



# Trends in Privacy and Data Security

Privacy and cybersecurity remain top priorities for regulators and companies alike, as the threats posed by large-scale data breaches and other cyber incidents show no signs of waning. Companies and their counsel must monitor privacy and data security-related enforcement trends, new laws and regulations, and key emerging issues to mitigate risks and minimize potential liability.



**JEFFREY D. NEUBURGER**  
PARTNER  
PROSKAUER

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.



**JONATHAN P. MOLLOY**  
TECHNOLOGY & NEW MEDIA  
LEGAL CONTENT EDITOR  
PROSKAUER


Jonathan is an attorney and a legal content editor at the firm's New York office, focusing on technology, intellectual property, data privacy, online content and e-commerce, and blockchain and cryptocurrency.

**R**eports of sophisticated cyberattacks and ransomware threats dominated 2021 headlines, along with evolving state data privacy laws in the absence of comprehensive federal data protection regulation. Cross-border data transfers between the European Union (EU) and the US still lack a clear, streamlined mechanism while national authorities continue to negotiate an EU-US Privacy Shield replacement. The past year also showcased the ongoing cyber risks of remote and hybrid working due to COVID-19 measures and the rise of double extortion ransomware attacks, which occur when hackers demand payment in exchange for decryption keys and promises to avoid disclosing compromised data.

Like 2020's SolarWinds cyberattack disclosure, December 2021 brought another winter cybersecurity surprise with news of a serious vulnerability in Log4j, a widely used, open-source logging library. The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) offered guidance on applying available patches (CISA, Apache Log4j Vulnerability Guidance, available at [cisa.gov](https://www.cisa.gov)). However, the high-risk exploit undoubtedly spurred attackers to infiltrate vulnerable networks, prompting the Federal Trade Commission (FTC) to issue a January 2022 advisory reminding companies that its reasonableness standard for data security measures demands appropriate patching (Press Release, FTC, FTC Warns Companies to Remediate Log4j Security Vulnerability (Jan. 4, 2022), available at [ftc.gov](https://www.ftc.gov)).

Organizations must keep up with the dynamic and increasing legal obligations governing privacy and data security, understand how these obligations apply, monitor cyber risks and attack trends, and manage their compliance to minimize exposure. This article reviews important privacy and data security developments in 2021 and highlights key issues for the rest of the year ahead. Specifically, it addresses:

- Federal and state guidance, regulations, and enforcement actions.
- Private litigation.
- Federal and state legislation.
- International developments likely to affect US companies, including the continued fallout from the invalidation of the EU-US Privacy Shield as a mechanism for cross-border data transfers.
- Trends likely to gain more attention in 2022.

 Search [Trends in Privacy and Data Security: 2021](#) for the complete online version of this resource, which includes more on new federal and state regulations and legislation, as well as industry self-regulation and guidance.

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 GUIDANCE, REGULATION, AND ENFORCEMENT

Several federal agencies issued guidance and took notable privacy and data security enforcement actions in 2021, including:

- The FTC.
- The Department of Health and Human Services (HHS).
- The Department of Commerce and its National Institute of Standards and Technology (NIST).
- The Federal Communications Commission (FCC).

 Search [Trends in Privacy and Data Security: 2021](#) for information on guidance and enforcement activity by the Securities and Exchange Commission (SEC), DHS, and various other federal agencies.

### FTC

The FTC is the primary federal agency regulating 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 Regulations and Guidance

In late 2021, the FTC updated its Safeguards Rule (16 C.F.R. §§ 314.1 to 314.6), under the Gramm-Leach-Bliley Act (GLBA), which requires non-banking financial institutions to implement and maintain a written information security program to protect customers' information. The updates, which generally take effect on December 9, 2022:

- Include significantly more prescriptive safeguards requirements.
- Expand the rule's scope and accountability obligations.

(For more information, search [FTC Amends Safeguards Rule to Strengthen Data Security Obligations](#) on Practical Law.)

In September, the FTC issued a policy statement applying the Health Breach Notification Rule (HBNR) (16 C.F.R. §§ 318.1 to 318.9) to apps and connected devices that collect consumers' health information if they both:

- Are not subject to regulations under the Health Insurance Portability and Accountability Act (HIPAA).
- Can draw data from multiple sources, which may include consumer inputs and application programming interfaces (APIs) that connect to devices such as fitness trackers.

(FTC, Statement of the Commission on Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021), available at [ftc.gov](https://www.ftc.gov).)

The HBNR generally requires personal health records vendors and related entities to notify consumers following certain data breaches, but the FTC has not previously enforced it against general health apps (see FTC, Revised Health Breach Notification Rule Resources Spell Out Companies' Legal Obligations (Jan. 21, 2022), available at [ftc.gov](https://www.ftc.gov); for more information, search [FTC Warns Health Apps to Comply with Its Health Breach Notification Rule](#) on Practical Law).

In August, the FTC removed Aristotle International, Inc. from its list of approved, self-regulatory safe harbor programs under the Children's Online Privacy Protection Act (COPPA). Aristotle was the first organization to be removed from the list. (For more information, search [Aristotle Inc. Removed from FTC's COPPA Safe Harbor Program](#) on Practical Law.)

The FTC also continued to blog and released notable guidance on:

- Internet service provider (ISP) data privacy practices (see Staff Report, FTC, A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers (Oct. 21, 2021), available at [ftc.gov](https://www.ftc.gov)).
- Board oversight of data security (see FTC, Corporate Boards: Don't Underestimate Your Role in Data Security Oversight (Apr. 28, 2021), available at [ftc.gov](https://www.ftc.gov)).
- Fairness in artificial intelligence (AI) applications (see FTC, Aiming for Truth, Fairness, and Equity in Your Company's Use of AI (Apr. 19, 2021), available at [ftc.gov](https://www.ftc.gov)).

