

# TRENDS IN PRIVACY AND DATA SECURITY

---



**JEFFREY D. NEUBURGER**

PARTNER  
PROSKAUER ROSE LLP

Jeff is co-head of the firm's Technology, Media & Telecommunications Group, head of the firm's Blockchain Group, and a member of the firm's Privacy & Cybersecurity Group. His practice focuses on technology, media, and intellectual property-related transactions, counseling, and dispute resolution.



*As large-scale data breaches and other cyber incidents continue to pose significant threats worldwide, privacy and cybersecurity remain top priorities for regulators and companies alike. To minimize risks and reduce potential liability, companies and their counsel should stay updated on privacy and data security-related enforcement activity, notable litigation, new regulations, and key emerging issues.*

the-lightwriter /iStock photo

Companies must keep up with the dynamic legal obligations governing privacy and data security, understand how these obligations apply in practice, improve their cyber intelligence, and manage their compliance to minimize risks. This article reviews important privacy and data security developments over the past year and highlights key issues for 2019. Specifically, it addresses recent:

- Federal regulation and enforcement actions.
- State regulation and enforcement actions.
- Private litigation.
- Federal and state legislation.
- International developments likely to affect US companies.
- Trends likely to gain more prominence this year.



Search [US Privacy and Data Security Law: Overview](#) for more on the current patchwork of federal and state laws regulating privacy and data security.

## 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).
- The Department of Health and Human Services (HHS).



Search [Trends in Privacy and Data Security: 2018](#) for the complete online version of this resource, which includes information on regulatory and enforcement activity by the Securities and Exchange Commission and other federal agencies, as well as industry self-regulation efforts in artificial intelligence, cybersecurity, the Internet of Things, and the online and mobile advertising and payment card industries.

## 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).



Search [FTC Data Security Standards and Enforcement](#) for more on the FTC's authority and standards.

## FTC Guidance

In 2018, the FTC published online blog posts to explain its existing guidance in several areas, including small business cybersecurity, use of 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 released a paper titled The Connected Cars Workshop: The Federal Trade Commission Staff Perspective (available at [ftc.gov](#)), which includes best practices for addressing privacy and data security risks related to automated and connected vehicles, such as information sharing, network design, risk assessment and mitigation, and industry self-regulation.

- **Children's privacy practices.** The FTC approved modifications to the Entertainment Software Rating Board's (ESRB's) COPPA safe harbor program. The ESRB is a self-regulatory organization for the video game industry.
- **Mobile device security.** The FTC issued a report titled FTC Recommends Steps to Improve Mobile Device Security Update Practices (available at [ftc.gov](#)), which makes several recommendations for expediting the mobile device security update process, including:
  - improving consumer education;
  - implementing minimum guaranteed security support periods; and
  - streamlining the update process.
- **Informational injuries.** The FTC released a paper titled Informational Injury Workshop: BE and BCP Staff Perspective (available at [ftc.gov](#)), which recounts key perspectives discussed at a workshop hosted by the FTC 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 would keep this 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 over a 2014 data breach of driver data after the FTC discovered that the company had failed to disclose a subsequent 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, a PayPal subsidiary, settled charges alleging that the company misled consumers about its app's privacy controls by 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.** The FTC reached settlements with, for example:
  - an electronic toy manufacturer, which agreed to pay \$650,000 to settle charges that its app violated COPPA by collecting children's personal information without providing notice to parents and obtaining their consent (for more information, search [FTC Settles COPPA Suit with Toy Maker](#) on Practical Law); and
  - a web-based talent search company, which agreed to pay \$235,000 over its alleged collection of users' 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 to 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) (*FTC v. RealPage, Inc.*, No. 18-2737 (N.D. Tex. Oct. 16, 2018)).
- **Make accurate representations about cross-border data transfer practices.** The FTC settled charges with several companies that allegedly 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 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't Screening, Inc.*, 2018 WL 6078361 (F.T.C. Nov. 15, 2018); *In re VenPath, Inc.*, 2018 WL 6078359 (F.T.C. Nov. 15, 2018); *In re ReadyTech Corp.*, 2018 WL 5631091 (F.T.C. Oct. 17, 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 Eleventh Circuit vacated an FTC order directing now-defunct LabMD, Inc. to overhaul and replace its data security program. 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. (*LabMD, Inc. v. FTC*, 894 F.3d 1221 (11th Cir. 2018).) Going forward, the FTC will likely 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.
- The Ninth Circuit ruled that telecommunications carriers are immune from FTC regulation of unfair and deceptive practices only 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

The HHS Office for Civil Rights (OCR) provides guidance and takes enforcement action under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and related regulations.



