- require notification in the most expedient time possible but no later than 60 days from the discovery of the breach, consistent with law enforcement needs; and
- allow for a harm threshold if there is no reasonable likelihood of harm to state residents from the breach, but requiring the covered entity to keep a copy of the supporting documentation for five years from the date of discovery of the breach.

(La. R.S. 51:3073 and 51:3074; see Legal Update, Louisiana Amends Data Breach Notification Law.)

- Oregon amended its data breach notification law to:
  - expand the definition of personal information to include information that permits access to a consumer's financial account;
  - update notice requirements to consumers and from third parties that maintain or possess personal data on behalf of organizations; and
  - prohibit entities that offer free credit monitoring services to consumers from requiring consumers to provide a credit card number or pay for other services.

(Or. Rev. Stat. §§ 646A.602 to 646A.622; see Legal Update, Oregon Amends Data Breach and Security Law.)

- Virginia amended its law to require income tax return preparers to notify the Department of Taxation without unreasonable delay if Virginia individuals' unencrypted tax return information is compromised, if the preparer reasonably believes that the incident has caused or is likely to cause identity theft (Va. Code Ann. §58.1-341.2).

For more details on state data breach notification laws, see State Q&A Tool, Data Breach Notification Laws.

State Cybersecurity Laws

Several states adopted other cybersecurity-related laws, including:

- California, which passed:
  - an IoT data security law that requires connected device manufacturers to equip their devices with reasonable security features (Cal. Civil Code §1798.91.04; see Practice Note, California Privacy and Data Security Law: Overview: Connected Devices); and

    - requirements for consumer credit reporting agencies or third parties that maintain personal information on their behalf to install security updates for known network vulnerabilities within 90 days after becoming aware of available patches (Cal. Civ. Code §1798.81.6).

- Ohio, which adopted legislation that provides a safe harbor from certain data breach-related tort claims to covered entities that implement a specified cybersecurity program (Ohio R.C. 1354.03; see Legal Update, Ohio Law Grants Safe Harbor Protection for Voluntary Adoption of Cybersecurity Program).

- Nebraska, which passed a law that:

    - prohibits a consumer reporting agency from charging a fee for placing or lifting a security freeze; and

    - requires covered entities to maintain reasonable security procedures to protect residents' personal information and contractually require their service providers to do the same.

    (Neb. Rev. St. §§ 8-2602 to 8-2609.01 and §§ 87-801 to 87-808.)

- South Carolina, which passed the Insurance Data Security Act as the first state to follow model data security legislation from the National Association of Insurance Commissioners (S.C. Code Ann. § 38-99-10 to 38-99-100; see Legal Update, South Carolina Enacts Insurance Data Security Law).

- Vermont, which passed a law to regulate data brokers, generally including businesses that aggregate and sell personal information of consumers with which they do not have a direct relationship. The Vermont Attorney General's Office also published guidance regarding related regulations. (See Legal Update, Vermont Enacts First Data Broker Law; see also Office of the Vermont AG: Attorney General's Office Issues Guidance on Data Broker Regulations.)

Other State Privacy Laws

California also enacted several other privacy-related laws covering:

- Chatbots, making it unlawful to use a bot to communicate online with the intent to mislead about its artificial identity and incentivize a commercial transaction or influence a vote (Cal. Bus. & Prof. Code §17940 through §17941).

- Lodging and passenger records, limiting how innkeepers and bus companies can disclose guest records and passenger manifests without a court order (Cal. Civ. Code §53.5).

Other notable new state laws include:

- Iowa, which enacted a student privacy law similar to previous states' laws that:

    - prohibits K-12 website and online service operators from selling or renting student data or using it for targeted advertising or profiling students other than for educational purposes;

- requires providers to implement industry standard security practices; and
- sets data deletion requirements.

(Iowa Code Ann. § 279.71.)