### 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, several 2021 actions emphasize that companies should:

- **Ensure that privacy and data security practices match promises.** For example, the FTC reached settlements with:
  - a movie ticket subscription service operator that claimed in its privacy policy that it protected personal information but allegedly failed to take reasonable steps to prevent unauthorized access (*In re Moviepass, Inc.*, 2021 WL 4786292 (F.T.C. Oct. 1, 2021)); and
  - a developer of an ovulation and fertility tracking app that allegedly shared users' sensitive health information with marketers and data analytics providers after promising to keep the information private (*In re Flo Health, Inc.*, 2021 WL 2709271 (F.T.C. June 17, 2021)).
- **Protect children by complying with COPPA obligations.** For example, the FTC reached settlements with:

- an online ad exchange platform for \$2 million after it allegedly failed to flag certain child-directed apps and knowingly collected children's personal information and location data even after user opt-out (Stipulated Order for Permanent Injunction and Civil Penalty Judgment, *U.S. v. OpenX Techs., Inc.*, No. 21-09693 (C.D. Cal. Dec. 27, 2021)); and
- a children's app developer for \$3 million after it allegedly failed to notify parents of its data collection and disclosure practices and obtain their consent (Stipulated Order for Permanent Injunction and Civil Penalty Judgment, *United States v. Kuuhub Inc.*, No. 21-01758 (D.D.C. July 21, 2021)).

- **Market mobile monitoring products only for legitimate and lawful purposes.** The FTC settled with a "stalking" app developer that provided products allowing purchasers with physical access to another person's mobile device to install an app and surreptitiously monitor them, while allegedly failing to take reasonable data security measures and investigate a cyber incident (for more information, search [FTC Announces Settlement Banning "StalkerApp" SpyFone and Ordering Deletion of All Data](#) on Practical Law).

In 2021, the FTC and observers also engaged in various discussions on its rulemaking authority, including the potential to promulgate data protection regulations, and its options for seeking monetary relief for consumers harmed by unfair or deceptive trade practices following the US Supreme Court's decision in *AMG Capital Management* (see below *Privacy-Related Supreme Court Decisions*).

### HHS

HHS's Office for Civil Rights (OCR) provides guidance and takes enforcement actions under HIPAA and its related regulations.



Search [HIPAA and Health Information Privacy Compliance Toolkit](#) for a collection of resources to assist counsel in HIPAA compliance and enforcement matters.

### HHS Guidance

In 2021, HHS:

- Offered guidance about the interplay between disclosures of an individual's COVID-19 vaccination status and the HIPAA Privacy Rule, focusing on covered entities versus other organizations or individuals (for more information, search [HHS Addresses HIPAA Privacy and COVID-19 Vaccinations in the Workplace](#) on Practical Law).
- Announced that OCR will exercise its enforcement discretion and not impose penalties for HIPAA violations related to good faith use of online scheduling for individual COVID-19 vaccine appointments (Press Release, HHS, OCR Announces Notification of Enforcement Discretion for Use of



Online or Web-Based Scheduling Applications for the Scheduling of COVID-19 Vaccination Appointments (Jan. 19, 2021), available at [hhs.gov](https://www.hhs.gov)).

### HHS Enforcement Activity

In early 2021, the Fifth Circuit issued a potentially wide-reaching decision when it vacated a \$4.3 million assessment, finding that OCR had misinterpreted its encryption and disclosure rules and acted arbitrarily in assessing the penalties (*Univ. of Tex. M.D. Anderson Cancer Ctr. v. U.S. Dep't of Health & Human Servs.*, 985 F.3d 472, 476-81 (5th Cir. 2021)); for more information, search [Fifth Circuit: HHS's HIPAA Enforcement Was "Arbitrary, Capricious, and Contrary to Law"](#) on Practical Law).

OCR also settled several notable HIPAA enforcement actions in 2021, highlighting that companies should:

- **Conduct a thorough risk analysis and implement effective safeguards.** For example:
  - Peachstate Health Management, LLC, a clinical laboratory, agreed to pay \$25,000, implement a robust corrective action plan, and retain an independent monitor for alleged systemic non-compliance with the HIPAA Privacy and Security Rules (Press Release, HHS, Clinical Laboratory Pays \$25,000 to Settle Potential HIPAA Security Rule Violations (May 25, 2021), available at [hhs.gov](https://www.hhs.gov)); and
  - Excellus Health Plan, Inc. agreed to pay \$5.1 million, implement corrective actions, and submit to monitoring following a cyberattack that compromised more than 9.3 million individuals' protected health information (PHI) (Press Release, HHS, Health Insurer Pays \$5.1 Million to Settle Data Breach Affecting Over 9.3 Million People (Jan. 15, 2021), available at [hhs.gov](https://www.hhs.gov)).
- **Support required patient access to PHI.** OCR continued increased enforcement under its HIPAA Right of Access Initiative throughout 2021, culminating in its 25th related action on November 30 (Press Release, HHS, Five Enforcement Actions Hold Healthcare Providers Accountable for HIPAA Right of Access (Nov. 30, 2021), available at [hhs.gov](https://www.hhs.gov)).

### DEPARTMENT OF COMMERCE AND NIST

In October 2021, the Department of Commerce's Bureau of Industry and Security released an interim final rule establishing export controls on certain cybersecurity tools that can support malicious activities (86 FR 58205-02 (Oct. 21, 2021)).

