THOMSON REUTERS
PRACTICAL LAW™

Trends in Privacy and Data Security: 2021

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

Status: **Published on 22 Feb 2022** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/w-034-2241**
Request a free trial and demonstration at: **us.practicallaw.tr.com/about/freetrial**

An Article addressing key privacy and data security developments in 2021 and likely trends for 2022, including federal and state regulation and enforcement. This Article also discusses private litigation related to data breaches, biometrics, and other privacy-related causes, recent developments in state data breach notification and other privacy and cybersecurity laws, and trends in industry self-regulation and international data protection laws and enforcement.

Reports 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 EU and 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 for decryption keys and promises to avoid disclosing compromised data.

Like 2020's SolarWinds attack disclosure, December 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 Cybersecurity and Infrastructure Security Agency (CISA) offered guidance on applying available patches. 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.

Organizations must keep up with the dynamic and increasing legal obligations governing privacy and data security, understand how they 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 year ahead. Specifically, it addresses:

- Federal and state guidance, regulations, and enforcement actions (see Federal Guidance, Regulation, and Enforcement and State Regulation and Enforcement).
- Private litigation (see Private Litigation).
- Federal and state legislation (see Federal Legislation and State Legislation).
- Industry self-regulation and standards (see Industry Self-Regulation and Guidance).
- 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 (see International Developments).
- Trends likely to gain more attention in 2022 (see Looking Forward).

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

Federal Guidance, Regulation, and Enforcement

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

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

- The Department of Commerce and its National Institute of Standards and Technology (NIST) (see Department of Commerce and NIST).
- The Federal Communications Commission (FCC) (see FCC).
- The Securities and Exchange Commission (see SEC).
- Various other agencies (see Other Federal Regulatory Developments).

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). For more on the FTC's authority and standards, see Practice Note, FTC Data Security Standards and Enforcement.

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, see Legal Update, FTC Amends Safeguards Rule to Strengthen Data Security Obligations.

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.

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. For details, see Legal Update, FTC Warns Health Apps to Comply with its Health Breach Notification Rule and the FTC's early 2022 guidance resources.

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. (See Legal Update, Aristotle Inc. Removed from FTC's COPPA Safe Harbor Program.)

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

- Internet service provider (ISP) data privacy practices (see FTC: A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers).
- Board oversight of data security (see FTC: Corporate boards: Don't underestimate your role in data security oversight).
- Fairness in artificial intelligence (AI) applications (see FTC: Aiming for truth, fairness, and equity in your company's use of AI).

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 (see *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 (see *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

(see *U.S. v. OpenX Techs., Inc.*, No. 21-09693 (C.D. Cal. Dec. 15, 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 (see *U.S. v. Kuuhuub Inc.*, No. 21-01758 (D.D.C. Stipulated Order 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 (see Legal Update, FTC Announces Settlement Banning "StalkerApp" SpyFone and Ordering Deletion of All Data).

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 Supreme Court's decision in *AMG Capital Management* (for more, see 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. For more on HIPAA compliance and enforcement, see HIPAA and Health Information Privacy Compliance Toolkit.

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 (see Legal Update, HHS Addresses HIPAA Privacy and COVID-19 Vaccinations in the Workplace).
- 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.

HHS Enforcement Activity

In early 2021, the US Court of Appeals for 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 (5th Cir. 2021)). For details, see Legal Update, Fifth Circuit: HHS's HIPAA Enforcement Was "Arbitrary, Capricious, and Contrary to 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; 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).
- **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.

Department of Commerce and NIST

In October, 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)). Commerce's NIST component 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.
- **Internet of things (IoT) cybersecurity.** NIST issued:
  - Special Publication (SP) 800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements, which helps federal agencies extend their risk management processes to IoT device procurement; and
  - NISTIR 8259B, IoT Non-Technical Supporting Capability Core Baseline, which provides IoT device manufacturers and others with a framework for

developing non-technical cybersecurity-supporting controls, such as documentation and consumer education programs.

- **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:
  - drafts followed by the early 2022 release of SP 1800-32, Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity;
  - a pre-draft call for comments on its planned updates for SP 800-82 (Rev. 3), Guide to Industrial Control Systems (ICS) Security; and
  - with CISA, Tips & Tactics for Control System Cybersecurity.
- **Supply chain risk management.** NIST offered guidance supporting Executive Order (EO) 14028 (for more, see Legal Update, President Biden Issues Cybersecurity Executive Order), including:
  - Critical Software - Definition & Explanatory Material;
  - Security Measures for "EO-Critical Software" Use;
  - NISTIR 8397, Guidelines on Minimum Standards for Developer Verification of Software; and
  - with CISA, Defending Against Software Supply Chain Attacks.

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 Update: NIST Issues Guidance on Software, IoT Security and Labeling (Feb. 4, 2022)).

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, notably including:

- 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, see Legal Update, FCC Launches Reassigned Numbers Database (RND) to Further Combat Unwanted Robocalls).
- Proposing a $5.1 million fine against a group of lobbyists and political consultants for making unlawful robocalls to wireless phones without prior express consent, marking the first action where the agency was not required to warn robocallers before counting violations toward a proposed fine under the TRACED Act (*In re John M. Burkman, et al.*, 2021 WL 3776700 (F.C.C. Aug. 24, 2021)).
- Sending cease and desist letters to various service providers in March, April, and May demanding that they stop carrying illegal robocall campaigns on their networks.
- Issuing its largest-to-date fine on March 17 against health insurance telemarketers for making approximately one billion illegally spoofed robocalls (*In re John C. Spiller, et al*, 2021 WL 1056077 (F.C.C. Mar. 18, 2021); for more, see Legal Update, FCC Issues Record $225 Million Fine Against Telemarketers for Making One Billion Spoofed Robocalls).
- Issuing a nearly $10 million fine under the Truth in Caller ID Act for using caller ID spoofing and targeting specific communities with pre-recorded messages (*In re Scott Rhodes*, 2021 WL 228066 (F.C.C. Jan. 14, 2021)).