- New Hampshire, where voters approved a state constitutional amendment that codified a right to privacy and gives New Hampshire residents a mechanism to challenge the state government's collection of personal information.
- Oklahoma, which now considers tracking individuals using a GPS device without consent to be stalking (Okla. Stat. Ann. tit. 21, § 1173).

Industry Self-Regulation and Guidance

Industry self-regulation and guidance from independent organization remained important components of the privacy and security landscape in 2018 for various sectors.

Artificial Intelligence

In 2018, several organizations released proposed guidelines and suggestions for potential regulation regarding artificial intelligence (AI) technology, including:

- The International Conference of Data Protection & Privacy Commissioners (ICDPPC), which recognized the benefits and privacy risks of AI for users and society and proposed a set of principles to achieve fairness, accountability, transparency, and responsible development (see ICDPPC: Declaration on Ethics and Data Protection in Artificial Intelligence).
- The AI Now Institute at New York University, which released a report advocating for regulation of facial recognition and related AI technologies (see AI Now Institute: AI Now Report 2018).
- The European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG), which released draft ethics guidelines, outlining a framework for trustworthy AI (see AI HLEG: Draft Ethics guidelines for trustworthy AI).

Cybersecurity

The technology industry and self-regulatory organizations continued to address cybersecurity and data protection issues in 2018, despite increasing federal and state legislation, for example:

- Apple and Google changed their developer guidelines to clarify privacy obligations, restrict data sharing, and limit uses of sensitive personal information, including geolocation data (see Apple: Updated Guidelines Now Available and Google: Project Strobe: Protecting your data, improving our third-party APIs, and sunsetting consumer Google+).

- The American Bar Association (ABA) released Formal Opinion 483, which clarifies data breach notification obligations for lawyers under the Model Rules of Professional Conduct (see Legal Update, New ABA Guidance Requires Data Breach Notifications to Current Clients).

- The International Council for Commercial Arbitration (ICCA), the International Institute for Conflict Prevention and Resolution (CPR), and the New York City Bar Association established a working group on arbitration cybersecurity and released a draft protocol (see Legal Update, Draft Cybersecurity Protocol Released for Consultation).

IoT

Several industry groups released guidance in 2018 to help improve IoT privacy and data security practices, including:

- The Online Trust Alliance (OTA), which updated its IoT security framework for software developers, purchasers, and retailers to use during product development, (see OTA: IoT Trust Framework v2.5).

- CTIA – The Wireless Association, which created a new certification and testing program for managed IoT devices (see CTIA: CTIA Cybersecurity Certification Test Plan for IoT Devices.)

For more details on emerging IoT issues and laws, see Practice Note, The Internet of Things: Key Legal Issues.

Online and Mobile Advertising

The Digital Advertising Alliance (DAA) and its enforcement partner, the Council of Better Business Bureaus, reported several inquiries under its accountability program. For example, it took actions against:

- Kiip, Inc., which agreed to a settlement requiring it to enhance its notice and consent procedures regarding collection of geolocation data for targeted advertising and update its privacy policy to reflect cross-device data collection.

- VRTCAL Markets, Inc., which agreed to a settlement requiring it to update its partner contracts to provide enhanced notice regarding data collection for targeted advertising.

- Vdopia, Inc., which agreed to update its partner agreements and provide enhanced transparency and control to users when serving targeted video ads through mobile apps, following a 2017 compliance warning (see DAA: DAA Accountability Partners Click Play on Mobile Video Ad Transparency; see also ASRC: Compliance Warning: Interest-Based Video Ads Require Transparency, Choice).

- Lifttopia Inc., which agreed to offer enhanced notice of third-party data collection for targeted advertising (see Legal Update, Website Agrees to Update Privacy Practices following BBB Accountability Program Investigation).

For more information on mobile app privacy, see Practice Note, Mobile App Privacy: The Hidden Risks and Mobile App Privacy Compliance Checklist.