NIST maintained its leadership role in setting cybersecurity and privacy standards. Some notable 2021 NIST guidance and standards addressed:

- **Differential privacy.** NIST highlighted related privacy and data security risks, issues, and methods in its ongoing Differential Privacy Blog Series (NIST, Privacy Engineering Program, Differential Privacy Blog Series, available at [nist.gov](https://nist.gov)).

- **Internet of things (IoT) cybersecurity.** NIST issued guidance to:

- help federal agencies extend their risk management processes to IoT device procurement (NIST Special Publication (SP) 800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements (Nov. 2021), available at [csrc.nist.gov](https://csrc.nist.gov)); and
- provide IoT device manufacturers and others with a framework for developing non-technical cybersecurity-supporting controls, such as documentation and consumer education programs (NISTIR 8259B, IoT Non-Technical Supporting Capability Core Baseline (Aug. 2021), available at [csrc.nist.gov](https://csrc.nist.gov)).

- **Operational technology (OT) and industrial control systems (ICS) security.** NIST continued its work with additional emphasis following the widely reported ransomware attack on Colonial Pipeline, including by:

- releasing a practice guide on monitoring information exchanges among commercial- and utility-scale distributed energy resources and electric distribution grid operations and protecting them from certain cybersecurity threats and vulnerabilities (NIST SP 1800-32, Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity (Feb. 2022), available at [csrc.nist.gov](https://csrc.nist.gov));
- initiating a pre-draft call for comments on planned updates to its guide on cybersecurity risks associated with industrial control systems (NIST SP 800-82 (Rev. 3) (Draft), PRE-DRAFT Call for Comments: Guide to Industrial Control Systems (ICS) Security (Apr. 23, 2021), available at [csrc.nist.gov](https://csrc.nist.gov)); and
- developing an infographic with CISA on quick steps for managing control system cybersecurity risks (NIST, Cybersecurity Insights, NIST Releases Tips & Tactics for Control System Cybersecurity (June 9, 2021), available at [nist.gov](https://nist.gov)).

- **Supply chain risk management.** NIST offered guidance supporting Executive Order (EO) 14028 (for more information, search [President Biden Issues Cybersecurity Executive Order](#) on Practical Law), including by:

- defining EO-critical software (NIST, Critical Software - Definition & Explanatory Material, available at [nist.gov](https://nist.gov));
- publishing guidance on security measures for critical software use (NIST, Security Measures for "EO-Critical Software" Use, available at [nist.gov](https://nist.gov));
- describing recommendations for software verification techniques (NISTIR 8397, Guidelines on Minimum Standards for Developer Verification of Software (Oct. 2021), available at [nvlpubs.nist.gov](https://nvlpubs.nist.gov)); and
- providing an overview with CISA of software supply chain risks and recommendations on how to identify, assess, and mitigate risks (NIST, Defending Against

Software Supply Chain Attacks (Apr. 2021), available at [cisa.gov](https://www.cisa.gov)).

Other related topics from NIST's 2021 work included the migration to post-quantum computing cryptography, automation for security controls assessments, and information exchange security.

In early 2022, NIST announced additional guidance in support of EO 14028 (NIST, NIST Issues Guidance on Software, IoT Security and Labeling (Feb. 4, 2022), available at [nist.gov](https://www.nist.gov)).

## FCC

The Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) (Pub. L. No. 116-105) gave the FCC additional tools to combat unwanted robocalls under the Telephone Consumer Protection Act (TCPA). The FCC issued guidance and took various robocall-related actions in 2021, including by:

- Shortening the time for certain small voice service providers to implement caller ID authentication STIR/SHAKEN standards, following evidence that several small voice service providers generate an increasing share of illegal robocalls (*In re Call Authentication Trust Anchor*, 2021 WL 5922842 (F.C.C. Dec. 10, 2021)).
- Launching the Reassigned Numbers Database, requiring providers to report, on a monthly basis, permanently disconnected numbers and offering a TCPA safe harbor for users (for more information, search [FCC Launches Reassigned Numbers Database to Further Combat Unwanted Robocalls](#) on Practical Law).
- Issuing its largest-to-date fine on March 17, 2021 against health insurance telemarketers for making approximately one billion illegally spoofed robocalls (*In re John C. Spiller*, 2021 WL 1056077 (F.C.C. Mar. 18, 2021); for more information, search [FCC Issues Record \\$225 Million Fine Against Telemarketers for Making One Billion Spoofed Robocalls](#) on Practical Law).

Responding to recent telecommunications industry data breaches, in January 2022, FCC Chair Jessica Rosenworcel informally circulated a Notice of Proposed Rulemaking to strengthen the FCC's data breach notification rules for incidents that affect customer proprietary network information (CPNI) (FCC, Chair Rosenworcel Circulates New Data Breach Reporting Requirements (Jan. 12, 2022), available at [fcc.gov](https://www.fcc.gov)).

## STATE GUIDANCE, REGULATION, AND ENFORCEMENT

Key 2021 regulatory developments at the state level included:

- Further rulemaking under the California Consumer Privacy Act of 2018 (CCPA) and California Consumer Privacy Rights Act of 2020 (CPRA).

- Continued enforcement trends focused on data breaches and insufficient security measures.



Search [Trends in Privacy and Data Security: 2021](#) for more on state regulatory developments and enforcement actions, including efforts related to children's privacy and multistate cooperation.

