THOMSON REUTERS
PRACTICAL LAW™

Trends in Privacy and Data Security: 2022

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

Status: **Published on 28 Feb 2023** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/w-038-3876**
Request a free trial and demonstration at: **us.practicallaw.tr.com/practical-law**

An Article addressing key privacy and data security developments in 2022 and likely trends for 2023, 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 consumer data protection, data breach notification, and other privacy and cybersecurity laws, and trends in industry self-regulation and international data protection laws and enforcement.

As the National Security Agency (NSA) noted in its 2022 cybersecurity yearly review, "[c]yberspace is dangerous" (NSA: NSA Cybersecurity Year in Review: 2022). Reports of sophisticated cyberattacks and ransomware threats were prevalent in 2022. The government, manufacturers, and others further developed standards for securing digital infrastructure like 5G, cloud services, cryptography, internet protocols, and internet of things (IoT) devices. Organizations deployed zero trust cybersecurity strategies more frequently to close operational technology gaps. On the data privacy side, businesses now face an increasing array of state laws in the absence of comprehensive federal data protection regulation.

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 2022 and highlights key issues as the year ahead takes shape. It addresses:

- Federal and state guidance, regulations, and enforcement actions.
- Private litigation.
- Federal and state legislation.
- Industry self-regulation and standards.
- International developments likely to affect US companies, including EU cross-border data transfer issues.
- Trends likely to gain more attention in 2023.

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 and State Data Privacy Laws Toolkit.

Federal Guidance, Regulation, and Enforcement

Several federal agencies issued guidance and took notable privacy and data security enforcement actions in 2022, including:

- The Federal Trade Commission (FTC) (see FTC).
- The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) (see HHS OCR).
- The Department of Commerce and its National Institute of Standards and Technology (NIST) (see Department of Commerce and NIST).
- The Department of Homeland Security (DHS) and its Cybersecurity and Infrastructure Security Agency (CISA) (see DHS and CISA).
- The Federal Communications Commission (FCC) (see FCC).
- The Securities and Exchange Commission (see SEC).
- The White House and 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

On November 15, 2022, the FTC extended by six months the deadline for companies to comply with some of its changes made to strengthen financial institutions' data security safeguards and better protect customers' personal information. The new deadline for complying with certain provisions of the updated Safeguards Rule is June 9, 2023. (87 Fed. Reg. 71,509 (Nov. 23, 2022); see FTC: Press Release: FTC Extends Deadline by Six Months for Compliance with Some Changes to Financial Data Security Rule.)

On August 11, the FTC issued an Advance Notice of Proposed Rulemaking (ANPR), announcing its intent to explore a rulemaking process to "crack down on harmful commercial surveillance and lax data security." The rulemaking process, if pursued, is likely a yearslong effort. The FTC:

- Invited comment on whether it should implement new regulations or other regulatory alternatives addressing:
  - the ways companies collect, aggregate, protect, use, and retain consumer data; and
  - how companies transfer, share, sell, or otherwise monetize consumer data in ways that may harm consumers.
- Posed 95 distinct questions in the ANPR.
- Later hosted a public forum and extended the commenting deadline through late November.

(87 Fed. Reg. 51,273 (Aug. 22, 2022); 87 Fed. Reg. 63,738 (Oct. 20, 2022); see FTC: Press Release: FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices.)

In May, the FTC posted data security guidance explaining its view that the FTC Act imposes a de facto data breach notification requirement and emphasizing the importance of effective security breach detection and response programs (see Legal Update, New Guidance Highlights FTC Act's Apparent De Facto Data Breach Notification Requirement).

The FTC also released reports and published guidance highlighting:

- **Dark patterns.** The FTC showed how companies increasingly use digital design practices to disguise ads and hidden fees, manipulate consumers' privacy choices, trick consumers into buying products or services, or make it difficult to cancel orders or reverse charges (see FTC: Bringing Dark Patterns to Light (Sept. 2022)).
- **Children's Online Privacy Protection Act (COPPA) enforcement.** In a report to Congress, the FTC detailed the 80 investigations opened over the last five years, the resources expended, and the various remedies and relief obtained (see FTC: Federal Trade Commission Report to Congress on COPPA Staffing, Enforcement and Remedies).
- **AI tools to detect harmful online content.** In a report to Congress, the FTC discussed the potential limitations of AI tools intended to detect harmful online content and various issues and policy concerns regarding their use, or government-mandated use, to reduce harmful online content (see FTC: Combatting Online Harms Through Innovation).
- **Mobile health app compliance** (see FTC: Health app developers: Updated interactive tool can help you get started on compliance (Dec. 7, 2022)).
- **The FTC's commitment to fully enforce the law against the illegal use and sharing of location, health, and other sensitive data** (see FTC: Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data (July 11, 2022)).
- **Edtech providers' obligations and COPPA compliance** (see FTC: FTC to Ed Tech: Protecting kids' privacy is your responsibility (May 19, 2022)).
- **Health Breach Notification Rule compliance** (see FTC: Revised Health Breach Notification Rule resources spell out companies' legal obligations (Jan. 21, 2022)).

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 2022 actions reiterated that companies should:

- **Ensure that privacy and data security practices match promises.** For example, the FTC reached settlements with:
  - an edtech provider for its alleged lax security practices that went unaddressed for several years, leading to multiple data breaches, exposing sensitive personal information about millions of its student customers and employees, including financial information and Social Security numbers (see Legal Update, FTC Announces Settlement with Chegg Over Lax Security Practices);

  - an online alcohol marketplace and its CEO over allegations that the company's security failures led to a data breach, including a proposed order requiring the company to destroy unnecessary data and limit future data collection and binding the CEO to specific data security requirements (see Legal Update, FTC Announces Settlement with Drizly and Its CEO Over Alleged Data Security Failures); and
  - an online customized merchandise platform for $500,000 concerning allegations that it failed to secure consumers' sensitive personal data and covered up a major breach (see Legal Update, FTC Announces Proposed Settlement with CafePress for Multiple Data Security Failures).

  For details on the FTC's evolving data security expectations under its reasonable data security measures standard, see FTC Data Security Actions Tracker.