Payment Card Industry

The Payment Card Industry (PCI) Security Standards Council (SSC) continued its efforts to improve payment card data security. Specifically, the PCI SSC released an evaluation tool and related resources to help small merchants assess their data security practices (see PCI: PCI SSC Launches Payment Security Tool to Help Small Merchants).

For more information on the PCI Data Security Standard (PCI DSS), see Practice Note, PCI DSS Compliance.

International Developments

In 2018, international agreements, cross-border data transfer frameworks, new regulations outside the US, especially in Europe, and related enforcement actions continued to affect US companies with international reach.

Europe

Data protection obligations for companies that collect and use information from individuals in the EU are undergoing a significant transition with the General Data Protection Regulation (GDPR), which took effect on May 25, 2018. This trend is likely to continue in 2019 as the EU and world continue to work on GDPR compliance and look for further guidance about:

- The GDPR's nuances and scope.
- European regulators' enforcement priorities, as initially seen in early 2019 actions.

The EU is also working to replace its current Privacy and Electronic Communications Directive, known as the E-Privacy Directive, with an updated regulation, which like the GDPR, would apply directly to all member states.

Important European developments in 2018 include those related to:

- The GDPR (see GDPR).
- Several enforcement actions filed (see Notable EU Enforcement Actions).
- The EU-US Privacy Shield cross-border data transfer framework (see EU-US Privacy Shield).

GDPR

The GDPR affects companies operating in the EU, but also applies extraterritorially to organizations that process personal data when:

- Offering goods or services to data subjects in the EU, regardless of whether payment is required (Article 3(2)(a), GDPR).

- Monitoring data subjects' behavior, such as interacting with websites and other online services, when it takes place in the EU (Article 3(2)(b), GDPR).

For more information on the GDPR, its general requirements, and its extraterritorial reach, see Practice Note, Overview of EU General Data Protection Regulation.

One month before the GDPR's effective date, the European Parliament published a corrigendum with a number of minor changes to the text. One notable amendment arguably broadened when a covered entity must appoint a data protection officer (see Legal Update, European Parliament LIBE Committee Publishes GDPR Corrigendum).

The EU's European Data Protection Board (EDPB), which replaced the Article 29 Working Party and includes member states' data protection authorities (DPAs), provided guidance on key GDPR concepts and compliance obligations, including:

- The GDPR's territorial scope. The guidance also discusses the designation of an EU representative for foreign data controllers or processors subject to the GDPR (see EDPB: Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation (Nov. 16, 2018)).

- Which processing operations require a data protection impact assessment (DPIA), based on lists from member states' DPAs. A DPIA is only mandatory where processing is likely to result in a high risk to the rights and freedoms of natural persons (Article 35(1), GDPR). The EDPB's assessment aims to develop consistent application of the GDPR and offer guidance to companies. (See EDPB: Data Protection Impact Assessment (DPIA).)

Some have also expressed concerns regarding the use of blockchain technology and the GDPR. The French DPA (CNIL) published an initial report analyzing certain fundamental questions, including:

- The challenges of identifying data controllers and data processors when using blockchain technology.

- The necessity of automated individual decision-making for the performance of smart contracts.

(See CNIL: Blockchain: Solutions for a responsible use of the blockchain in the context of personal data; for more detail on blockchain technology and tensions with the GDPR, see Practice Note, Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview: Tensions between Using Blockchain Technology and Data Privacy Obligations.)

Notable EU Enforcement Actions

The DPAs began receiving complaints from data subjects and consumer organizations after the GDPR took effect, with some DPAs announcing that they received thousands of complaints.

Some notable GDPR complaints filed in 2018 against the major tech companies include:

- Privacy activist Max Schrems' organization nyob filed four complaints against major social media companies relating to their alleged forced consent policies, which according to the complaint, violate the GDPR because they require users to agree to a privacy policy on an all-or-nothing basis (see nyob: GDPR: noyb.eu filed four complaints over “forced consent” against Google, Instagram, WhatsApp and Facebook).