Search [HIPAA and Health Information Privacy Compliance Toolkit](#) for resources to assist companies in complying with HIPAA regulations.

### HHS Guidance

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

- HIPAA authorizations for using and disclosing protected health information (PHI) for research purposes.
- Vulnerabilities in computer chips that could pose threats.
- Electronic device and media disposal.

In late December 2018, HHS also issued a four-volume set of voluntary cybersecurity practices. The publications are the result of a Cybersecurity Act of 2015 mandate and public-private partnership. (See HHS, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, available at [phe.gov](#).)

### 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 over a series of cyberattacks, which began with a phishing email to an employee and exposed the PHI of approximately 79 million people (for more information, search [Anthem's \\$16 Million HIPAA Settlement Is Largest in History](#) on Practical Law).
- **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 (for more information, search [Health Provider Must Pay HHS \\$125,000 for Disclosing PHI to the Press](#) on Practical Law); 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 (for more information, search [Television Crew's Filming of Hospital Patients Results in HIPAA Settlements Totaling Nearly \\$1 Million](#) on Practical Law).
- **Conduct a thorough risk analysis and implement effective safeguards.** For example:
  - Fresenius Medical Care North America agreed to pay \$3.5 million for multiple data breaches related to alleged failures to adequately safeguard hardware and electronic media that contained PHI (for more information, search [Five Breaches Result in \\$3.5 Million HIPAA Settlement](#) on Practical Law);
  - 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 the loss of unencrypted thumb drives (for more information, search [Failure to Encrypt Leads to \\$4.3 Million in HIPAA Civil Money Penalties](#) on Practical Law); and
  - Pagosa Springs Medical Center in Colorado agreed to pay \$111,400 to settle allegations that the hospital failed to terminate a former employee's access to PHI. Under a two-year corrective action plan, the hospital agreed, among other things, to update policies and procedures and train its workforce. (See Pagosa Springs Medical Center Resolution Agmt. and Corrective Action Plan, available at [hhs.gov](#).)
- **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 (for more information, search [Receiver for Out-of-Business HIPAA BA Reaches \\$100,000 Settlement with HHS](#) on Practical Law).

ArtHead-/iStock photo

## STATE REGULATION AND ENFORCEMENT

Cybersecurity regulations for state-regulated financial services organizations remained an important issue in 2018. 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 §§ 500.00 to 500.23).
- Expanded the scope of its regulations to include credit reporting agencies (23 NYCRR §§ 201.00 to 201.09).



Search [The NYDFS Cybersecurity Regulations](#) for more on NYDFS requirements.

Other key developments at the state level included those involving:

- Single-state enforcement actions.
- High-profile multi-state and joint FTC 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 over inadvertent PHI disclosures (see California Department of Public Health: Breach of Confidential Patient Medical Information, available at [cdph.ca.gov](#)).
- Massachusetts, which settled with:
  - UMass Memorial Medical Group Inc., which agreed to pay \$230,000 and improve security practices regarding employee data access following two data breaches (see Press Release, Massachusetts Office of the AG, UMass Memorial Health Care Entities to Pay \$230,000 to Resolve AG's Lawsuit Over Data Breaches, available at [mass.gov](#)); and
  - Yapstone Holdings Inc., which agreed to pay \$155,000 and update security policies following the payment processor's alleged website error that exposed residents' personal information (Press Release, Massachusetts Office of the AG, Payment Processor to Pay \$155,000 Over Data Breach Affecting Thousands of Massachusetts Residents, available at [mass.gov](#)).
- 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 over the same data breach (see Press Release, New Jersey Office of the AG, Defunct Georgia Vendor Responsible for Exposing Virtua Medical Group Patient Files Online Agrees to \$200,000 Settlement; Press Release, Virtua Medical Group Agrees to Pay Nearly \$418,000, Tighten Data Security to Settle Allegations of Privacy Lapses Concerning Medical Treatment Files of Patients, available at [nj.gov](#));
  - Unixiz, Inc., which agreed to shut down its teen social website, pay a \$98,000 fine, and comply with applicable laws on its other websites to resolve allegations related to