- **Protect children by complying with COPPA obligations.** For example, the FTC reached settlements with:
  - a video game developer in two actions for a total $520 million in penalties and consumer refunds over claims it allegedly violated COPPA and deployed dark patterns to mislead millions of players, with Epic Games agreeing to delete previously collected data unless it obtains further consent or age verification, adopt strong privacy default settings for children and teens, and stop charging consumers without obtaining their affirmative consent (see Legal Update, FTC Announces Settlement with Epic Games Over Alleged Fortnite COPPA Violations); and
  - a nutrition and weight loss app operator for $1.5 million after it allegedly marketed its app to children under 13 and collected personal information without parental consent, with the company agreeing to delete the personal information collected from children and destroy any models or algorithms derived from the data (see Legal Update, FTC Announces Settlement with WW International and Kurbo for COPPA Violations).
- **Avoid dark patterns that result in unfair trade practices.** The FTC reached a settlement with a credit services company for $3 million over its allegedly using dark patterns and misrepresenting that consumers were preapproved for credit card offers (see Legal Update, FTC Settles with Credit Karma Over Allegations of Dark Patterns Used to Deceive Consumers in False "Pre-Approved" Credit Card Offers).

The agency also brought suit against a digital marketing and analytics firm, seeking an order halting its alleged acquisition and downstream sale of large quantities of precise geolocation data from consumers' mobile devices. In response, the company:

- Denied that the mobile location data that it acquires can be used to identify individuals and track them to sensitive locations.
- Claimed that it employs technical controls to prohibit its customers from identifying consumers.

(Complaint, *FTC v. Kochava Inc.*, 2022 WL 4080538 (D. Idaho Aug. 29, 2022); see FTC: Press Release: FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations (Aug. 29, 2022).)

HHS OCR

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

HHS Guidance and Regulation

In 2022, HHS:

- Issued guidance highlighting HIPAA covered entities' obligations when they use online tracking technologies, including when data tracking may result in impermissible disclosures of protected health information (PHI) to tracking technology vendors (see Legal Update, HIPAA Compliance and Tracking Technologies for Apps and Webpages).
- Proposed changes to its Confidentiality of Substance Use Disorder Patient Records regulations under 42 C.F.R. §§ 2.1 to 2.67, implementing provisions of Section 3221 of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), to:
  - improve care coordination;
  - better align with the HIPAA Privacy Rule; and
  - continue protecting the confidentiality of sensitive treatment records.

  (See HHS: Press Release: HHS Proposes New Protections to Increase Care Coordination and Confidentiality for Patients With Substance Use Challenges (Nov. 28, 2022).)
- Issued guidance for the post-*Dobbs* environment addressing how HIPAA safeguards individuals' PHI relating to abortion and reproductive health care,

including the extent to which PHI is protected on apps and devices and how individuals can better protect their data (see Legal Update, In Post-Dobbs Guidance, HHS Addresses Disclosures of Abortion-Related Information).

- Offered additional guidance through OCR on:
  - cyber incident response (see Legal Update, HHS Addresses Cybersecurity Incident Response Procedures Under HIPAA); and
  - telehealth services (see Legal Update, HHS Addresses HIPAA Compliance and Audio-Only Telehealth Services).

HHS Enforcement Activity

Notable 2022 actions reiterated that companies should:

- **Support required patient access to PHI.** OCR continued increased enforcement under its HIPAA Right of Access Initiative throughout 2022, culminating in its 42nd related action in mid-December (see HHS: Press Release: HHS Civil Rights Office Resolves HIPAA Right of Access Investigation with $20,000 Settlement (Dec. 15, 2022)).
- **Refrain from disclosing PHI in social media responses.** New Vision Dental agreed to pay $23,000 and implement a corrective action plan following the provider's alleged inappropriate disclosures of PHI in response to patient reviews on social media (see HHS: Press Release: HHS Civil Rights Office Enters Settlement with Dental Practice Over Disclosures of Patients' Protected Health Information (Dec. 14, 2022)).
- **Securely dispose of PHI.** New England Dermatology P.C. agreed to pay $300,640 and implement a corrective action plan after empty specimen containers with PHI on the labels were insecurely discarded (see Legal Update, Disposal of Specimen Containers Labeled with PHI in Parking Lot Dumpster Leads to HIPAA Settlement).
- **Conduct a thorough risk analysis and implement effective safeguards.** Oklahoma State University's Center for Health Services agreed to pay $875,000, implement corrective actions, and submit to monitoring following a cyberattack that compromised almost 300,000 individuals' PHI (see Legal Update, Malware Cyberattack Leads to $875,000 HIPAA Settlement).

Department of Commerce and NIST

In July, the National Institute of Standards and Technology (NIST) selected the first group of quantum-resistant encryption algorithms for its multi-year standardization project. The algorithms are designed to withstand a potential quantum computer attack as that technology evolves. Quantum computing promises many innovations but risks cracking current cryptographic algorithms, including the public-key cryptography currently used for most internet communications. (See NIST: Press Release: NIST Announces First Four Quantum-Resistant Cryptographic Algorithms (July 5, 2022).)

In February, NIST issued a request for information on potential changes to its widely adopted Cybersecurity Framework (CSF) and began a multi-year process to likely issue in 2024 the CSF 2.0 (see NIST: Updating the NIST Cybersecurity Framework – Journey To CSF 2.0; for details on the current framework, see Practice Note, The NIST Cybersecurity Framework).

Some other notable 2022 NIST guidance and standards included:

- **Supply chain cybersecurity.** NIST revised its cybersecurity supply chain risk management (C-SCRM) guidance on identifying, assessing, and responding to cybersecurity risks throughout the technology supply chain in response to Exec. Order No. 14028, 86 Fed. Reg. 26,633 (May 12, 2021) (see NIST: Press Release: NIST Updates Cybersecurity Guidance for Supply Chain Risk Management (May 5, 2022); for more on C-SCRM, see NIST: Cybersecurity Supply Chain Risk Management).
- **Cybersecurity framework for ransomware.** NIST published a ransomware profile and related guidance to help organizations combat ransomware and align their efforts with its Cybersecurity Framework (see NIST: NISTIR 8374: Ransomware Risk Management: A Cybersecurity Framework Profile and Getting Started with Cybersecurity Risk Management: Ransomware (Feb. 2022)).

Other related topics from NIST's 2022 cybersecurity work addressed:

- The manufacturing sector (see NIST: Protecting Information and System Integrity in Industrial Control System Environments).
- Consumer IoT products (see Legal Update, NIST Publishes Recommendations for Labeling Consumer Internet of Things Products).
- Enterprise risk management (see NIST: Press Release: Prioritizing Cybersecurity Risk for Enterprise Risk Management: NISTIR 8286B (Feb. 10, 2022)).