## CCPA/CPRA REGULATORY DEVELOPMENTS

In 2020, the California Attorney General (CAG) released final CCPA implementing regulations, after extensive proposal and commenting activities (Cal. Code Regs., tit. 11, §§ 999.300 to 999.337). However, the CAG has continued to refine them and, in 2021, issued updated regulations that notably:

- Ban so-called "dark patterns" that delay or obscure the process for consumers to opt out of the sale of personal information.
- Provide businesses with an optional Privacy Options icon to communicate privacy choices to consumers.

(For more information, search [California OAL Approves Additional CCPA Regulations](#) on Practical Law.)

In March 2021, California Governor Gavin Newsom and other officials announced the establishment of the inaugural board for the California Privacy Protection Agency (CPPA) (Press Release, Office of Governor, California Officials Announce California Privacy Protection Agency Board Appointments (Mar. 17, 2021), available at [gov.ca.gov](https://www.gov.ca.gov)). The CPPA is a new administrative agency created under the CPRA, which directs the CPPA to adopt final implementing regulations by July 1, 2022 (Cal. Civ. Code § 1798.185(d)). The new agency released in September an invitation for preliminary comments on its CPRA rulemaking (CPPA, Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01-21) (Sept. 22, 2021), available at [cppa.ca.gov](https://www.cppa.ca.gov)).

Other 2021 CCPA-related developments from the CAG include:

- Updated CCPA FAQs signaling approval of the Global Privacy Control (GPC) standard (for more information, search [Updated CCPA FAQs Approve Use of Global Privacy Control Standard](#) on Practical Law).
- A report on enforcement actions noting that on receiving a notice of alleged violation, 75% of businesses acted to come into compliance within the 30-day statutory cure period, and a CAG-provided interactive tool for consumers to report CCPA noncompliance to businesses (Press Release, California Department of Justice, Attorney General Bonta Announces First-Year Enforcement Update on the California Consumer Privacy Act, Launches New Online Tool for Consumers to Notify Businesses of Potential Violations (July 19, 2021), available at [oag.ca.gov](https://www.oag.ca.gov)).

## DATA BREACH AND CYBERSECURITY ENFORCEMENT ACTIONS

State regulators continued to focus their enforcement efforts on large-scale data breaches and safeguards deemed inadequate to meet their reasonableness standards, with some notable actions in:

- Colorado, which settled with a construction company for more than \$63,000 and promises to institute an information security plan and data disposal policy. When phishing attackers targeted the company in October 2018, it allegedly did not have a data disposal policy and some employees had stored customers' personal information in their email accounts for as long as 20 years. (Press Release, C.O. Office of the Att'y Gen., Colorado Reaches Agreement with Colorado-Based Construction Company that Failed to Protect the Data of Nearly 2,000 People (Nov. 8, 2021), available at [coag.gov](https://coag.gov).)
- New Jersey, which took actions that included alleged HIPAA violations, reaching:
  - a \$425,000 settlement with three cancer care providers following events that exposed personal information and PHI of 105,200 individuals, including 80,333 residents (Press Release, N.J. Office of the Att'y Gen., New Jersey Health Care Providers Will Adopt New Security Measures and Pay \$425,000 to Settle Investigation into Two Data Breaches (Dec. 15, 2021), available at [njoag.gov](https://njoag.gov)); and
  - a \$495,000 settlement with an infertility clinic, following a data breach that compromised the personal information and PHI of 14,663 patients (Press Release, N.J. Office of the Att'y Gen., Acting AG Bruck Announces Settlement with Fertility Clinic over Cybersecurity Lapses and Data Breach (Oct. 12, 2021), available at [njoag.gov](https://njoag.gov)).
- New York, which:
  - settled with an online water filtration retailer for \$200,000 to resolve allegations stemming from a 2019 data breach that compromised the personal information of approximately 320,000 nationwide consumers and 16,500 residents (Press Release, N.Y. Office of the Att'y Gen., Attorney General James Announces Agreement with Filters Fast After 2019 Data Breach (May 18, 2021), available at [ag.ny.gov](https://ag.ny.gov)); and
  - through the New York Department of Financial Services (NYDFS), reached settlements ranging from \$1.5 million to \$3 million in three separate actions, highlighting the need to use multifactor authentication and engage in appropriate risk assessments (see Press Releases, NYDFS, DFS Superintendent Lacewell Announces Cybersecurity Settlement with Licensed Insurance Company (Apr. 14, 2021) and Dep't of Financial Services Announces Cybersecurity Settlement with Mortgage Lender (Mar. 3, 2021), available at [dfs.ny.gov](https://dfs.ny.gov); for more information, search [NYDFS Announces \\$1.8 Million Settlement with Unum Group Insurers](#) on Practical Law).

## PRIVATE LITIGATION

Private litigation highlights and trends from 2021 focused on:

- Several notable data privacy-related Supreme Court decisions.
- Data breach actions.
- Biometrics, especially under Illinois law.




Search [Trends in Privacy and Data Security: 2021](#) for more on notable cases, including data breach-related class settlements, data privacy settlements, TCPA litigation, and additional causes of action.