COPPA violations and a 2016 data breach (see Press Release, 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, available at [nj.gov](#));

- Meitu, Inc., a Chinese software company, which agreed to pay \$100,000 and alter its practices to settle charges that it violated COPPA (see Press Release, 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, available at [nj.gov](#)); and
- Lightyear Dealer Technologies, which agreed to pay \$80,000 and institute comprehensive data security changes after a security researcher accessed an unencrypted database containing the personal information of auto dealership customers (see Press Release, 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, available at [nj.gov](#)).
- New York, which settled with:
  - Oath, Inc. (formerly AOL) for \$4.95 million in a COPPA enforcement action regarding billions of ad auctions on websites directed to children under age 13 (for more information, search [NY Attorney General Announces \\$4.95 Million COPPA Penalty](#) on Practical Law);
  - Aetna Inc. for \$1.15 million following claims that the health insurer revealed the HIV status of thousands of members (the health insurer reached separate settlements with other states and also paid \$17 million to settle a class action lawsuit over the incident) (see Press Release, New York Office of the AG, A.G. Schneiderman Announces Settlement with Aetna Over Privacy Breach of New York Members' HIV Status, available at [ag.ny.gov](#); *Beckett v. Aetna Inc.*, 2018 WL 2089301 (E.D. Pa. Jan. 15, 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 Press Release, New York Office of the AG, A.G. Schneiderman Announces \$575,000 Settlement with EmblemHealth After Data Breach Exposed Over 80,000 Social Security Numbers, available at [ag.ny.gov](#)); and
  - Equifax Consumer Services, LLC, Priceline.com, LLC, and other companies for operating mobile apps that allegedly failed to address known cyber vulnerabilities (for more information, search [New York AG Settles Charges Against Five Companies for Mobile Application Security Failures](#) on Practical Law).

## 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 over 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. (For more information, search [Uber Agrees to \\$148 Million Data Breach Settlement with State Attorneys General](#) on Practical Law.)

- Equifax Inc. agreed to a consent order with the NYDFS and seven other state banking regulators to take corrective actions in the wake of its massive 2017 data breach (see Press Release, NYDFS, DFS Takes Additional Action to Hold Equifax Accountable for Massive 2017 Data Breach, available at [dfs.ny.gov](#)).

## PRIVATE LITIGATION

Article III 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) (see, for example, *Bassett v. ABM Parking Servs., Inc.*, 883 F.3d 776 (9th Cir. 2018) (denying standing for a bare procedural FACTA violation); *Auer v. Trans Union, LLC*, 902 F.3d 873 (8th Cir. 2018) (denying standing for an alleged FCRA procedural violation); *Muransky v. Godiva Chocolatier, Inc.*, 905 F.3d 1200 (11th Cir. 2018) (conferring standing where the printing of full credit card numbers on receipts exposed the plaintiffs to increased risk)).

Other highlights for 2018 include:

- US Supreme Court rulings on privacy-related issues.
- Data breach-related actions.
- Biometrics actions.



Search [Trends in Privacy and Data Security: 2018](#) for the complete online version of this resource, which includes information on recent cases involving the Telephone Consumer Protection Act of 1991 and other notable privacy and data security-related decisions from the past year.