In early 2023, NIST released its Artificial Intelligence Risk Management Framework, using a similar structure

to its prior cybersecurity and privacy frameworks and providing guidance for managing AI-associated risks while fostering innovation and promoting trustworthiness (see Legal Update, NIST Releases Artificial Intelligence Risk Management Framework).

DHS and CISA

DHS supported a variety of cybersecurity-related activities in 2022, including:

- In October, announcing new Transportation Security Administration (TSA) cybersecurity regulations for designated passenger and freight railroad carriers (see Legal Update, TSA Announces Cybersecurity Requirements for Railroad Carriers).
- Issuing Cybersecurity and Infrastructure Security Agency (CISA) guidance on voluntary cybersecurity information sharing and cyber incident reports, while CISA engages in rulemaking under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (see CISA: Sharing Cyber Event Information: Observe, Act, Report (Apr. 2022); see also Federal Legislation).
- In early 2022, establishing, under Exec. Order No. 14028, the Cyber Safety Review Board, a public-private initiative that brings together government and industry leaders to review and assess significant cybersecurity events (see DHS: Press Release: DHS Launches First-Ever Cyber Safety Review Board (Feb. 3, 2022)).
- Through CISA, publishing other cybersecurity advisories and guidance on, for example:
  - phishing-resistant multifactor authentication (MFA) (see CISA: CISA Releases Guidance on Phishing-Resistant and Numbers Matching Multifactor Authentication (Oct. 31, 2022));
  - critical infrastructure cybersecurity (see Legal Update, CISA Issues Critical Infrastructure Cybersecurity Performance Goals);
  - visibility into IT assets and vulnerability detection standards for federal networks through a binding directive for the federal civilian executive branch (see CISA: Binding Operational Directive 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks (Oct. 3, 2022));
  - software supply chain security for customers and suppliers (see CISA: Securing the Software Supply Chain: Recommended Practices Guide for Customers (Oct. 2022) and Securing the Software Supply Chain: Recommended Practices Guide for Suppliers (Sept. 2022)); and
  - secure cloud migration (see CISA: Cloud Security Technical Reference Architecture (June 2022)).

FCC

FCC Regulatory Activity

Several 2022 FCC activities sought to combat spoofed scam robocalls. For example, the FCC:

- In December:
  - released a new enforcement bureau online portal for reporting illegal robocalls, suggesting that health care providers, small businesses, and other private entities can use it to report robocallers flooding their phone lines with incoming calls or spoofing their phone numbers to trick others (see FCC: Private Entity Robocall and Spoofing Portal); and
  - issued an order affirming its three-call limit and opt-out requirements for exempted callers under the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) (*In re Rules & Regulations Implementing the Telephone Consumer Protection Act of 1991*, 2022 WL 18023141 (F.C.C. Dec. 27, 2022)).
- Issued a declaratory ruling that ringless voicemails require consumer consent because they are a call under the Telephone Consumer Protection Act (TCPA) (*In re Rules & Regulations Implementing the Telephone Consumer Protection Act of 1991*, 2022 WL 17225556 (F.C.C. Nov. 21, 2022); see Legal Update, FCC Rules That Ringless Voicemails to Consumer Wireless Phones Are Subject to TCPA Robocall Restrictions).
- Stated that it would seek to address the gap in implementing STIR/SHAKEN caller ID authentication, namely, that the authentication standards only work on IP-based phone networks, leaving non-IP networks available for bad actors to exploit (FCC Seeks to Fill Challenging Gap in STIR/SHAKEN Robocall Defenses, 2022 WL 16570426 (F.C.C. Oct. 28, 2022)).
- Announced that previously exempted small phone companies must comply with its rules to implement STIR/SHAKEN on their networks, addressing the continuing flood of unwanted robocalls, under the TRACED Act (see FCC: Press Release: FCC Closes Robocall Loophole (June 30, 2022)).

In early 2023, the FCC also proposed strengthening its longstanding customer proprietary network information (CPNI) data breach notification rules with the goal of better aligning its CPNI rules with recent developments in federal

and state data breach laws (*In re Data Breach Reporting Requirements*, 2023 WL 143389 (F.C.C. Jan. 6, 2023)).

FCC Enforcement Activity

The FCC took enforcement actions to combat unwanted robocalls, including by:

- Announcing a "record-breaking," almost $300 million robocall fine (*In re Sumco Panama SA*, 2022 WL 17958841 (F.C.C. Dec. 23, 2022)).
- Cutting off a voice service provider from other networks for failing to meet its robocall mitigation requirements (*In re Global UC Inc.*, 2022 WL 17225519 (F.C.C. Nov. 22, 2022)). The action followed the FCC's announcing its first-ever plans to remove seven voice service providers from its Robocall Mitigation Database. Removing a provider from the database results in other networks no longer carrying their traffic. (FCC Plans to Remove Companies from Key Database for Non-Compliance with Anti-Robocall Rules, 2022 WL 5241281 (F.C.C. Oct. 3, 2022).)
- Proposing a $116 million fine for robocalls made in an apparent toll-free traffic pumping robocalling scheme (*In re Dorsher*, 2022 WL 2805894 (F.C.C. July 14, 2022)).
- Proposing a $45 million fine against a company that allegedly conducted an illegal robocall campaign to sell health insurance under false pretenses (*In re Robbins*, 2022 WL 565928 (F.C.C. Feb. 22, 2022)).
- Announcing robocall investigation partnerships with a growing set of state attorneys general (see FCC: Press Release: FCC Signs Robocall Partnerships with Nine More State Attorneys General (May 19, 2022) and Press Release: Majority of U.S. States Have Joined FCC in Robocall Partnerships (Apr. 7, 2022)).

In August, the FCC also proposed a $100,000 fine against Q Link for failing to respond adequately and promptly to its inquiry into an alleged security flaw in the carrier's app that may have permitted unauthorized access to customer proprietary network information (CPNI) (*In re Quadrant Holdings LLC*, 2022 WL 3339390 (F.C.C. Aug. 5, 2022)).

SEC

In 2022, the SEC proposed new and updated regulations aiming to bolster cybersecurity practices, including proposing:

- Enhanced cybersecurity risk management, strategy, governance, and incident reporting for publicly traded reporting companies (see Legal Update, SEC Proposes Enhanced Cybersecurity Disclosure Rules).
- New cybersecurity risk management rules for registered investment advisers, registered investment companies, and business development companies, as well as amendments to existing rules governing investment adviser and fund cyber risk and incident disclosures (see Legal Update, SEC Proposes Cybersecurity Risk Management Rules for Investment Advisers).