## PRIVACY-RELATED SUPREME COURT DECISIONS

In 2021, the Supreme Court issued decisions addressing:

- **Article III standing in cases asserting intangible statutory harms.** In *TransUnion LLC v. Ramirez*, the Court narrowed the baseline for Article III standing by holding that in a damages class action, class members must show concrete and particularized harm. The case involved claims that a credit bureau's failure to use reasonable procedures led to an inaccuracy in the plaintiffs' credit reports. The Court held that putative class members who were incorrectly listed as terrorists on their credit reports did not suffer a sufficiently concrete injury unless those reports were disseminated to a third party. (141 S. Ct. 2190 (2021); for more information, search [Supreme Court: Every Damages Class Member Must Show Concrete and Particularized Harm to Establish Article III Standing](#) on Practical Law.) Proposed federal privacy legislation that contains a private right of action may face similar standing issues, depending on the types of harm contemplated. This narrowing of Article III standing also may push more privacy-related suits into state court.
- **The FTC's enforcement powers.** In *AMG Capital Management, LLC v. FTC*, the Court held that Section 13(b) of the FTC Act, which authorizes the FTC to seek a permanent injunction for unfair or deceptive acts or practices, does not authorize the FTC to seek, or a court to award, equitable monetary relief such as restitution or disgorgement. The Court's decision compels the FTC to use certain administrative proceedings to obtain those forms of relief as otherwise outlined in the FTC Act. (141 S. Ct. 1341 (2021).) The *AMG Capital Management* decision has the potential to affect privacy and data security-related actions because the FTC has long used Section 13(b) to obtain relief for consumer harm in various areas.
- **The scope of the Computer Fraud and Abuse Act (CFAA).** In *Van Buren v. United States*, the Court resolved a circuit split and narrowed the CFAA's scope by holding that "exceeding authorized access" covers those who obtain information from areas of a computer that are off limits to them, not those who have valid access to but improper purposes for accessing the



**Standing remained a key issue in 2021 for data breach actions in federal courts. Some courts found that plaintiffs could not satisfy the injury-in-fact requirement to sustain Article III standing where there was no evidence that the plaintiff's information was used fraudulently or improperly accessed.**

information they obtain (141 S. Ct. 1648 (2021)); for more information, search [Supreme Court Resolves Circuit Split Narrowing Scope of CFAA Unauthorized Access](#) on Practical Law). The Court later remanded *LinkedIn Corp. v. hiQ Labs, Inc.*, which addresses the growing issue of whether the CFAA provides a cause of action against organizations that scrape data from publicly available websites contrary to their terms of use, to the Ninth Circuit for further consideration in light of *Van Buren* (141 S. Ct. 2752 (2021)).

- **The definition of an automatic telephone dialing system (ATDS) under the TCPA.** The Court resolved a circuit split concerning whether ATDSs include any device that can store and automatically dial telephone numbers, even if the device does not use a random or sequential number generator. The Court took the narrower view, holding that a necessary feature of an autodialer under 47 U.S.C. § 227(a)(1)(A) is the capacity to use a random or sequential number generator to either store or produce phone numbers to be called. (For more information, search [Supreme Court Reverses Ninth Circuit and Defines ATDS Under the TCPA](#) on Practical Law.)

#### DATA BREACH LITIGATION

Standing remained a key issue in 2021 for data breach actions in federal courts. Some courts found that plaintiffs could not satisfy the injury-in-fact requirement to sustain Article III standing where there was no evidence that the plaintiff's information was used fraudulently or improperly accessed. For example, in:

- *Tsao v. Captiva MVP Restaurant Partners, LLC*, the Eleventh Circuit affirmed the dismissal of a customer's proposed class action against fast food chain PDQ over a data breach, rejecting the argument that an increased risk of identity theft was a concrete injury sufficient to confer Article III standing (986

F.3d 1332 (11th Cir. 2021)); for more information, search [No Standing for Data Breach Claims Without Specific Risks or Data Misuse: Eleventh Circuit](#) on Practical Law).

- *McMorris v. Carlos Lopez & Associates, LLC*, the Second Circuit:
  - laid out three factors for courts to consider when determining whether data breach claims warrant standing; and
  - affirmed a lack of standing because the plaintiffs failed to allege that they were at a substantial risk of future identity theft or fraud sufficient to establish Article III standing.

(995 F.3d 295 (2d Cir. 2021)); for more information, search [Unauthorized Disclosure of Sensitive Data May Establish Article III Standing: Second Circuit](#) on Practical Law.)

Other notable 2021 data breach litigation addressed some contours of a CCPA settlement following a data breach. In *Atkinson v. Minted, Inc.*, a California district court granted preliminary approval to a \$5 million settlement of CCPA and related claims after online marketplace Minted, Inc. suffered a data breach and allegedly failed to respond to the notice to cure sent by the plaintiffs under Cal. Civ. Code § 1798.150 (2021 WL 6028374 (N.D. Cal. Dec. 17, 2021)).

The year also continued a steady stream of data breach-related class settlements, with notable cases involving:

- Equifax, which gained district court approval of its \$380.5 million settlement of hundreds of consumer data breach class action suits in 2019. The settlement was upheld by the Eleventh Circuit (*In re Equifax, Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247 (11th Cir. 2021)).



- Zoom Video Communications, Inc., which agreed to an \$85 million settlement and to make certain security and complaint review upgrades (*In re Zoom Video Commc'ns, Inc. Privacy Litig.*, No. 20-02155 (N.D. Cal. Oct. 21, 2021)).
- Capital One Financial Corp., which agreed to a proposed \$190 million settlement stemming from a 2019 breach that affected over 100 million people and was allegedly caused by a former employee of the bank's cloud services provider (*In re Capital One Customer Data Sec. Breach Litig.*, No. 19-2915 (E.D. Va. Dec. 12, 2021)).



Search [Key Issues in Consumer Data Breach Litigation](#) for more on data breach litigation issues, including applicable law and recovery theories, the roles of harm and standing, class certification, and settlement considerations.

Search [Data Breaches: The Attorney-Client Privilege and the Work Product Doctrine](#) for information on protecting the attorney-client privilege following a data breach, including 2021 case developments.