## PRIVACY-RELATED SUPREME COURT ACTIONS

In 2018, the Supreme Court:

- Issued an opinion in *Carpenter v. United States*, in which it:
  - declined to extend the third-party doctrine (under which individuals generally have no legitimate expectation of privacy in information they voluntarily turn over to third parties) to the government's collection of cell-site location information from the defendant's wireless carrier; and
  - deemed the collection a Fourth Amendment search. (138 S. Ct. 2206 (2018)).
- Declined to review a decision that invalidated the Federal Communications Commission's (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*, 138 S. Ct. 1043 (2018)).
- Heard arguments regarding an \$8.5 million *cy pres* settlement in a privacy-related class action against Google. The Supreme Court ordered supplemental briefing on Article III standing, signaling a potential impact on future privacy litigation (*Frank v. Gaos*, 2018 WL 5722840 (U.S. Oct. 31, 2018); *Frank v. Gaos*, 139 S. Ct. 475 (2018)).

## DATA BREACH LITIGATION

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

- The type and sophistication of the data intrusion.
- The sensitivity of the stolen personal information.
- The amount of time that 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 who 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 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 the 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 Seventh Circuit held that consumers had standing based on payments made for credit monitoring and unavailability of funds from affected accounts (*Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826 (7th Cir. 2018); but see *Cnty. Bank of Trenton v. Schnuck Mkts., Inc.*, 887 F.3d 803 (7th Cir. 2018) (holding that 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 involving:


- 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 their consent (*In re Vizio, Inc., Consumer Privacy Litig.*, No. 16-2693 (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. 16-2752 (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 over legal fees (*In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2019 WL 387322 (N.D. Cal. Jan. 30, 2019)).

## State law activity increased over the past year given the lack of comprehensive federal privacy or data security legislation.

- 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 finalized its \$115 million settlement with consumers following a 2015 data breach involving nearly 80 million records (*In re Anthem, Inc. Data Breach Litig.*, No. 15-2617 (N.D. Cal. Aug. 16, 2018)).

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

- *Sgarlata v. PayPal Holdings, Inc.*, 2018 WL 6592771 (N.D. Cal. Dec. 13, 2018) (dismissing a shareholder suit alleging misleading statements over a newly acquired subsidiary's cyber incident).
- *Ali v. Intel Corp.*, 2018 WL 2412111 (N.D. Cal. May 29, 2018) (consolidating a shareholder suit over vulnerabilities discovered in Intel processors).
- *In re Yahoo! Inc. Securities Litigation*, 2018 WL 4283377 (N.D. Cal. Sept. 7, 2018) (issuing final approval of an \$80 million settlement following large-scale cyberattacks).
- *In re Facebook, Inc. Shareholder Derivative Privacy Litigation*, No. 18-1792 (N.D. Cal. June 27, 2018) (consolidating a shareholder suit over the Cambridge Analytica data leak).


 Search [Shareholder Derivative and Securities Fraud Litigation After Data Breaches](#) for more on these suits and the obstacles plaintiffs face establishing their claims.

### BIOMETRICS PRIVACY LITIGATION

Litigation under the Illinois Biometric Information Privacy Act (BIPA) against employers, businesses, and social media sites and other mobile platforms remained robust in 2018. 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 an actual injury beyond a statutory violation to sustain a private action (2019 WL 323902 (Ill. Jan. 25, 2019)). This ruling will most likely:

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

Companies with connections to Illinois should carefully consider how they collect and use biometrics information.

 Search [Biometrics in the Workplace and Biometrics Litigation: An Evolving Landscape](#) for more on BIPA and emerging issues in biometrics law and litigation.

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 F. App'x 368 (9th Cir. 2018)).

### FEDERAL AND STATE LEGISLATION

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

- The Clarifying Lawful Overseas Use of Data (CLOUD) Act (Pub. L. No. 115-141), which:
  - amends portions of the Stored Communications Act (SCA) (18 U.S.C. §§ 2701 to 2713) 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 the data 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.
- The NIST Small Business Cybersecurity Act, which requires the National Institute of Standards and Technology (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 the Department of Homeland Security to lead the national effort against cybersecurity threats to critical infrastructure (Pub. L. No. 115-278).

Additionally, state law activity increased over the past year given the lack of comprehensive federal privacy or data security legislation. Key developments included the enactment of:

- The California Consumer Privacy Act of 2018 (CCPA), which establishes comprehensive consumer data protection rights.
- Data breach notification laws by the remaining states that did not have these laws.
- New data security laws by several states.