However, following issues with its online comment submission system, the SEC briefly reopened its commenting periods in late 2022 (see Legal Update, SEC Reopens Comment Periods for Several Proposed Rules).

The SEC also expanded its Crypto Assets and Cyber Unit enforcement staff and took related enforcement actions (see SEC: Press Release: SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit (May 3, 2022)). For example, the SEC settled charges with several companies for alleged deficiencies in their identity theft prevention programs under its Identity Theft Red Flags Rule, or Regulation S-ID, including fines and program remediation (see *In re TradeStation Securities, Inc.*, 2022 WL 3018261 (S.E.C. July 27, 2022)).

Other Federal Regulatory Developments

Other federal agencies also increased their privacy and data security activities in 2022. Some notable examples include those from:

- The Commodity Futures Trading Commission (CFTC), which settled charges against a designated contract market over alleged violations of the Commodity Exchange Act and CFTC system safeguards regulations (see Legal Update, CFTC Fines Financial Trading Platform $6.5 Million for Alleged Reporting and Cybersecurity Risk Assessment and Testing Failures).
- The Consumer Financial Protection Bureau (CFPB), which:
  - released guidance noting that consumer reporting agencies and furnishers may be liable under the Fair Credit Reporting Act (FCRA) if they fail to conduct reasonable investigations of consumer report disputes (see Legal Update, CFPB Advises That Failure to Conduct Reasonable Investigation of Disputes May Violate FCRA);
  - advised financial firms that failure to comply with federal data security requirements, including the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, may also trigger liability under the Consumer Financial Protection Act (CFPA) unfairness standard (see Legal Update, CFPB Advises That Insufficient Consumer Data Protection or Information Security

May Violate CFPA Prohibition on Unfair Acts or Practices); and

  - brought an enforcement action against a bank for alleged CFPA, FCRA, and other violations when its sales-incentivized employees accessed customers' credit reports and used personal data to open unauthorized accounts (CFPB: Press Release: CFPB Fines U.S. Bank $37.5 Million for Illegally Exploiting Personal Data to Open Sham Accounts for Unsuspecting Customers (July 28, 2022)).

- The Federal Financial Institutions Examination Council (FFIEC), which updated its Cybersecurity Resource Guide for Financial Institutions to include ransomware-specific resources (see FFIEC: Cybersecurity Resource Guide for Financial Institutions (Sept. 2022)).
- The Federal Reserve, which published its annual report to Congress covering its cyber-related policies and risk management and current and emerging cybersecurity threats, highlighting ransomware, sophisticated distributed denial of service (DDoS) attacks, and supply chain risks (see Federal Reserve: Report to Congress: Cybersecurity and Financial System Resilience Report (July 2022)).
- The Department of Justice (DOJ), which:
  - brought actions to seize 48 internet domains associated with a leading DDoS-for-hire service and charged six defendants who allegedly oversaw the booter service cyberattack platforms (see DOJ: Press Release: Federal Prosecutors in Los Angeles and Alaska Charge 6 Defendants with Operating Websites that Offered Computer Attack Services (Dec. 14, 2022));
  - announced that the US-UK data access agreement, authorized by the Clarifying Lawful Overseas Use of Data (CLOUD) Act, entered into force on October 3, allowing service providers in one country to respond to qualifying, lawful orders for electronic data issued by the other country (see DOJ: Press Release: Landmark U.S.-UK Data Access Agreement Enters into Force);
  - entered into a non-prosecution agreement with Uber Technologies, Inc. to resolve a criminal investigation into allegations the company concealed its 2016 data breach from the FTC (see DOJ: Press Release: Uber Enters Non-Prosecution Agreement Related to 2016 Data Breach (July 22, 2022); for more on a related action, see Legal Update, Criminal Jury Finds Former Uber Security Chief Guilty for Concealing Data Breach); and
  - revised its policy regarding prosecution under the Computer Fraud and Abuse Act (CFAA) (see Legal Update, DOJ Revises CFAA Charging Policy to Support Security Research).
- The National Credit Union Administration (NCUA), which proposed a rule requiring federally insured credit unions to report certain cyber incidents as soon as possible but no later than 72 hours after discovery (87 Fed. Reg. 45,029 (July 27, 2022)). The NCUA Board approved the final rule in early 2023 (see NCUA: Press Release: NCUA Board Approves Final Rule on Cyber Incident Reporting Requirements (Feb. 16, 2023)).
- The NSA, which released a cybersecurity technical report on best practices for overall network security and protection of individual network devices (see NSA: Network Infrastructure Security Guide (June 2022)).
- The Department of Treasury (DOT), which:
  - through its Office of Foreign Assets Control (OFAC), updated its cyber-related sanctions (see Legal Update, OFAC Amends and Reissues Its Cyber-Related Sanctions Regulations); and
  - sanctioned various individuals and entities for their alleged roles in ransomware and hacking activities (see DOT: Press Release: Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity (Sept. 14, 2022), Press Release: U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats (May 6, 2022), and Press Release: Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex (Apr. 5, 2022)).
- The White House, which among other sector-specific and targeted cybersecurity activities:
  - hosted the Second International Counter Ransomware Initiative, attended by 36 nations (see White House: Fact Sheet: The Second International Counter Ransomware Initiative Summit (Nov. 1, 2022));
  - summarized the administration's recent efforts to strengthen the nation's cybersecurity (see White House: Fact Sheet: Biden-Harris Administration Delivers on Strengthening America's Cybersecurity (Oct. 11, 2022));
  - released a voluntary AI bill of rights blueprint, which addresses data privacy and protecting individuals from discriminatory practices (see White House: Blueprint for an AI Bill of Rights);
  - through its Office of Management and Budget (OMB), issued a memorandum requiring agencies to comply with NIST guidance on software supply chain security (see White House: M-22-18: Enhancing the Security of

the Software Supply Chain through Secure Software Development Practices (Sept. 14, 2022));

- issued Exec. Order No. 14083, 87 Fed. Reg. 57,369 (Sept. 15, 2022) on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States (CFIUS), calling on CFIUS to spot foreign investments that seek to obtain access to sensitive data and technologies or that might create cybersecurity or supply chain risks; and
- recommended actions companies should take to protect themselves in light of the heightened cyber threat surrounding the Ukraine conflict (see Legal Update, White House Issues Recommendations to Protect Against Cyberattacks).

State Regulation and Enforcement

State Regulations and Guidance

Key 2022 regulatory developments at the state level included:

- Continued activities surrounding the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA).
- Other states' privacy law rulemaking activities, including cybersecurity regulations for financial services companies and cyberattack prevention guidance.