## BIOMETRIC INFORMATION PRIVACY ACT LITIGATION

Litigation under the Illinois Biometric Information Privacy Act (BIPA) (740 ILCS 14/1) remained robust in 2021. These lawsuits often target employers using biometric timekeeping systems, especially following the Illinois Supreme Court's 2019 ruling that BIPA does not require an injury beyond a statutory violation to sustain a private action (for more information, search [Illinois Supreme Court Rules Biometric Information Privacy Act Lawsuits Do Not Require Actual Injury](#) on Practical Law). In 2021, the parties in that landmark BIPA case reached a \$36 million settlement covering 1.1 million class members, one of the largest BIPA class action settlements (*Rosenbach v. Six Flags Entm't Corp.*, No. 16-13 (Ill. Cir. Ct. 19th Dist. Oct. 29, 2021)).

Likely to further increase employer-targeted suits, in early 2022, the Illinois Supreme Court ruled that the Illinois workers' compensation law does not preclude damages under BIPA because the two laws address distinct harms (for more information, search [Illinois Supreme Court Holds Workers' Compensation Act Does Not Preempt BIPA Claims](#) on Practical Law).

Some other 2021 BIPA developments concerned:

- **Applicable statutes of limitation.** In *Tims v. Black Horse Carriers, Inc.*, involving alleged BIPA violations when collecting employees' fingerprints for timekeeping purposes, an Illinois appellate court held that:
  - 735 ILCS 5/13-201, which sets a one-year limitations period, governs actions under BIPA Sections 15(c) and (d) for claims alleging unlawful profiting or disclosure; and
  - 735 ILCS 5/13-205, which sets a five-year limitations period, governs actions under BIPA Sections 15(a), (b), and (e) for claims alleging data retention policies, informed consent, and safeguarding violations. (2021 IL App (1st) 200563 (Ill. App. Sept. 17, 2021).)

- **When claims accrue.** An Illinois appellate court held that BIPA claims accrue with each scan of the plaintiff's biometric information, not just the first alleged violation (*Watson v. Legacy Healthcare Fin. Servs., LLC*, 2021 IL App (1st) 210279 (Ill. App. Dec. 15, 2021)). The Illinois Supreme Court may soon resolve the issue of whether BIPA claims accrue only once or repeatedly because the Seventh Circuit declined to rule on the issue and certified the question to the Illinois high court in *Cothron v. White Castle System, Inc.* (20 F.4th 1156 (7th Cir. 2021)).
- **Insurance coverage.** In *West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan, Inc.*, the Illinois Supreme Court ruled that a BIPA defendant's insurer had a duty to defend because the complaint's third-party disclosure allegations potentially fell within the policies' personal or advertising injury coverage, and the violations of statutes exclusion for distinguishable federal privacy laws like the TCPA did not apply to the BIPA claims at issue (2021 IL 125978 (Ill. May 20, 2021)).

Organizations with connections to Illinois should carefully consider their practices for collecting and using biometric information.



Search [US Privacy Litigation: Overview](#) for more on BIPA litigation.

## FEDERAL LEGISLATION


Despite debating multiple bills, Congress again failed to pass comprehensive data privacy legislation in 2021, still disagreeing on the extent of federal preemption of state laws and the inclusion of a private right of action.

However, some narrowly focused federal laws enacted in 2021 include:

- The omnibus 2021 National Defense Authorization Act (Pub. L. 116-283 (Jan. 1, 2021)), which includes the Anti-Money Laundering Act of 2020 and the Corporate Transparency Act. Both Acts made major changes to federal anti-money laundering (AML) laws, including establishing a whistleblower protection program. (For more information, search [Senate and House Override Veto and Pass 2021 National Defense Authorization Act with Significant AML Updates](#) on Practical Law.)
- Legislation amending the Health Information Technology for Economic and Clinical Health Act to require HHS to consider whether HIPAA covered entities and business associates have implemented certain recognized security practices when taking enforcement actions (Pub. L. No. 116-321 (Jan. 5, 2021); for more information, search [Legislation Requires HHS to Consider Entities' Cybersecurity Practices in Enforcing HIPAA](#) on Practical Law).
- The Secure Equipment Act of 2021 (Pub. L. No. 117-55 (Nov. 11, 2021)), requiring the FCC to make specified rules regarding communications supply chain security.



Senators also introduced and considered a bipartisan bill to update and expand COPPA (S. 1628 - Children and Teens' Online Privacy Protection Act, available at [congress.gov](https://www.congress.gov)).

 Search [Federal Privacy-Related Legislation Tracker](#) for updates on the progress of various federal data privacy-related bills.

## STATE LEGISLATION


Following the CCPA/CPRA's enactment and in the absence of comprehensive federal legislation, many state legislatures have or are currently considering bills to strengthen consumer data protection. In 2021, the Uniform Law Commission (ULC) also approved a model personal data protection act, which has already influenced some states' early 2022 legislative activities (see ULC, Personal Data Protection Act, available at [uniformlaws.org](https://uniformlaws.org)). Other efforts continue to target specific sectors or data types.