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 effect customer proprietary network information (CPNI).

SEC

The SEC has made cybersecurity an increasing priority since its 2018 guidance update on disclosure obligations for public companies to address cyber risks and incidents in their periodic and other public SEC filings (for more, see Practice Note, Data Security Risk Assessments and Reporting: Public Company Obligations).

In 2021, the SEC:

- Announced its intentions to further focus on cyber disclosures as part of its regulatory agenda, making additional remarks implying potential regulation of companies' cyber risk management practices in

early 2022 (see Legal Updates, Preparing for SEC's Upcoming Proposal on Cyber Risks Disclosures and SEC Chair Gary Gensler Discusses Cybersecurity Governance and Disclosure).

- Took related enforcement actions, including:
  - announcing that it had sanctioned eight firms in three separate actions for alleged failures in their cybersecurity policies and procedures resulting in email account takeovers that exposed customers' personal information at each firm (SEC: SEC Announces Three Actions Charging Deficient Cybersecurity Procedures (Aug. 30, 2021));
  - settling for $1 million with a London-based educational publishing company, alleging that it misled investors about a 2018 student records data breach and had inadequate disclosure controls and procedures in place to ensure company officials were adequately informed (*In re Pearson plc*, Exchange Act Release No. 10963, 2021 WL 3627064 (Aug. 16, 2021));
  - settling for nearly $500,000 with real estate settlement services company First American Financial Corporation over alleged deficient disclosure controls and procedures relating to a cybersecurity vulnerability that exposed customers' personal information (see Legal Update, SEC Settles Cybersecurity Disclosure Control Violations Charges Against Real Estate Settlement Services Company); and
  - settling charges with a Colorado-based registered broker-dealer for allegedly violating federal securities laws on filing Suspicious Activity Reports (SARs) when it detected cybercriminals' attempts to access participant accounts in the employer-sponsored retirement plans it serviced (*In re GWFS Equities, Inc.*, Exchange Act Release No. 91853, 2021 WL 1911733 (May 12, 2021)).

The SEC also settled securities fraud allegations against app market data provider App Annie Inc. for $10 million, marking its first enforcement action against an alternative data provider (*In re App Annie Inc.*, Exchange Act Release No. 92975, 2021 WL 4202225 (Sept. 14, 2021)). For details, see Legal Update, SEC Announces $10 Million Settlement With Alternative Data Firm App Annie.

Other Federal Regulatory Developments

Other federal agencies also increased their privacy and data security activities in 2021. Some notable activities include those from:

- The federal banking regulators, with:
  - the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) issuing a final rule requiring banking organizations to notify authorities of certain material cyber incidents within 36 hours and service providers to notify their banking customers as soon as possible (for details, see Legal Update, Federal Banking Agencies Issue Cyber Incident Notification Requirements);
  - the Federal Reserve System offering a blog post on synthetic identity fraud (The Federal Reserve: Synthetic Identity Fraud: Defined It to Fight It); and
  - the interagency Federal Financial Institutions Examination Council (FFIEC) issuing new authentication and access guidance, stressing that multifactor authentication or similar measures, combined with other layered security controls, can more effectively mitigate risks associated with customer authentication (FFIEC: Authentication and Access to Financial Institution Services and Systems).
- The Department of Defense (DoD) announced the release of its updated Cybersecurity Maturity Model Certification Program (CMMC 2.0) for federal defense contractors. The new standard streamlines and clarifies cybersecurity requirements and increases DoD oversight.
- The Department of Homeland Security, with:
  - CISA continuing to offer cybersecurity advisories, creating anti-ransomware resources, and launching a new joint cyber defense collaborative to coordinate defensive cyber activities across the public and private sectors; and
  - the Transportation Security Administration announcing new cybersecurity requirements for the transportation sector and critical pipeline owners and operators (DHS: DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators (Dec. 2, 2021); see Legal Updates, DHS Announces Cybersecurity Requirements for Pipeline Companies and DHS Announces Second Set of Cybersecurity Requirements for Pipeline Companies).
- The Department of Labor Employee Benefits Security Administration (EBSA) releasing:
  - first-of-its-kind guidance for plan sponsors, plan fiduciaries, record keepers, and plan participants on best practices for maintaining cybersecurity (EBSA: Cybersecurity Program Best Practices); and
  - a companion guide on reviewing service providers (EBSA: Tips for Hiring a Service Provider with Strong Cybersecurity Practices).