CCPA/CPRA Regulatory Developments

In April 2022, rulemaking authority under the CCPA/CPRA formally transferred from the California Attorney General (CAG) to the California Privacy Protection Agency (CPPA) that the CPRA established. The CPRA amendments took effect January 1, 2023, but enforcement for the new requirements begins July 1, 2023. The CPPA continues its rulemaking process and submitted a rulemaking package to the Office of Administrative Law for approval on February 14, 2023 (see CPPA: Press Release: CPPA Files Proposed Regulations with the Office of Administrative Law (OAL)). To track current rulemaking developments, see CPRA Regulation Tracker.

The CPRA amendments removed the previous 30-day cure period from the CAG's enforcement process. There is instead a 30-day cure period before the CPPA can issue probable cause findings. (Cal. Civ. Code §§ 1798.155(a) and 1798.199.50; for more on CCPA/CPRA enforcement, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Enforcement.)

The California legislative session ended in 2022 without the legislature extending the CCPA's temporary exemptions for certain workforce and B2B data, leaving their January 1, 2023, expiration in place. To track privacy-related bills in the current California legislature or review the 2021-2022 session, see California Privacy-Related Legislation Tracker and California Privacy-Related Legislation Tracker (2021-2022).

The CAG issued related guidance:

- Emphasizing health apps' obligations under California law, including the Confidentiality of Medical Information Act, to protect and secure reproductive health information (see CAG: Press Release: Attorney General Bonta Emphasizes Health Apps' Legal Obligation to Protect Reproductive Health Information (May 26, 2022)).
- Clarifying that under the CCPA, a consumer's right to know the specific pieces of personal information that a business has collected about them includes internally generated inferences the business holds about that consumer, unless a statutory exception applies (see Legal Update, California AG Issues Opinion on Data Inferences and CCPA Consumer Rights).

Other State-Level Regulatory Developments

Other key state-level regulatory developments in 2022 include those from:

- **Colorado.** The Colorado Privacy Act (CPA), enacted on July 7, 2021, requires the Attorney General to adopt certain implementing rules by July 1, 2023, with additional rulemaking required by July 1, 2025. The Attorney General:
  - released proposed rules on October 1, 2022, following various statements and feedback gathering activities, and continues the rulemaking process (to track CPA rulemaking developments, see Colorado Privacy Act Regulation Tracker); and
  - issued guidance on data security best practices and the CPA (see Legal Update, Colorado Attorney General Releases Guidance on Data Security Practices and the Colorado Privacy Act).
- **New York.** Notably:
  - on November 9, the Department of Financial Services (NYDFS) proposed amendments to its NYDFS Cybersecurity Requirements for Financial Services Companies (23 NYCRR §§ 500.0 to 500.23), including changes to notification obligations, risk assessments, and other program elements and heightened standards for certain larger covered entities (see NYDFS: Proposed Financial Services Regulations); and

- the New York Attorney General released guidance on credential stuffing attacks, including strategies to detect and defend against these attacks, as well as recommendations for strengthening data security programs (see NY AG: Business Guide for Credential Stuffing Attacks (Jan. 5, 2022)).

Single-State Enforcement Actions

Key single-state enforcement actions in 2022 primarily targeted:

- Data breaches and insufficient data security measures (see Data Breaches and Cybersecurity Failures).
- Mobile data privacy, including location data and opt-out controls (see Privacy-Related Enforcement).

Data Breaches and Cybersecurity Failures

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

- Settled for $1.9 million with an e-commerce retailer to resolve allegations stemming from a 2018 data breach that compromised tens of millions of accounts (see NY AG: Press Release: Attorney General James Secures $1.9 Million from E-Commerce SHEIN and ROMWE Owner Zoetop for Failing to Protect Consumers' Data (Oct. 12, 2022)).
- Settled for $400,000 with a grocery store chain to resolve allegations over a 2021 discovery of misconfigured cloud storage containers that potentially exposed consumer information to hackers (see NY AG: Press Release: Attorney General James Secures $400,000 From Wegmans After Data Breach Exposed Consumers' Personal Information (June 30, 2022)).
- Through the NYDFS, reached settlements ranging from $4.5 million to $30 million in three separate actions, highlighting the need to conduct periodic risk assessments, manage a compliant cybersecurity program, and use multifactor authentication (see NYDFS: Press Release: DFS Superintendent Harris Announces $4.5 Million Cybersecurity Settlement with EyeMed Vision Care LLC (Oct. 18, 2022), Press Release: DFS Superintendent Harris Announces $30 Million Penalty on Robinhood Crypto for Significant Anti-Money Laundering, Cybersecurity & Consumer Protection Violations (Aug. 2, 2022), and Press Release: DFS Superintendent Harris Announces $5 Million Penalty on Cruise Company Carnival Corporation and Its Subsidiaries for Significant Cybersecurity Violations (June 24, 2022)).

Privacy-Related Enforcement

Privacy enforcement efforts at the state level also continued with:

- Arizona reaching an $85 million settlement with Google LLC over allegations that the company misled consumers and used dark patterns to gain access to their location data even after consumers disabled the Location History setting (see AZ AG: Press Release: Attorney General Mark Brnovich Achieves Historic $85 Million Settlement with Google (Oct. 4, 2022)). The District of Columbia later reached a $9.5 million settlement with Google over similar allegations, with the company agreeing to change how it informs users of its location data practices and their choices (see DC AG: Press Release: AG Racine Announces Google Must Pay $9.5 Million for Using "Dark Patterns" and Deceptive Location Tracking Practices that Invade Users' Privacy (Dec. 30, 2022)).
- California:
  - settling its first public enforcement action under the CCPA against retailer Sephora USA, Inc. for $1.2 million, resolving allegations that the company failed to disclose to consumers that it was selling their personal information, including precise location data, and honor opt-out requests made through user-enabled global privacy control signals (see Legal Update, California AG Announces $1.2 Million Settlement with Sephora for CCPA Personal Information Sales Violations); and
  - through the CAG, sending CCPA non-compliance notices to various businesses operating loyalty programs for failing to clearly describe the material terms of their financial incentive programs (see CA AG: Press Release: On Data Privacy Day, Attorney General Bonta Puts Businesses Operating Loyalty Programs on Notice for Violations of California Consumer Privacy Act (Jan. 28, 2022)).