New comprehensive state data privacy laws and continuing implementation activities included those in:

- **California.** Rulemaking efforts for the CCPA/CPRA continued and initial enforcement trends emerged throughout 2021. California also enacted several clarifying amendments. (For more information, search [California Privacy-Related Legislation Tracker](#) on Practical Law.)
- **Virginia.** In March 2021, Virginia became the second state to enact a comprehensive data privacy law. The Virginia Consumer Data Protection Act (VCDPA) (SB 1392) takes effect on January 1, 2023. It does not contain a private right of action, instead granting enforcement authority to the attorney general. (Virginia's Legislative Information System, SB 1392 Consumer Data Protection Act; Establishes a Framework for Controlling and Processing Personal Data, available at [lis.virginia.gov](https://lis.virginia.gov); for more information, search [Virginia Enacts Consumer Data Protection Act](#) on Practical Law.)
- **Colorado.** In July 2021, Colorado Governor Jared Polis signed the Colorado Privacy Act (CPA) (SB21-190), making Colorado the third state to enact a comprehensive consumer data privacy law. The CPA takes effect on July 1, 2023. It contains no private right of action and grants enforcement authority to the attorney general or district attorneys. (Colorado General Assembly, SB21-190, Protect Personal Data Privacy, available at [leg.colorado.gov](https://leg.colorado.gov); for more information, search [Colorado Enacts Privacy Act](#) and [Colorado Attorney General Releases Guidance on Data Security Practices and the Colorado Privacy Act](#) on Practical Law.)

(For a comparison of the CPRA and the VCDPA, search [Quick Comparison Chart \(CPRA and VCDPA\)](#) on Practical Law.)

Several states also continued the trend of increased data security obligations for insurers, enacting insurance data security laws that generally follow the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law (MDL-668) (NAIC, Insurance Data Security Model Law, available at [content.naic.org](https://content.naic.org)), including Hawaii, Iowa, Maine, Minnesota, North Dakota, Tennessee, and Wisconsin (for more information, search [NAIC Model Data Security Law and State-Specific Implementations](#) on Practical Law).

 Search [Trends in Privacy and Data Security: 2021](#) for more on new and modified state laws, including those addressing data breach notification, genetic information privacy, and other privacy and cybersecurity-related issues.

Search [State Omnibus Privacy Legislation Tracker](#) for updates on the progress of various state comprehensive consumer data privacy and data protection bills.

## INTERNATIONAL DEVELOPMENTS

The global momentum for enacting and enforcing comprehensive data protection laws and regulations continued in 2021, with a sampling of activities that may affect US-based multinationals occurring in:

- **Canada.** Québec adopted Bill 64, which includes significant amendments to the current Québec Act addressing various data protection obligations for businesses and rights for individuals. The transition spreads over three years, with most of the provisions coming into force on September 22, 2023. However, some requirements, including data breach notification, take effect sooner. (National Assembly of Québec, Bill 64, available at [www.publicationsduquebec.gouv.qc.ca](https://www.publicationsduquebec.gouv.qc.ca).)
- **China.** The National People's Congress (NPC) enacted notable new laws in 2021, with regulations emerging, that have potentially wide-ranging effects for businesses, including:
  - the Personal Information Protection Law (PIPL), which the NPC adopted on August 20 and which took effect on November 1, an omnibus privacy law that addresses processing personal information and sensitive personal information, cross-border transfers, government processing, individual rights, and fines for violations, among other things; and
  - the Data Security Law, which the NPC passed on June 10 and which took effect on September 1, that calls for creating a data classification system and imposes significant penalties, including potential business shutdowns, for unauthorized cross-border transfers of certain data designated "core" or "important."
- **The EU.** (See below *EU Developments*.)
- **The UK.** (See below *UK Developments*.)
- **Other countries.** New data protection laws also appeared in various other countries and regions in 2021, including Belarus, the British Virgin Islands,

El Salvador, Rwanda, Thailand (fully effective in 2021), Saudi Arabia, Uganda, and the United Arab Emirates.

### EU DEVELOPMENTS

While 2021 did not offer an EU-US Privacy Shield replacement, EU and US officials released a joint statement in March noting that they are engaged in intensifying negotiations on transatlantic data privacy flows and a new framework that can withstand court challenge (Statement, Intensifying Negotiations on Transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo (Mar. 25, 2021), available at [ec.europa.eu](https://ec.europa.eu)).

In early June 2021, the European Commission announced new standard contractual clauses (SCCs) that reflect requirements under the EU General Data Protection Regulation (GDPR) and the 2020 *Schrems II* decision,

transparency and data security controls, resulting in numerous fines and remediation demands.



Search [GDPR Resources for US Practitioners Toolkit](#) for a collection of resources to assist counsel in advising US-based clients on GDPR compliance.

### UK DEVELOPMENTS

The European Commission adopted adequacy decisions regarding the UK in late June 2021, allowing personal data to continue to flow freely from the EU to the UK post-Brexit. The adequacy decisions include a sunset clause, causing the decisions to expire in four years and requiring an additional future determination.

Beginning in September 2021, the UK Information Commissioner's Office (ICO) was obligated to take its Children's Code into account when considering whether

**State House watching will be warranted again as legislatures are already showing their willingness in early 2022 activities to continue filling the gap left by the absence of federal data privacy regulation.**

including SCCs for cross-border data transfers to third countries and for transfers between controllers and processors. Contracts using the previous SCCs executed before September 27, 2021 remain valid until December 27, 2022 if processing operations remain unchanged and are subject to appropriate safeguards. (For more information, search [European Commission Adopts Final Versions of Standard Contractual Clauses Under EU GDPR](#) on Practical Law.)

The European Data Protection Board (EDPB), comprised of representatives of the EU member states' data protection authorities (DPAs), finalized its recommendations on supplementary measures to assist controllers and processors in the wake of the *Schrems II* ruling (EDPB, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, Version 2.0 (June 18, 2021), available at [edpb.europa.eu](https://edpb.europa.eu)).