- The Department of the Treasury, with:
  - its Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) providing guidance on ransomware and virtual currency sanctions compliance risks (see Legal Update, OFAC Issues Guidance and Updated FAQs on Virtual Currency Sanctions Compliance and FinCEN Issues Updated Advisory on Ransomware); and
  - OFAC adding several virtual currency exchanges and individuals to its sanctions lists for allegedly supporting ransomware attacks (see Legal Update, OFAC Adds Russian-Based Crypto Exchange SUEX OTC and Related Parties to Specially Delegated Nationals (SDN) List Over Ransomware Attacks).
- The National Security Agency (NSA) releasing guidance on implementing a zero trust security model (NSA: Cybersecurity Information Sheet: Embracing a Zero Trust Security Model (February 2021)).
- The White House:
  - issuing Executive Order 14028, Improving the Nation's Cybersecurity (May 12, 2021), imposing new cybersecurity prevention, detection, response, and reporting requirements on federal agencies and certain contractors and software providers, and creating a Cyber Safety Review Board to investigate cyberattacks (for more, see Legal Update, President Biden Issues Cybersecurity Executive Order);
  - through its Office of Management and Budget (OMB) releasing annual Federal Information Security Modernization Act (FISMA) guidance for federal agencies on security practices and reporting, including a mandate to notify CISA and the OMB within one hour of determining that a major cyber incident has occurred (OMB: Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements (Dec. 6, 2021));
  - issuing Executive Order 14034, Protecting Americans' Sensitive Data from Foreign Adversaries (June 9, 2021), replacing a Trump administration order banning certain apps with a criteria-based decision framework; and
  - publishing additional memoranda on anti-ransomware measures companies should take and on critical infrastructure security (see Legal Updates, White House Issues Memo Urging Business Leaders to Improve Ransomware Defenses and White House Issues Memo on Critical Infrastructure Cybersecurity).

State Regulation and Enforcement

State Regulations and Guidance

Key 2021 regulatory developments at the state level included:

- Continued developments surrounding the California Consumer Privacy Act of 2018 (CCPA) and California Consumer Privacy Rights Act (CPRA) (see CCPA/CPRA Regulatory Developments).
- Other developments on ransomware guidance, health privacy, cyber insurance risk, and cyber incident response plans (see Other State-Level Regulatory Developments).

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. The updates notably:

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

For more, see Legal Update, California OAL Approves Additional CCPA Regulations.

In March, California Governor Gavin Newsom and other officials announced the establishment of the inaugural board for the California Privacy Protection Agency (CPPA). 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.

Other 2021 CCPA-related developments from the CAG include:

- Updated CCPA FAQs signaling approval of the Global Privacy Control (GPC) standard (for more, see Legal Update, Updated CCPA FAQs Approve Use of Global Privacy Control Standard).
- 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 (CAG: 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)).

For details on CCPA/CPRA legislative developments, see Comprehensive State Data Privacy Laws.

Other State-Level Regulatory Developments

Other key state-level regulatory developments in 2021 include those from:

- **California.** The California Department of Public Health also updated its data breach reporting requirements for certain licensed health care organizations, better aligning its breach definition with HIPAA's and making clarifications regarding the administrative penalty structure (Cal. Code Regs. title 22, §§ 79901 to 79902). The CAG later issued guidance to health care organizations reminding them of their obligations to comply with state and federal health data privacy laws, including data breach notification requirements, and to continue to monitor government health data security advisories (CAG Bulletin: Obligation to Proactively Reduce Vulnerabilities to Ransomware Attacks and Requirements Regarding Health Data Breach Reporting (Aug. 24, 2021)).
- **Connecticut.** Notably:
  - the Attorney General reminded businesses of their data protection duties in light of increased ransomware attacks (Press Release: AG Tong Alerts Businesses and Government Entities to Take Prompt Action to Protect Operations and Personal Information (July 29, 2021)); and
  - the Insurance Department issued a bulletin offering guidance to covered insurers on complying with the Connecticut Insurance Data Security Law (Conn. Gen. Stat. Ann. § 38a-38) and adding compliance with the New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR §§ 500.0 to 500.23) to Connecticut's list of compliance safe harbors (CT Insurance Dep't: Bulletin IC-43 (Feb. 10, 2021)).
- **Massachusetts.** In light of increased ransomware attacks, the Attorney General reminded businesses of their data protection duties, especially under the Massachusetts Data Security Regulations (201 Code Mass. Regs. 17.01 to 17.05; Press Release: AG Healey Urges Businesses and Government Agencies to Take Immediate Steps to Protect Operations From Ransomware Attacks (June 8, 2021)).
- **New York.** Notably:
  - in early 2022, the Attorney General issued guidance for businesses to protect themselves and their customers' information from credential stuffing cyberattacks following a study identifying affected companies (Press Release: Attorney General James Alerts 17 Companies to "Credential Stuffing" Cyberattacks Impacting More Than 1.1 Million Consumers (Jan. 5, 2022)); and
  - the NYDFS provided guidance on reducing ransomware risks (Press Release: Superintendent Lacewell Announces DFS Issues New Guidance on Ransomware Prevention (June 30, 2021)), offered a Cyber Insurance Risk Framework (Insurance Circular Letter No. 2 (2021): Cyber Insurance Risk Framework (Feb. 3, 2021)), and released a report on the New York financial services industry's response to the SolarWinds supply chain attack (Legal Update, NYDFS Issues Report on SolarWinds Response and Recommends Critical Cybersecurity Measures).

Single-State Enforcement Actions

Key single-state enforcement actions in 2021 focused primarily on:

- Data breaches and insufficient security measures (see Data Breaches and Cybersecurity Failures).
- Children's privacy (see Children's Privacy).

Data Breaches and Cybersecurity Failures

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 for more than $63,000 and promises to institute an information security plan and data disposal policy with a construction company. When phishing attackers targeted it in October 2018, the company 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: Colorado reaches agreement with Colorado-based construction company that failed to protect the data of nearly 2,000 people (Nov. 8, 2021)).
- 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 for 105,200 individuals,

including 80,333 residents (Press Release: New Jersey Health Care Providers Will Adopt New Security Measures and Pay $425,000 to Settle Investigation into Two Data Breaches (Dec. 15, 2021)); 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: Acting AG Bruck Announces Settlement with Fertility Clinic over Cybersecurity Lapses and Data Breach (Oct. 12, 2021)).