Multistate Enforcement Actions

The trend of multistate cooperation in privacy enforcement continued in 2022. For example:

- New York and Pennsylvania settled with a school memorabilia producer and seller for $200,000 over allegations stemming from a 2021-discovered data breach (see PA AG: Press Release: AG Shapiro Secures Settlement with Herff Jones After Data Breach Exposed Pennsylvanians' Private Info (Dec. 16, 2022)).
- Google LLC reached a $391.5 million settlement with a bipartisan coalition of 40 attorneys general who

alleged that the company misled consumers and used dark patterns to gain access to their location data even after consumers disabled the Location History setting (see Legal Update, Forty State Attorneys General Settle with Google for $391.5 Million Over Misleading Location Tracking Allegations; for information about related single-state actions, see Privacy-Related Enforcement).

- Six states and the District of Columbia reached an $8 million settlement with convenience store chain Wawa, Inc. to resolve allegations stemming from a data breach that compromised approximately 34 million payment cards in the Atlantic coast area (see NJ AG: Press Release: Acting AG Platkin Co-Leads $8 Million Settlement with Wawa Inc. over Data Breach that Compromised Millions of Payment Cards in New Jersey (July 26, 2022)).

Private Litigation

Private litigation highlights and notable trends for 2022 focused on:

- Cases brought under the Computer Fraud and Abuse Act (CFAA).
- Data breach and cybersecurity-related litigation.
- Biometric privacy litigation, especially under Illinois's Biometric Information Privacy Act (BIPA).
- Other notable class settlements and developments, including several related to web privacy and state wiretapping laws.

CFAA Litigation

In a closely watched appeal, on remand, the US Court of Appeals for the Ninth Circuit affirmed the lower court's order preliminarily enjoining LinkedIn Corp. from blocking data analytics company hiQ Labs, Inc.'s access to publicly available member profiles (*hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022); see Legal Update, On Remand, Ninth Circuit Affirms Web Scraping Public Website Unlikely to Be Unauthorized Access Violating CFAA). The Ninth Circuit held that hiQ Labs had raised a serious question about whether the CFAA's "without authorization" provision applies to data scraping of public websites. The parties settled the matter in December 2022.

Various district courts also continued to explore the CFAA's limits following the Supreme Court's 2021 ruling interpreting the "exceeds authorized access" clause and holding that:

- The CFAA's "exceeds authorization" provision applies to those who obtain information from areas on a computer network that they do not have access to but not those who misuse their access.
- The CFAA's "without authorization" provision protects computer networks and data from those who access them without any permission at all.
- Liability stems from a gates-up-or-down inquiry, in which one either can or cannot access a computer system.

(*Van Buren v. United States*, 141 S. Ct. 1648 (2021); see, for example, *Ryanair DAC v. Booking Holdings Inc.*, 2022 WL 13946243 (D. Del. Oct. 24, 2022) (allowing claim to proceed because cease-and-desist letters withdrew authorization to access an authentication-protected portion of website); *Salinas v. Cornwell Quality Tools Co.*, 2022 WL 3130875 (C.D. Cal. June 10, 2022) (holding CFAA does not apply to publicly accessible database, even if owner intended to protect access); *ACI Payments, Inc. v. Conservice, LLC*, 2022 WL 622214 (D. Utah Mar. 3, 2022) (allowing payment processor platform's without authorization claim when defendant continued to submit payment requests following cease-and-desist letters; however, plaintiff failed to adequately plead a requisite loss).)

For more details on common CFAA litigation issues and cases, see Practice Note, Key Issues in Computer Fraud and Abuse Act (CFAA) Civil Litigation.

Data Breach Litigation

Standing remained a key issue in 2022 for data breach and cybersecurity-related actions in federal courts. For example:

- The US Court of Appeals for the Third Circuit reversed the dismissal of an employee's proposed class action against a pharmaceutical company over a ransomware attack that led to publication of their personal information on the dark web, finding that injury was sufficiently imminent to constitute an injury-in-fact for standing purposes (*Clemens v. ExecuPharm Inc.*, 48 F.4th 146 (3d Cir. 2022)).
- The US Court of the Appeals for the Seventh Circuit affirmed a dismissal for lack of standing in a dispute over an apparent vulnerability in a vehicle's infotainment system that may have allowed attackers to control the car. The carmaker had later remediated the vulnerability in a software update. The Seventh Circuit held that the plaintiffs failed to plead an injury-in-fact, noting that the cybersecurity vulnerability never manifested outside controlled research. (*Flynn v. FCA US LLC*, 39 F.4th 946 (7th Cir. 2022); see also *Greenstein v. Noblr Reciprocal Exchange*, 2022 WL

17418972 (N.D. Cal. Dec. 5, 2022) (ruling that driver's license numbers are less sensitive than SSNs and do not rise to the level of sensitive personal information needed to establish a credible and imminent threat of future harm); *Riordan v. W. Digital Corp.*, 2022 WL 2046829 (N.D. Cal. June 7, 2022) (finding loss of stored data due to alleged cyberattacker-exploited vulnerability on internet-connected hard drives, without plaintiffs' offering details on the data and loss, insufficient for standing).)

For more information on data breach litigation developments, see Practice Note, Key Issues in Consumer Data Breach Litigation.

BIPA Litigation

Litigation under Illinois's Biometric Information Privacy Act (BIPA) (740 ILCS 14/1 to 14/99) remained steady in 2022. Lawsuits often target employers using biometric timekeeping systems or online biometric interactive services on e-commerce sites, 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 (*Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186).

In early 2023, the Illinois Supreme Court issued two important BIPA rulings:

- Holding that a separate claim accrues each time a private entity scans or transmits to a third party an individual's biometric identifier or information without the individual's prior informed consent (*Cothron v. White Castle Sys., Inc.*, 2023 IL 128004; see Legal Update, Illinois Supreme Court Holds That Each BIPA Violation Is Separately Actionable).
- Clarifying that all BIPA violations are subject to a five-year statute of limitations (*Tims v. Black Horse Carriers, Inc.*, 2023 IL 127801). BIPA does not expressly include a statute of limitations, but prior courts had imposed limits of either one or five years, depending on the violation.