Search [Trends in Privacy and Data Security: 2018](#) for the complete online version of this resource, which includes information on other new and notable privacy-related statutes.

## CALIFORNIA CONSUMER PRIVACY ACT OF 2018

California passed and subsequently clarified the CCPA, a comprehensive data protection law that grants consumers rights to:

- Notice, either before or at the point of collection, about what personal information categories a company collects and the intended use purposes. Companies 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 a consumer is 16 years old or older.
- Affirmatively opt in to the sale of their personal information by providing direct authorization, if a consumer is between 13 and 16 years old, or through parental or guardian consent, if a consumer is under age 13.
- Not face discrimination for asserting their CCPA rights, although companies may offer certain price or service differences directly related to the value of a consumer's data or financial incentive programs, provided this does not result in unjust, unreasonable, coercive, or usurious practices.

The CCPA broadly defines personal information and imposes specific obligations on covered entities. The California Attorney General holds rulemaking authority and will 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.



Search [Understanding the California Consumer Privacy Act \(CCPA\)](#) for more on the CCPA.

## STATE DATA BREACH NOTIFICATION LAWS

2018 brought data breach notification obligations to all 50 states when the last two holdouts, South Dakota and Alabama, enacted data breach notification laws.

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

- Arizona amended its law to:
  - expand the definition of personal information; and
  - update notification timing requirements. (A.R.S. §§ 18-551 to 18-552.)
- 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 numbers, and medical information; and
  - require notice to the state attorney general if a breach affects more than 500 Colorado residents. (C.R.S. §§ 6-1-713, 6-1-713.5, 6-1-716.)
- 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 so that notification is not required if there is no reasonable likelihood of harm to state residents from the breach, but require 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.)
- Oregon amended its 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.)
- Virginia amended its law to require income tax return preparers to notify the state's Department of Taxation without unreasonable delay if:
  - Virginia individuals' unencrypted tax return information is compromised; and
  - the preparer reasonably believes that the incident has caused or will cause identity theft. (Va. Code Ann. § 58.1-341.2.)



## STATE CYBERSECURITY LAWS

Several states adopted other cybersecurity-related laws, including:

- California, which passed:
  - an Internet of Things data security law that requires connected device manufacturers to equip their devices with reasonable security features (Cal. Civ. Code § 1798.91.04); 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 (R.C. 1354.02 to 1354.03).
- 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. §§ 8-2609 and 87-808.)
- South Carolina, which became the first state to follow model data security legislation from the National Association of Insurance Commissioners with its passage of the Insurance Data Security Act (S.C. Code Ann. §§ 38-99-10 to 38-99-100).
- Vermont, which passed a law to regulate data brokers, generally including businesses that aggregate and sell personal information of consumers with whom they do not have a direct relationship (9 V.S.A. §§ 2430, 2433, 2446, 2447). The Vermont Attorney General's Office also published guidance regarding related regulations.

## 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.

Important developments include those related to:

- The General Data Protection Regulation (GDPR).
- Enforcement actions in the EU.
- The EU-US Privacy Shield cross-border data transfer framework.

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



Search [Trends in Privacy and Data Security: 2018](#) for the complete online version of this resource, which includes information on the APEC Cross-Border Privacy Rules system and new data protection guidelines in Canada.

## GDPR

Data protection obligations for companies that collect and use information from individuals in the EU are undergoing a significant transition with the adoption of the GDPR, which took effect on May 25, 2018 and applies directly to all member states. This trend will persist in 2019 as the EU and the rest of the 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 GDPR affects companies operating in the EU, but also applies extraterritorially to companies 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).

One month prior to 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.

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 and 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, available at [edpb.europa.eu](#)).
- Which processing operations require a data protection impact assessment (DPIA), based on lists from member states' DPAs. A DPIA is mandatory only 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), available at [edpb.europa.eu](#).)

Some regulators 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 and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data](#), available at [cnil.fr](#).)

# Data protection obligations for companies that collect and use information from individuals in the EU are undergoing a significant transition with the adoption of the GDPR.



Search [Overview of EU General Data Protection Regulation](#) for more on the GDPR.

Search [Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview](#) for more on cybersecurity risks and potential tensions between blockchain technology and the GDPR.