- New York, which:
  - settled for $200,000 with an online water filtration retailer to resolve allegations stemming from a 2019 data breach that compromised approximately 320,000 nationwide consumers' and 16,500 residents' personal information (Press Release: Attorney General James Announces Agreement with Filters Fast After 2019 Data Breach (May 18, 2021)); and
  - through the NYDFS, reached settlements ranging from $1.5 to $3 million in three separate actions, highlighting the need to use multifactor authentication and engage in appropriate risk assessments (see Legal Update, NYDFS Announces $1.8 Million Settlement with Unum Group Insurers; Press Release: DFS Superintendent Lacewell Announces Cybersecurity Settlement with Licensed Insurance Company (Apr. 14, 2021); Press Release: Dep't of Financial Services Announces Cybersecurity Settlement with Mortgage Lender (Mar. 3, 2021)).

Children's Privacy

Children's privacy enforcement efforts at the state level also continued with New Mexico taking notable actions that included COPPA claims, specifically:

- Reaching settlements with Google in two separate cases concerning alleged data collection practices for the company's Workspace for Education products (formerly known as G-Suite for Education) and its ad network app labeling practices for child-directed apps. Google agreed in the settlement to fund the Google New Mexico Kids Initiative as well as more actively address app compliance (Press Release: Attorney General Hector Balderas Announces Landmark Settlements with Google Over Children's Online Privacy (Dec. 13, 2021); *New Mexico ex rel. Balderas v. Google, LLC*, No. 20-2172 (10th Cir. Stipulation Dec. 13, 2021)).
- Filing claims against Angry Birds app developer Rovio Entertainment, alleging that the company knowingly collects personal information from children under 13 and discloses it to third party marketing companies for targeted advertising (Press Release: AG Balderas Announces Lawsuit Against Developer of Popular Game Angry Birds for Illegally Collecting Child Data (Aug. 25, 2021); *New Mexico v. Rovio Entm't Corp.*, D.N.M., No. 21-824 (D. N.Mex. filed Aug. 25, 2021)).

Multistate Enforcement Actions

The trend of multistate cooperation in privacy enforcement continued in 2021. For example, a medical collection agency settled with a bipartisan coalition of 41 attorneys general, agreeing to strengthen its information security program and better safeguard consumers' personal information. The action followed a 2018-19 data breach that compromised some 21 million individuals' personal information nationwide. Emerging from bankruptcy due to data breach response-related costs, the company may also be liable for a $21 million payment to the states if it violates the agreement's terms. (Press Release: Attorney General James Holds American Medical Collection Agency Responsible for 2019 Data Breach (Mar. 11, 2021).)

Private Litigation

Private litigation highlights and notable trends for 2021 focused on:

- The Supreme Court's decisions interpreting the FTC's enforcement powers, the scope of the Computer Fraud and Abuse Act (CFAA), and Article III standing in cases asserting intangible statutory harms (see Privacy-Related Supreme Court Decisions).
- Data breach actions and data privacy-related settlements (see Data Breach Litigation and Data Privacy Settlements).
- Biometrics, especially under Illinois law (see Biometric Information Privacy Act Litigation).
- Cases brought under the TCPA (see TCPA Litigation).
- Other privacy and data security-related topics (see Other Notable Cases).

Privacy-Related Supreme Court Decisions

In 2021, the Supreme Court issued several noteworthy data privacy-related 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 (141 S.

Ct. 2190 (2021)). The case involved claims that a credit bureau's failure to use reasonable procedures led to an inaccuracy in 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. 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. For more, see Legal Update, Supreme Court: Every Damages Class Member Must Show Concrete and Particularized Harm to Establish Article III Standing.

- **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 CFAA's scope.** In *Van Buren v. US*, 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 to those who have valid access to but improper purposes for accessing the information they obtain (141 S.Ct. 1648 (2021)). For more, see Legal Update, Supreme Court Resolves Circuit Split Narrowing Scope of CFAA Unauthorized Access. 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 US Court of Appeals for 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 details, see Legal Update, Supreme Court Reverses Ninth Circuit and Defines ATDS Under the TCPA.

Data Breach Litigation

Standing remained a key issue in 2021 for data breach actions in federal courts. For example, 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:

- In *Tsao v. Captiva MVP Restaurant Partners, LLC*, the US Court of Appeals for the Eleventh Circuit affirmed the dismissal of a customer's proposed class action lawsuit 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); see Legal Update, No Standing for Data Breach Claims Without Specific Risks or Data Misuse: Eleventh Circuit).
- Similarly, in *McMorris v. Carlos Lopez & Assoc., LLC*, the US Court of Appeals for the Second Circuit:
  - laid out three factors for courts to consider when determining whether these claims warrant standing; and
  - affirmed a lack of standing because plaintiffs failed to allege that they are at a substantial risk of future identity theft or fraud sufficient to establish Article III standing.

  (995 F.3d 295 (2d Cir. 2021); see Legal Update, Unauthorized Disclosure of Sensitive Data May Establish Article III Standing: Second Circuit.)

Other notable 2021 data breach litigation addressed:

- **Negligence claims in a data breach action.** In *Doe v. Sutherland Healthcare Solutions, Inc.*, a California appellate court allowed negligence claims against a county and medical billing company following a prior data breach involving stolen computers. The court found that no proof of unauthorized access is required for the negligence cause of action, where plaintiffs established triable issues of fact regarding actual damages and causation, even as it dismissed claims under the California Confidentiality of Medical Information Act due to the plaintiffs' lack of evidence that their confidential medical information was compromised (2021 WL 5765978 (Cal. App. Dec. 6, 2021)).