Some notable 2022 BIPA developments concerned:

- **Arbitration provisions.** In *Johnson v. Mitek Systems, Inc.*, the Seventh Circuit affirmed a lower court's order denying a motion to compel arbitration, finding that an identity verification service provider is not a beneficiary under the agreement between a driver and a rideshare service when the agreement's binding arbitration clause did not expressly include like suppliers (55 F.4th 1122 (7th Cir. 2022)).
- **Construing BIPA's "otherwise profit" language.** In *In re Clearview AI, Inc., Consumer Privacy Litigation*, the district court denied a facial recognition platform's motion to dismiss claims under BIPA Section 15(c), which prohibits private entities from selling, leasing, trading, or otherwise profiting from a person's biometric information. The court found that the defendant's business model is premised on collecting plaintiffs' biometric information and then profiting from paying subscribers. (585 F. Supp. 3d 1111 (N.D. Ill. 2022).)
- **Data retention schedules.** An Illinois appellate court held that BIPA Section 15(a), which contains a requirement to develop, publish, and comply with a retention-and-destruction schedule, means that the schedule must exist on the date of collection. The court rejected the defendant's argument that its statutory duty was satisfied if a schedule existed on the day that the biometric data it possessed was no longer needed or the parties' relationship ended. (*Mora v. J&M Plating, Inc.*, 2022 IL App (2d) 210692; see Legal Update, Illinois Appellate Court Holds Possession of Biometric Data Triggers BIPA Requirements for Data Retention and Destruction Policies.)
- **Exemptions.** Courts continued exploring the contours of BIPA's exemptions. For example:
  - an Illinois appellate court found that while BIPA Section 10 excludes HIPAA-protected patient information, the statute does not exclude hospital employee information (*Mosby v. Ingalls Mem'l Hosp.*, 2022 IL App (1st) 200822, *appeal denied*, 201 N.E.3d 591 (Ill. 2023)); and
  - a federal district court held that a university qualifies for BIPA's exemption for GLBA-regulated financial institutions because it participates in the US Department of Education's Federal Student Aid Program (*Powell v. DePaul Univ.*, 2022 WL 16715887 (N.D. Ill. Nov. 4, 2022) (citing additional 2022 cases concluding the same)).
- **Extraterritoriality.** In *Vance v. Microsoft Corp.*, a federal court granted summary judgment in favor of Microsoft over its use of a data set of some 100 million photos extracted from the Flickr photo storage service, including images of plaintiffs without their consent. The court held that the extraterritorial doctrine bars plaintiffs' BIPA claims because:
  - none of Microsoft's relevant conduct occurred primarily and substantially in Illinois; and
  - other entities were responsible for collecting, scanning, and generating facial templates from the photos.

  (2022 WL 9983979 (W.D. Wash. Oct. 17, 2022).)

- **Mobile device authentication.** In *Barnett v. Apple Inc.*, an Illinois appellate court affirmed dismissal of BIPA claims against Apple over iPhone Touch ID and Face ID, holding that:
  - the biometric features are purely optional;
  - Apple never collects the information but instead stores it locally on the device; and
  - users may delete the data and disable the features at any time without impairment to the device's utility.

  (2022 IL App (1st) 220187.)

For details on BIPA-related issues and litigation, see Practice Note, BIPA Compliance and Litigation Overview. For information on related insurance coverage, see Practice Note, Insurance Coverage for Biometric Data Privacy Claims.

Class Settlements

2022 also brought several noteworthy class settlements, including:

- IT operations software company SolarWinds Corp. reaching a $26 million settlement to end a shareholder action over allegedly misleading claims about its cybersecurity controls before 2020's widely publicized cyberattack and ensuing business and government customer impacts (Stipulation & Agreement of Settlement, *In re SolarWinds Corp. Sec. Litig.*, No. 21-00138 (W.D. Tex. Dec. 8, 2022)).
- Illinois district courts approving two different settlements involving TikTok:
  - one for $92 million over BIPA and other claims regarding the company's alleged use of facial recognition technology without consent (*In re TikTok, Inc., Consumer Priv. Litig.*, 2022 WL 2982782 (N.D. Ill. July 28, 2022)); and
  - another for $1.1 million regarding COPPA-related claims over its alleged collection of children's data without parent consent (*T.K. Through Leshore v. Bytedance Tech. Co.*, 2022 WL 888943 (N.D. Ill. Mar. 25, 2022)).
- A California court approving an $85 million class settlement with Zoom Video Communications, Inc., over allegations that Zoom improperly shared users' data through third-party software, made misleading claims about the security of communications, and failed to prevent unauthorized meeting disruptions (*In re Zoom Video Commc'ns, Inc. Privacy Litig.*, 2022 WL 1593389 (N.D. Cal. Apr. 21, 2022)).

Other Notable Cases

Other notable privacy and data security litigation in 2022 included cases addressing:

- **Browser and mobile device privacy.** California district courts dismissed suits against Google LLC over its alleged Chrome web browser and Android mobile phone data collection practices, with:
  - one court dismissing claims that the company allegedly secretly collected Android users' third-party app data due to the plaintiff's inadequate pleading and lack of injury (*Hammerling v. Google LLC*, 2022 WL 17365255 (N.D. Cal. Dec. 1, 2022)); and
  - another court ruling that Google had adequately disclosed its third-party site data collection policy and that users had consented to that collection (*Calhoun v. Google LLC*, 2022 WL 18107184 (N.D. Cal. Dec. 12, 2022)).
- **COPPA preemption.** The Ninth Circuit:
  - reversed dismissal of a data tracking suit under state privacy laws over the alleged collection of children's persistent identifiers without parental consent; and
  - ruled that COPPA does not preempt state law claims based on underlying conduct that may also violate COPPA's regulations.

  (*Jones v. Google LLC*, 56 F.4th 735 (9th Cir. 2022); see Legal Update, COPPA Does Not Preempt State Laws Consistent with Its Substantive Requirements: Ninth Circuit.)
- **The right of publicity.** In a suit over allegations that a publication rented or exchanged subscriber list data with third parties for profit in violation of state right of publicity laws, a New York federal court:
  - dismissed the complaint; and
  - held that the alleged disclosure is not a prohibited public commercial use because "classifying this limited, private disclosure only to the third parties who purchase the Subscriber Lists as publicity would transform the [right of publicity statutes] into sweeping data privacy laws."

  (*Wallen v. Consumer Reps., Inc.*, 2022 WL 17555723 (S.D.N.Y. Dec. 9, 2022); see *Huston v. Hearst Commc'ns, Inc.*, 53 F.4th 1097 (7th Cir. 2022) (finding that multimedia company's alleged sale of subscriber mailing lists without consent is not a violation of the Illinois right of publicity statute because "[plaintiff's] name and other information may have been sold, but it was not used to sell anything").)