The EDPB and member states' DPAs also continued to publish resources offering additional targeted guidance on the GDPR and various technologies. The DPAs' enforcement priorities in 2021 generally focused on

an online service has complied with its GDPR and other data protection obligations (ICO, Age Appropriate Design: A Code of Practice for Online Services, available at [ico.org.uk](https://ico.org.uk)).

The ICO imposed several significant penalties for data protection violations, including those against:

- Clearview AI, Inc., provisionally for GBP 17 million, based on its alleged failure to comply with UK data protection laws by not processing individuals' biometric information in a way they are likely to expect or that is fair (Press Release, ICO, ICO Issues Provisional View to Fine Clearview AI Inc. Over £17 million (Nov. 29, 2021), available at [ico.org.uk](https://ico.org.uk)).
- American Express Services Europe Limited, for GBP 90,000, based on its more than four million marketing emails to customers without appropriate consent (Press Release, ICO, Amex Fined for Sending Four Million Unlawful Emails (May 20, 2021), available at [ico.org.uk](https://ico.org.uk)).

The UK Supreme Court also issued a long-awaited decision in *Lloyd v Google LLC* [2021] UKSC 50, restricting claimants' ability to bring data privacy class actions in

the UK under the previous Data Protection Act 1998. The Court did not consider the differences in language under the GDPR.

## LOOKING FORWARD

Data privacy compliance will remain a priority and challenge for many organizations, with a special focus on the GDPR, the CCPA, and advance preparation for the 2023 compliance dates for the VCDPA, CPA, and many CPRA provisions. While most of the CPRA provisions do not become operative until January 1, 2023, the law contains a longer look-back provision for the personal information that consumer access requests may cover, spurring covered entities to address compliance early in 2022.

Companies must hone their compliance procedures and carefully watch privacy and data security enforcement, litigation, and other related trends, including:

- Tracking the FTC's evolving priorities, which, according to a 2021 report to Congress, include a closer look at how market power may enable privacy violations and competitive advantages may come through deceptive statements about data privacy practices (FTC, FTC Report to Congress on Privacy and Security (Sept. 13, 2021), available at [ftc.gov](https://www.ftc.gov)). The FTC has also indicated that it is considering undertaking additional studies on technology industry privacy practices under Section 6(b) of the FTC Act and conducting its own rulemaking regarding digital privacy abuses and algorithmic decision-making that may result in unlawful discrimination.
- Increasing their engagement with industry-specific information sharing and analysis organizations (ISAOs) and suitable public-private cybersecurity programs to share substantive cyber threat information, given the increasing speed of hackers' identifying cyber vulnerabilities and adapting to current cyber defenses.

State House watching will be warranted again as legislatures are already showing their willingness in early 2022 activities to continue filling the gap left by the absence of federal data privacy regulation.

Additional privacy and data security issues likely to receive particular attention in 2022 include:

- **Cross-border data transfers.** Many organizations, including large multinational companies and small-to-medium sized entities, likely engage in some cross-border data transfers and must continue to assess the nature of their lawful options under the GDPR, particularly given the increasing fines issued by EU DPAs. In particular, those entities using the old SCCs must digest the updated SCCs and integrate them into current or new contracts with customers, suppliers, and affiliates, or use an alternative data transfer mechanism.
- **Mobile data privacy.** Location data remains more valuable to marketers and other commercial entities,

even as the mobile platforms and certain apps have tightened developers' data collection and privacy notification practices amid increased scrutiny. With the growth of fintech and money transfer apps offering digital services that integrate with users' financial accounts, financial transactions data is another type of highly sought-after information, which may generate additional privacy-related litigation in the coming year.

- **Sector-specific and online cyber risks.** Sophisticated cyber intrusions from non-US hackers and ransomware attacks remain a serious concern for 2022, with many organizations dedicating more resources to their own cybersecurity practices and those of their vendors. Certain sectors that hold especially valuable personal data, such as health care and financial services, including retirement plan providers, and widely used third-party software services will remain key targets for bad actors. Additional high-risk attack targets include utilities and critical infrastructure, remote workers and contractors, sports betting and online gambling platforms and user accounts, and insecure IoT devices. Beyond cyber intrusions, 2021 also showed certain privacy harms that can arise from mass scraping attacks on publicly available websites, which may only increase.
- **Cryptocurrency and digital assets as cybercrime targets.** As cryptocurrencies and digital assets such as non-fungible tokens (NFTs) garner more mainstream acceptance, hackers have increasingly targeted online trading platforms, digital wallet applications, and decentralized autonomous organizations (DAOs) and engineered user account takeovers to steal valuable digital currencies. Holders of crypto and digital assets, as well as platforms, must maintain careful safeguards and control procedures to prevent theft or intrusions. This need has also spawned institutions that offer secure digital asset custody services and offline "cold" wallet storage of digital currency. Given the Biden administration's cybersecurity focus and the enhanced AML laws, there will likely be increased Treasury Department oversight and regulation of virtual currency platforms to curb their use by cybercriminals.
- **Increased government cybersecurity regulations and standards.** In recent years, important cybersecurity guidance and regulations have emerged, including the NYDFS Cybersecurity Regulation and other state-level regulations, as well as executive orders and laws governing cybersecurity standards for federal agency procurement of certain technologies. Just in the past year, we saw new cybersecurity guidance from the Department of Labor and increased SEC scrutiny of public companies over certain cybersecurity failures. With the Biden administration and state regulators taking more aggressive steps to tackle ransomware and bolster cybersecurity, it is likely that we will continue to see the release of stricter cybersecurity regulations and increased enforcement. 