- **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 plaintiffs under Cal. Civ. Code § 1798.150 (2021 WL 2411041 (N.D. Cal. May 14, 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 and saw the settlement upheld by the Eleventh Circuit (*In re: Equifax, Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247 (11th Cir. 2021)).
- Grocery chain Hy-Vee, Inc., which agreed to a $20 million settlement and promises to make significant security upgrades to resolve claims that its alleged inadequate security practices led to a 2019 data breach and stolen credit card information (*Perdue v. Hy-Vee Inc.*, 2021 WL 3081051 (C.D. Ill. July 21, 2021)).
- Zoom Video Communications, Inc., which agreed to an $85 million settlement and agreements to make certain security and complaint review upgrades (*In re: Zoom Video Communications, 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)).

For more on data breach litigation issues, including applicable law and recovery theories, the roles of harm and standing, class certification, and settlement considerations, see Practice Note, Key Issues in Consumer Data Breach Litigation. For details on protecting the attorney-client privilege for materials following a data breach, including some 2021 cases, see Practice Note, Data Breaches: The Attorney-Client Privilege and the Work Product Doctrine: Ensure Third-Party Retainer Agreement and Report Evidence Reasonable Anticipation of Litigation.

Data Privacy Settlements

In 2021, there were several notable settlements concerning data privacy, with claims generally alleging that defendants collect, use, and sell access to consumers' personal data without meaningful notice or choice or proper safeguards, including those with:

- Fintech services company, Plaid, Inc., which agreed to pay $58 million to settle claims surrounding its data collection practices and make certain changes to its methods of notice and consumer data collection, including deleting some banking transaction data (*Cottle v. Plaid Inc.*, 2021 WL 5415252 (N.D. Cal. Nov. 19, 2021)). A similar suit against financial analytics company Envestnet, Inc., which operates Yodlee, Inc., remains ongoing (*Wesch v. Yodlee Inc.*, 2021 WL 1399291 (N.D. Cal. Feb. 16, 2021)).
- The operators of the social media video app TikTok, which agreed to a $92 million settlement and various injunctive relief that includes barring it from storing or transmitting certain user data outside the US, resolving claims that it harvested users' biometric data, geolocation information, personally identifiable information, and unpublished digital recordings. (*In Re: TikTok, Inc., Consumer Privacy Litig.*, 2021 WL 4478403 (N.D. Ill. September 30, 2021)).

Biometric Information Privacy Act Litigation

Litigation under Illinois's Biometric Information Privacy Act (BIPA) (740 ILCS 14/1) remained robust in 2021. 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 (see Legal Update, Illinois Supreme Court Rules Biometric Information Privacy Act Lawsuits Do Not Require Actual Injury). 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 Illinois's workers' compensation law does not preclude damages under BIPA because the two laws address distinct harms (for more, see Legal Update, Illinois Supreme Court Holds Workers' Compensation Act Does Not Preempt BIPA Claims).

Some other notable 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 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 now soon resolve the issue of whether BIPA claims accrue only once or repeatedly because the US Court of Appeals for the Seventh Circuit declined to rule and certified the question to the Illinois high court in *Cothron v. White Castle System, Inc.* (20 F.4th 1156 (7th Cir. Dec. 20, 2021)).
- **Insurance coverage.** In *West Bend Mutual Ins. 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. For more details on BIPA litigation, see Practice Note, US Privacy Litigation: Overview: Illinois Biometric Information Privacy Act (BIPA).

TCPA Litigation

The TCPA regulates how businesses may make certain voice calls and send texts or faxes and provides consent options for some of these communications. For more on the TCPA and compliance obligations, see Practice Notes, Telephone Consumer Protection Act (TCPA): Overview and TCPA Litigation: Key Issues and Considerations.

TCPA litigation continued apace in 2021, including multiple class settlements. Key litigated issued included:

- **The ATDS definition.** Following the Supreme Court's ruling narrowing the ATDS definition, multiple TCPA actions were dismissed for failure to allege that an ATDS made the calls at issue. For more, see Privacy-Related Supreme Court Decisions and cases such as:
  - *Borden v. eFinancial LLC*, 2021 WL 3602479 (D. Wash. Aug. 13, 2021) (on appeal to Ninth Circuit) (failing to allege that eFinancial's system "generate[s] random or sequential phone numbers" to be dialed, but instead showing that plaintiff expressly provided his phone number); and
  - *Timms v. USAA Fed. Savings Bank*, 2021 WL 2354931 (D.S.C. June 9, 2021) (rejecting plaintiff's contention that defendant's system qualified as an ATDS if it used a random number generator to determine the order for picking phone numbers from a preproduced list because the "preproduced list" was not one that was "sequentially generated and stored").
- **Job-recruiting robocalls.** In *Loyhayem v. Fraser Financial and Ins. Services, Inc.*, the Ninth Circuit held that the TCPA prohibits "any call," regardless of content, that is made to a cell phone using an ATDS or an artificial or pre-recorded voice unless the call is made either for emergency purposes or with the prior express consent of the person being called (7 F.4th 1232 (9th Cir. 2021)).
- **Standing.** In *Cranor v. 5 Star Nutrition, L.L.C.*, the Fifth Circuit held that a single unsolicited commercial text message is a concrete injury-in-fact, stating that the scope of the TCPA sought to remediate nuisance and invasion of privacy in a broad set of circumstances (998 F.3d 686 (5th Cir. 2021)). However, in *Leyse v. Bank of America National Ass'n*, the US Court of Appeals for the Third Circuit affirmed dismissal of TCPA claims due to a lack of standing where the plaintiff failed to allege any annoyance or nuisance from a recorded call he received (856 Fed.Appx. 408 (3d Cir. May 19, 2021)).