- Multiple consumer advocacy groups across Europe filed complaints with their respective DPAs against Google for its geolocation data collection practices, alleging the company has no legal basis for processing that data in violation of the GDPR.

- After ruling that Microsoft's data collection methods pose a risk to user privacy, the Dutch authorities alerted Microsoft regarding possible regulatory action if it fails to take prescribed steps to remediate its data collection practices. Microsoft has until April 2019 to comply or face a fine under the GDPR.

Facebook continued to be at the center of high-profile proceedings involving privacy and data security issues before EU tribunals and European courts, including:

- **In a dispute relating to standard contractual clauses.** The Irish Supreme Court granted Facebook leave to appeal a ruling regarding standard contractual clauses (SCCs) and the Privacy Shield to the European Court of Justice (ECJ). SCCs remain a valid mechanism for data transfers until the ECJ issues a ruling otherwise. The dispute stems from Max Schrems' complaint to the Ireland DPA regarding Facebook's data transfers. Facebook countered that its data transfers were lawful.

- **In enforcement actions relating to the Cambridge Analytica data incident.** For example,

  - in October,the UK's Information Commissioner Office (ICO) issued Facebook a £500,000 fine under the Data Protection Act 1998 (DPA 1998), the UK's implementation of the GDPR's predecessor, for failing to suitably check on apps and developers using its platform, related to the Cambridge Analytica data incident. In November, Facebook filed an appeal. The European Parliament initiated a series of hearings related to the same incident and issued a resolution demanding a full audit to assess Facebook's data security practices; and

  - in December, the Italian Data Protection Authority (*Garante per la protezione dei dati personali*) fined Facebook EUR10 million for misleading users regarding its data practices and directed the company to publish an apology to users on its website and app.

- **In disputes relating to deceased user profiles.** The UK High Court granted an application requesting Facebook provide information about the party that requested deletion of a deceased user's profile months after the user's death (see *Sabados v Facebook Ireland* [2018] EWHC 2369).

The ICO also brought several privacy and data security-related enforcement actions against other US companies or their affiliates, related to breaches or incidents predating the GDPR, including:

- A fine against Yahoo! UK Services Ltd. for £250,000 for failing to take appropriate measures to prevent its 2014 data breach affecting more than 500,000 UK accounts.

- A fine against Uber for £385,000 for failing to protect customers' and drivers' personal information during a 2016 data breach. The Dutch DPA issued a fine of EUR600,000 for violating the Dutch data breach regulation regarding the same incident, and the French DPA issued a fine of EUR400,000 for the 2016 breach.

- A £500,000 fine against Equifax Ltd. for failing to protect the personal information of almost 15 million UK citizens stemming from its 2017 data breach.

EU-US Privacy Shield

The EU-US Privacy Shield Framework supports cross-border personal information data transfers from EU member states to the US. After EU and US officials met for a second annual review of the Privacy Shield, the European Commission (EC) published:

- A report, concluding that the US continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield (see Legal Update, European Commission's Second Annual Review of EU-US Privacy Shield Shows Improvements but a Permanent Ombudsperson Should Be Nominated).

- A report on whether the safeguards for automated decision-making are adequate under the Privacy Shield. The EC concluded that US laws, notably the Equal Credit Opportunity Act, the FCRA, and the Fair Housing Act, offer certain protections against adverse decisions where companies most likely resort to automated processing to make decisions affecting the individual (see EC: Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield.)

For steps to take when self-certifying to the EU-US Privacy Shield Framework, see Privacy Shield Self-Certification Checklist.

Other International Developments

APEC Cross-Border Privacy Rules System Expansion

The group of countries that participate in the APEC Cross-Border Privacy Rules System (APEC CBPR) continued to expand in 2018, with Singapore, Australia, and Chinese Taipei joining the program. The program consists of eight participating system economies, including the US.