## 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.

Notable GDPR complaints filed in 2018 against major tech companies included the following:

- Privacy activist Max Schrems' organization, *noyb*, filed four complaints against major social media companies over 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 *noyb*, GDPR: *noyb.eu* Filed Four Complaints Over "Forced Consent" Against Google, Instagram, WhatsApp and Facebook, available at *noyb.eu*).
- 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 this data in violation of the GDPR.
- After concluding that Microsoft's data collection methods pose a risk to user privacy, the Dutch authorities alerted the company about 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. (See Government of the Netherlands, Update on Negotiations Between Dutch Central Government and Microsoft on GDPR Compliance, available at *rijksoverheid.nl*).

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 over standard contractual clauses.** The Irish Supreme Court granted Facebook leave to appeal the Irish High Court's decision to refer to the European Court of Justice (ECJ) questions regarding the validity of standard contractual clauses (SCCs) and the Privacy Shield (*Data Prot. Comm'r v. Facebook Ireland Ltd.* [2018] IESC 38). SCCs remain a valid mechanism for data transfers until the ECJ rules 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.

- **Enforcement actions over 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 and, in November, Facebook filed an appeal (additionally, 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 DPA (*Garante per la protezione dei dati personali*) fined Facebook €10 million for misleading users over its data practices and directed the company to publish an apology to users on its website and app.

- **A dispute over deceased user profiles.** The UK High Court granted an application seeking to have Facebook provide information about who requested deletion of a deceased user's profile months after his death (see *Sabados v. Facebook Ireland* [2018] EWHC 2369).

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

- A £250,000 fine against Yahoo! UK Services Ltd. for failing to take appropriate measures to prevent its 2014 data breach affecting over 500,000 UK accounts.
- A £385,000 fine against Uber for failing to protect customers' and drivers' personal information during a 2016 data breach. Additionally, the Dutch DPA issued a fine of €600,000 and the French DPA issued a fine of €400,000 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 reports:



*With more companies introducing technologies that use biometric authentication, counsel should expect continued litigation under BIPA. This trend will likely increase following the Illinois Supreme Court's early 2019 decision in Rosenbach.*

- Concluding that the US continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield (for more information, search [European Commission's Second Annual Review of EU-US Privacy Shield Shows Improvements But a Permanent Ombudsperson Should Be Nominated](#) on Practical Law).
- Addressing 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, available at [ec.europa.eu](http://ec.europa.eu).)



Search [Privacy Shield Self-Certification Checklist](#) for information on the steps to take when self-certifying to the EU-US Privacy Shield Framework.

## LOOKING FORWARD

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

- **Data privacy compliance issues, with a special focus on the GDPR, Brexit, and the CCPA.** Counsel should expect multinational companies to carefully watch and continue to improve their compliance procedures as regulators reveal their GDPR enforcement priorities. Brexit will also require 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 is inspired by the GDPR, but the laws are different. Compliance with the GDPR does not necessarily equate to compliance with the CCPA. While unlikely, Congress might pass a comprehensive privacy law in 2019, creating additional compliance concerns.

- **Biometric privacy.** With more companies testing or introducing consumer-facing technologies that use biometric authentication, counsel should expect continued litigation under BIPA. This trend will likely rapidly increase following the Illinois Supreme Court's early 2019 decision in *Rosenbach*, holding that individuals need not suffer an actual injury beyond a statutory violation to take action under BIPA.
- **Mobile geolocation privacy.** Mobile geolocation data privacy has become an increasing concern for app developers, end users, and regulators. This issue will 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, cyber insurance, and cyberattack prevention through reasonable data security practices will continue to demand attention across sectors and in merger and acquisition due diligence processes. Buyers will 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. Trends in regulatory enforcement, consumer class actions, and shareholder derivative suits continue to drive these needs. Companies should enhance their privacy and data flow audits to avoid an incident like Cambridge Analytica.
- **New applications of blockchain and artificial intelligence (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. These technologies are likely to garner further attention as industries continue to test and launch pilot programs.

*The author would like to thank his colleague Jonathan P. Mollo for his tremendous efforts in co-authoring this article.*