Other Notable Cases

Other notable privacy and data security-related litigation in 2021 included cases addressing:

- **Call recording consent statutes.** Two state supreme courts interpreted their state's wiretapping laws surrounding alleged unauthorized recording of telephone calls:
  - in *Smith v. Loanme, Inc.*, the California Supreme Court held that the state's telephone call recording statute, Cal. Penal Code §§ 631 to 632, applies to parties to the conversation as well as non-parties to the call, prohibiting them both from recording a covered communication without the consent of all participants (11 Cal.5th 183 (2021)); and
  - in *Curtatone v. Barstool Sports, Inc.*, the Supreme Judicial Court of Massachusetts, in interpreting the state's wiretap statute, M.G.L. c. 272, § 99(B)(4),

found that a politician that had actual knowledge that a telephone interview was being recorded could not state a claim under the wiretap act because the call was neither secret nor an interception, despite the other party having conducted the interview under the guise of being a local newspaper reporter (487 Mass. 655 (June 14, 2021)).

- **Session replay website analytics.** Several courts considered state wiretap and related claims stemming from website operators using vendor-provided session analytics software to record visitor data and activities on the site, including vendor and operator liability. Compare, *Goldstein v. Costco Wholesale Corp.*, 2021 WL 4134774 (S.D. Fla. Sep. 9, 2021) (finding that recordings of plaintiff's purported communications on the site "contained no substance," and therefore, no interception occurred under Florida statute) with *Saleh v. Nike, Inc.*, 2021 WL 4437734 (C.D. Cal. Sep. 27, 2021) (allowing some California state wiretap claims to go forward).
- **Unauthorized access claims.** In *Sartori v. Schrodt*, the Eleventh Circuit affirmed dismissal of CFAA and Stored Communications Act claims, finding that a spouse's access to a shared laptop and online accounts negated any allegations of unauthorized use (2021 WL 6060975 (11th Cir. Dec. 20, 2021)).
- **Arizona's Dealer Law.** In *CDK Global LLC v. Brnovich*, the Ninth Circuit affirmed the denial of a request for a preliminary injunction blocking Arizona's enforcement of its Dealer Law, which aims to:
  - strengthen privacy protections for consumers whose data car dealers collect; and
  - restrict anticompetitive business practices by technology companies that provide database services for dealers.

  (16 F.4th 1266 (9th Cir. Oct. 25, 2021).)

Federal Legislation

Congress again failed to pass comprehensive data privacy legislation in 2021, despite debating multiple bills, 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 included the Anti-Money Laundering (AML) Act of 2020 and the Corporate Transparency Act. Both acts made major changes to federal AML laws, including establishing a whistleblower protection program (for more, see Legal Update, Senate and House Override Veto and Pass 2021 National Defense Authorization Act With Significant AML Updates).
- 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, see Legal Update, Legislation Requires HHS to Consider Entities' Cybersecurity Practices in Enforcing HIPAA).
- 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, The Children and Teens' Online Privacy Protection Act). For more on notable federal privacy-related legislation, see Practice Note, Federal Privacy-Related Legislation Tracker.

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, Virginia and Colorado passed their own comprehensive data privacy laws. The Uniform Law Commission (ULC) in 2021 also approved a model personal data protection act, which has already influenced some states' early 2022 legislative activities (see ULC: Personal Data Protection Act). Other efforts continue to target specific sectors or data types.

For example, states and some local governments focused their efforts in 2021 and continue to do so in early 2022 on:

- Comprehensive data privacy laws and updated data breach notification laws (see Comprehensive State Data Privacy Laws).
- Genetic information privacy (see Genetic Information Privacy).
- Other privacy and cybersecurity-related laws (see Other Privacy and Cybersecurity-Related Laws).

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) Model

Insurance Data Security Law (MDL-668), including Hawaii, Iowa, Maine, Minnesota, North Dakota, Tennessee, and Wisconsin (for more, see Practice Note, NAIC Model Data Security Law and State-Specific Implementations).

Comprehensive State Data Privacy Laws

New comprehensive state data privacy laws for 2021 and continuing implementation activities included those in:

- **California.** Rulemaking efforts for the CCPA/CPRA continued and initial enforcement trends emerged throughout 2021 (see CCPA/CPRA Regulatory Developments). California also enacted several clarifying amendments, including:
  - AB 825, which adds genetic data to the personal information definition used in California's data breach notification law, indirectly expanding the CCPA's private right of action for certain data breaches because it uses that law for its personal information definition;
  - AB 335, which provides an exemption to the CCPA's right to opt-out of personal information sales for vessel or ownership information retained or shared between vessel owners and dealers for certain warranty and repair purposes; and
  - AB 694, which makes technical, non-substantive changes to the CPRA enacting provisions and clarifies that the CPPA's rulemaking authority begins six months after it notifies the Attorney General that it is ready to assume that responsibility.

  To track proposed CCPA/CPRA amendments and additional privacy-related bills pending in the California Legislature for the 2021-2022 session, see California Privacy-Related Legislation Tracker.
- **Virginia.** In March, Virginia became the second state to enact a comprehensive data privacy law. The Virginia Consumer Data Protection Act (VCDPA) (S.B. 1392) takes effect on January 1, 2023. It does not contain a private right of action, instead granting enforcement authority to the attorney general. For details, see Legal Update, Virginia Enacts Consumer Data Protection Act.
- **Colorado.** In July, Colorado Governor Jared Polis signed the Colorado Privacy Act (CPA) (SB 21-190), making Colorado the third state to enact a comprehensive consumer data privacy law. The CPA takes effect on July 1, 2023. It also contains no private right of action and grants enforcement authority to the attorney general or district attorneys. For more, see Legal Updates, Colorado Enacts Privacy Act and Colorado Attorney General Releases Guidance on Data Security Practices and the Colorado Privacy Act.