In September, the released final draft of the United States-Mexico-Canada Agreement (USMCA), which revised NAFTA, stated that the APEC CBPR is a valid mechanism to facilitate cross-border information transfers, recognizing the CBPRs as a workable method (see Office of the US Trade Representative: United States-Mexico-Canada Agreement).

Canada

Canada's Office of the Privacy Commissioner (OPC) issued guidance for companies regarding requirements under the Personal Information Protection and Electronic Documents Act (PIPEDA) and related regulations, including:

- Final guidance regarding obligations under Canada's new data breach notification requirements (see OPC: What you need to know about mandatory reporting of breaches of security safeguards).

- Guidance on meaningful consent under Canadian law, including key elements of consent and issues surrounding consent and children (see OPC: Guidelines for obtaining meaningful consent and Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)).

Also in Canada:

- The Supreme Court of Canada (SCC) protected privacy in shared computing devices, finding that a person that shares an electronic device with someone else cannot waive the other user's rights under the Canadian Charter of Rights and Freedoms (*R. v. Reeves, 2018 SCC 56*).

- The Canadian Radio-Television Commission (CRTC) issued guidelines on its approach to Canada's anti-spam legislation (CASL) (see CRTC: Compliance and Enforcement Information Bulletin CRTC 2018-415).

- The OPC adopted the ICDPPC's Declaration on Ethics and Data Protection in Artificial Intelligence (see Artificial Intelligence).

- The House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI Committee) released its final reports on the Cambridge Analytica scandal, recommending greater government regulation to limit unwanted surveillance and hate speech and to protect Canadian elections from foreign interference (see ETHI: Breach of Personal Information Involving Cambridge Analytica and Facebook).

Looking Forward

Privacy and data security issues likely to get particular attention in 2019 include:

- **Data privacy compliance issues, with a special focus on the GDPR, Brexit, and the CCPA.** Expect multinational companies to carefully watch and continue to improve their compliance procedures as regulators reveal their GDPR enforcement priorities. Brexit also requires compliance attention, particularly if a no-agreement situation occurs, leaving the UK without a data protection adequacy position. The CCPA takes effect in 2020 and requires attention from companies that collect and use Californians' personal information. The CCPA took its inspiration from the GDPR, but the laws are different. Compliance with the GDPR does not necessarily mean compliance with the CCPA. While not likely, it is conceivable that Congress may pass a comprehensive privacy law in 2019, creating additional compliance concerns.

- **Continued attention on biometric privacy.** With more companies testing or rolling out consumer-facing technologies that use biometric authentication, expect continued litigation under Illinois' biometric privacy law. This trend is likely to take an even sharper increase following the Illinois's Supreme Court's early 2019 decision in *Rosenbach*, holding that individuals need not suffer actual injury beyond a statutory violation to take action under the state's law.

- **Mobile geolocation privacy.** Mobile geolocation data privacy has become an increasing concern for app developers, end users, and regulators. This issue is likely to continue to garner more attention, especially in light of the GDPR, the Supreme Court's decision in *Carpenter*, and increasing consumer awareness stemming from several notable media reports.

- **Privacy and data security risk management across sectors and in due diligence processes.** Risk management, cyberinsurance, and cyberattack prevention using reasonable data security practices are likely to continue to demand attention across sectors and in merger and acquisition due diligence processes. Buyers should be increasingly concerned about undisclosed data security incidents or the risk of undiscovered intrusions, even as they perform now-standard activities, such as examining a target company's security practices and audits. Regulatory enforcement, consumer class actions, and shareholder derivative suit trends all continue to drive these needs. Expect companies to step up privacy and data flow audits to avoid their own Cambridge Analytica incident.

- **New applications of blockchain and AI technologies.** Emerging blockchain technology may soon offer innovative approaches to identity management and other cybersecurity challenges, such as trusted information sharing and data tampering prevention. AI technology also offers innovative solutions, but raises ethical concerns. Expect these technologies to garner further attention as industries continue to test and launch pilot programs.