To track comprehensive state data privacy legislation, see Practice Note, State Omnibus Privacy Legislation Tracker. For a comparison of the CPRA and the VCDPA, see Practice Note, Quick Comparison Chart (CPRA and VCDPA).

Data Breach Notification Laws

Reacting to mega breaches and ongoing cyber threats, some states amended their existing private sector data breach notification laws in 2021, generally extending them. For example:

- California AB 825 added genetic data to the personal information definition used in its data breach notification law, indirectly expanding the CCPA's private right of action for certain data breaches because it uses that law for its personal information definition.
- Connecticut HB 5310 expanded the personal information definition and shortened certain notification deadlines (see Legal Update, Connecticut Amends Data Breach Notification Law).
- Texas HB 3746 requires that the state attorney general publicly post data breach notifications it receives under the data breach notification statute for one year.

For more details on state data breach notification laws, see State Q&A Tool, Data Breach Notification Laws. Some states also expanded data breach and cyber incident notification obligations for state and local government agencies.

Genetic Information Privacy

Several states enacted laws regulating direct-to-consumer genetic testing companies and limiting disclosure of an individual's genetic information. For example:

- **California** passed the Genetic Information Privacy Act (SB 41), which requires direct-to-consumer genetic testing companies to:
  - provide consumers with certain information regarding the company's policies and procedures for the collection, use, maintenance, and disclosure of genetic data; and
  - obtain consumers' express consent for collection, use, or disclosure of their genetic data.

  (For more, see Legal Update, California Enacts Genetic Information Privacy Law, CPRA and CMIA Amendments, and Other Privacy-Related Bills.)
- **South Dakota** enacted SB 178, which prohibits:

  - health, life, and long-term care insurers from requiring an individual or blood relative to take a genetic test in determining eligibility or for certain coverage and underwriting decisions; and
  - direct-to-consumer genetic testing companies from sharing genetic testing or other information with health, life, or long-term care insurers without written consumer consent unless the disclosure is made for limited purposes in compliance with HIPAA.
- **Utah** passed the Genetic Information Privacy Act (SB227), which requires direct-to-consumer genetic testing companies to:
  - provide consumers clear information regarding the company's collection, use, and disclosure of genetic data;
  - obtain consumers' consent, making specified disclosures, for initial collection, uses, or disclosures of genetic data and separate consent for certain future activities;
  - develop, implement, and maintain a comprehensive security program to protect consumers' genetic data;
  - provide consumers with rights of data access and deletion and biological sample destruction; and
  - prohibits disclosure, absent consumer consent, to health, life, or long-term care insurers or the consumer's employer.

Other Privacy and Cybersecurity-Related Laws

Other notable state and local data privacy laws new or updated in 2021 address:

- **Biometric identifiers.** New York City's biometrics identifier law took effect July 9, 2021:
  - requiring specified commercial establishments that collect, retain, or share customers' biometric identifiers, including retina scans, fingerprints, voiceprints, hand scans, facial geometry, or other identifying characteristics, to conspicuously disclose their practices with appropriate signage near the establishment's entrances;
  - barring them from selling, leasing, trading, sharing, or otherwise profiting from the transaction of customers' biometric identifiers; and
  - providing a private right of action.

  (N.Y.C. Admin. Code §§ 22-1201 to 22-1205.)
- **Consumer personal information sales opt-out.** Nevada enacted SB 260, updating the state's current consumer personal information sales opt-out law to address data brokers, broaden the definition of a sale, limit covered businesses' right to cure to first violations, and extend the list of exempted organizations and information (for more, see Legal Update, Nevada Amends Online Privacy Law to Broaden "Sales" Definition and Address Data Brokers).
- **Cybersecurity standards.** For example, some private-sector-affecting laws include:
  - Connecticut passed H.B. 6607, which incentivizes businesses to adopt certain cybersecurity standards by allowing them to plead an affirmative defense to data breach actions that allege a failure to implement reasonable cybersecurity controls (for more, see Legal Update, Connecticut Enacts Law Incentivizing Cybersecurity Program Adoption); and
  - Utah enacted a similar law, the Cybersecurity Affirmative Defense Act (HB 80) that creates an affirmative defense to certain data breach-related actions if the organization maintains and reasonably complies with a specified written cybersecurity program (see Legal Update, Utah Enacts Data Breach Safe Harbor Law).
- **Employee monitoring.** New York passed S2628, which requires private employers to notify employees when electronically monitoring their telephones, emails, and internet access and usage, with some exceptions (see Legal Update, New York State Enacts Employee Monitoring Notice Law).
- **Health data privacy.** For example:
  - California passed AB 1184, which prohibits a health care service plan or insurer from requiring a protected individual to obtain the policyholder or primary subscriber's authorization to receive certain "sensitive services," or services related to sexual or reproductive health care, or to submit a claim for sensitive services if the protected individual has the right to consent to care (see Legal Update, California Enacts Genetic Information Privacy Law, CPRA and CMIA Amendments, and Other Privacy-Related Bills); and
  - Oregon passed HB 3284, which prohibits covered organizations, including those not already subject to other health privacy laws, such as contact tracing apps, from collecting, using, or disclosing data about resident's COVID-19 status or infection without affirmative express consent and imposes other limits and obligations. The statute does not apply to data

collected in an employment context and permits retention of certain de-identified or aggregated data or statistical analyses.

- **Student privacy.** Oklahoma passed HB 1875, which updates its educational records law to prohibit educational agencies and institutions that have lawfully accessed student directory information from releasing or selling it unless authorized under the Family Educational Rights and Privacy Act, its implementing regulations, or Oklahoma law.
- **Telemarketing limits.** Florida amended its telemarketing laws to limit the timing and number of calls to a particular consumer and to require prior express written consent before any telephonic sales calls are made with an automated system (see Legal Update, Florida Legislature Strengthens Existing Telemarketing Laws).
- **Tenant data privacy.** The City of New York enacted N.Y.C. Admin. Code §§ 26-3001 to 26-3007, which requires owners of multiple dwelling buildings that use keyless entry systems to provide tenants with a privacy policy, obtain their consent, implement specified security and data retention measures, and limit data uses (for more, see Legal Update, NYC Enacts Law Protecting Tenant Data Privacy).

Industry Self-Regulation and Guidance

Industry self-regulation and guidance from independent organizations remained important components of the privacy and data security landscape in 2021 across various sectors.

For example:

- The Children's Advertising Review Unit (CARU), one of the self-regulatory units of BBB National Programs, released revised self-regulatory guidelines for children's advertising. The revised guidelines include guidance on current issues such as in-app advertising and purchases and marketing involving endorsements and social media influencers. (CARU: Self-Regulatory Guidelines for Children's Advertising (effective Jan. 1, 2022).)
- The Digital Advertising Alliance (DAA), another BBB National Programs unit, with CARU, took action against a publisher of several children's gaming apps, working to bring its online services into compliance with the DAA Principles after discovering that the apps apparently contained third-party trackers collecting data for interest-based advertising for users under 13 without parental consent (Press Release: Two of BBB National Programs' Self-Regulatory Watchdogs Bring Azerion Gaming Website and App into Compliance with Privacy Best Practices (Mar. 9, 2021)). For more on complying with the DAA Principles and related obligations, see Online Behavioral Advertising Legal Considerations for Advertisers and Website Publishers Checklist.
- The Financial Industry Regulatory Authority (FINRA), which is an industry self-regulator for the broker-dealer industry:
  - issued Regulatory Notice 21-29 reminding member firms of their obligation to establish and maintain a supervisory system to manage the risks of outsourcing to third-party vendors, including cybersecurity issues; and
  - reached a $125,000 settlement with Securities America, Inc. for alleged violations of the SEC's Regulation S-P, claiming that 12 recruited representatives took customers' nonpublic personal information from their former firms and disclosed it a third-party vendor that was assisting them with their transition into Security America (FINRA No. 2019064323201 (Feb. 23, 2021)).
- The Payment Card Industry (PCI) Security Standards Council (SSC), which manages the PCI Data Security Standard (PCI DSS), published remote assessment guidelines that can be followed during and after the pandemic (PCI SSC: Remote Assessment (September 2021)).

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 a wide variety of 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.
- **China.** The National People's Congress enacted notable new laws in 2021, with regulations emerging, that have potentially wide-ranging effect for businesses, including:
  - the Personal Information Protection Law (PIPL), which the National People's Congress (NPC) adopted

on August 20 and which took effect on November 1, is 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, 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 EU Developments).
- **The UK** (see UK Developments).
- **Other countries.** New data protection laws also appeared in a variety of 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 (UAE).

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.

The European Court of Justice (ECJ) July 16, 2020 decision in *Schrems II* invalidating the EU-US Privacy Shield focused primarily on the potential for interference with data subjects' rights by insufficiently limited US government surveillance programs. The ECJ upheld as valid controller-to-processor standard contractual clauses (SCCs) if:

- Data exporters perform case-by-case evaluations to determine if a recipient country's laws, such as government surveillance or reporting requirements, interfere with the ability to meet adequate protection requirements under the EU General Data Protection Regulation (GDPR). Exporters may need to supplement SCCs with additional safeguards, such as technical measures, to ensure they meet GDPR standards.
- Data importers inform data exporters of any inability to comply with the SCCs, at which point the data exporter must suspend data transfers or terminate the SCCs.

In early June, the European Commission announced new SCCs that reflect requirements under the GDPR and the *Schrems II* decision, 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, see Legal Update, European Commission adopts final versions of standard contractual clauses under EU GDPR.)

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 (June 18, 2021)).

The EDPB and member states' DPAs also continued to publish a wide variety of resources, offering additional targeted guidance on the GDPR and various technologies. The DPAs enforcement priorities in 2021 generally focused on transparency and data security controls, resulting in a variety of fines and remediation demands. For more on GDPR compliance, see GDPR Resources for US Practitioners Toolkit.

UK Developments

The European Commission adopted adequacy decisions regarding the UK in late June, 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, the UK's Information Commissioner's Office's (ICO) was obligated to take its Children's Code into account when considering whether an online service has complied with its GDPR and other data protection obligations (see ICO: Age appropriate design: a code of practice for online services).

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

- Clearview AI, Inc., provisionally for GBP17, based on its alleged failure to comply with UK data protection laws by processing individuals' biometric information in a way they are likely to expect or that is fair (Press Release: ICO issues provisional view to fine Clearview AI Inc over £17 million (Nov. 29, 2021)).
- American Express Services Europe Limited, for GBP90,000, for its sending more than four million marketing emails to customers without appropriate

consent (ICO: Amex fined for sending four million unlawful emails (May 20, 2021)).

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, 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)). The FTC has also indicated that it is considering undertaking additional Section 6(b) studies on technology industry privacy practices 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.

Statehouse 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 get particular attention in 2022 include:

- **Cross-border data transfer issues.** 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.
- **Focus on 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.
- **Managing 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 priority 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 remain an enviable target of cybercriminals.** 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 Administration's cybersecurity focus and the enhanced AML laws, we are likely to see 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 Administration and state regulators taking more aggressive steps to tackle ransomware and bolster cybersecurity, it is likely we will continue to see the release of stricter cybersecurity regulations and increased enforcement.