- **Stored Communications Act (SCA) claims.** The US Court of Appeals for the Tenth Circuit ruled that a plaintiff must show actual damages to recover statutory damages under the SCA, in a case involving alleged ex-employee unauthorized access to a real estate agent platform account (*Seale v. Peacock*, 32 F.4th 1011 (10th Cir. 2022)). For more information on the SCA and similar claims, see Practice Note, Key Issues in Electronic Communications Privacy Act (ECPA) Litigation.
- **TCPA damages.** The Ninth Circuit partially vacated the district court's judgment after a jury awarded plaintiffs over $925 million for almost two million prerecorded calls in violation of the statute, remanding the case with instructions to reassess the constitutionality of the substantial statutory damages award (*Wakefield v. ViSalus, Inc.*, 51 F.4th 1109 (9th Cir. 2022); see Legal Update, Aggregated Statutory Damages Award of $925,220,000 May Violate Due Process: Ninth Circuit).
- **Website session replay and analytics.** A wave of lawsuits asserted claims under state wiretap laws and related causes of action stemming from website operators' use of vendor-provided session replay and analytics software to record site visitor data and activities. For example, see:
  - *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121 (3d Cir. 2022) (examining whether deploying third-party cookies to track website visitor behavior and the exchange of information involved are subject to the Pennsylvania Wiretapping and Electronic Surveillance Control Act (WESCA)) (see Legal Update, Third-Party Website Tracking Could Trigger Pennsylvania's Wiretap Statute Protections: Third Circuit); and
  - *Javier v. Assurance IQ, LLC*, 2022 WL 1744107 (9th Cir. May 31, 2022) (allowing claims to proceed against insurance platform that recorded plaintiff's web activity in real time, finding that California's wiretapping law requires prior all-party consent and plaintiff sufficiently alleged lack of express prior consent).

Federal Legislation

Congress again failed to pass broad consumer data privacy legislation in 2022. Despite apparent bipartisan agreement on basic principles, state law preemption and whether to include a private cause of action remained contentious.

However, some narrowly focused federal cybersecurity laws enacted in 2022 include:

- The Cyber Incident Reporting for Critical Infrastructure Act of 2022, which requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report certain cyber incidents and ransom payments to CISA (Pub. L. 117-103, 136 Stat. 49 (2022) (codified at 6 U.S.C. §§ 681 to 681g); see Legal Update, President Biden Signs Cyber Incident Reporting for Critical Infrastructure Act of 2022). CISA later issued a request for information to inform its rulemaking process (87 Fed. Reg. 55,833 (Sept. 12, 2022); see CISA: Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)).
- The Better Cybercrime Metrics Act, which sets various standards to improve the collection of cybercrime-related data (Pub. L. 117-116, 136 Stat. 1180 (2022)).
- Medical device cybersecurity requirements, including software bill of materials (SBOM) obligations, under the Consolidated Appropriations Act, 2023 (Pub. L. 117-328, 136 Stat. 4459 (2022)).
- The Small Business Cyber Training Act of 2022, mandating that the Small Business Administration create and staff a cyber counseling program in its lead small business development centers (Pub. L. 117-319, 136 Stat. 4424 (2022)).
- The Quantum Computing Cybersecurity Preparedness Act, which sets agency obligations to prepare for quantum computing effects on cryptography and agency systems and recognizes NIST standard-setting activities (Pub. L. 117-260, 136 Stat. 2389 (2022); see Department of Commerce and NIST).

To track developments in selected privacy and data security federal legislation, see Federal Privacy-Related Legislation Tracker. For more details on the 2021-2022 Congressional session, see Federal Privacy-Related Legislation Tracker (2021-2022).

State Legislation

Following enactment of the CCPA/CPRA and other states' broad consumer data privacy laws and in the continued absence of comprehensive federal legislation, many state legislatures have or are considering bills to strengthen consumer data protection.

For example, states and some local governments focused their efforts in 2022 and continue to do so in 2023 on:

- Broad consumer data privacy laws (see State Consumer Data Privacy Laws).
- Updated data breach notification laws (see Data Breach Notification Laws).

- Other privacy and cybersecurity-related laws (see Other Privacy and Cybersecurity-Related Laws).

Several states also continued the trend of enacting insurance data security laws that generally follow the National Association of Insurance Commissioners (NAIC) Model Insurance Data Security Law (MDL-668), including Kentucky, Maryland, and Vermont (see Practice Note, NAIC Model Data Security Law and State-Specific Implementations).

For more information on state-specific privacy and data security laws, see State Data Privacy Laws Toolkit.

State Consumer Data Privacy Laws

New broad state consumer data privacy laws and related amendments in 2022 include those in:

- **Connecticut.** The Connecticut Personal Data Privacy and Online Monitoring Act (Connecticut Data Privacy Act or CTDPA), effective July 1, 2023:
  - offers some consumer rights like those in California and Colorado;
  - excludes data collected in B2B and employment contexts;
  - requires controllers to obtain a consumer's consent before processing sensitive data, including precise location data; and
  - does not contain a private right of action.

  For details on the CTDPA, see Practice Note, Connecticut Personal Data Privacy and Online Monitoring Act (CTDPA) Quick Facts: Overview.
- **Utah.** The Utah Consumer Privacy Act, effective December 31, 2023, also excludes data collected in B2B and employment contexts (Utah Code §§ 13-61-101 to 13-61-404). For details on the Utah Consumer Privacy Act, see Practice Note, Utah Consumer Privacy Act (UCPA) Quick Facts: Overview.
- **Virginia.** Legislators amended the Virginia Consumer Data Protection Act (VCDPA) to:
  - allow a controller that has obtained a consumer's personal data from a source other than the consumer to comply with deletion requests using certain specified methods;
  - expand the nonprofit organization definition to include political organizations and certain insurers; and
  - change the disposition of collected enforcement funds.

  For details on the VCDPA amendments, see Legal Update, Virginia Amends Virginia Consumer Data Protection Act. For more information on the VCDPA, see Practice Note, Virginia Consumer Data Protection Act (VCDPA) Quick Facts: Overview.

To track state consumer data privacy legislation, see State Consumer Privacy Legislation Tracker. For more details on the 2021-2022 legislative season, see State Consumer Privacy Legislation Tracker (2019-2022).

Data Breach Notification Laws

Reacting to mega breaches and ongoing cyber threats, some states amended their existing private sector data breach notification laws in 2022, generally extending them. For example:

- Arizona's HB 2146 requires notice to the state Department of Homeland Security in addition to the state's attorney general if a breach involves notification of more than 1,000 individuals.
- Indiana's HB 1351 added a requirement that disclosure or notice must occur not more than 45 days after the discovery of a breach (see Legal Update, Indiana Amends Data Breach Notification Requirements).
- Maryland's HB 962 expanded its definition of protected data to include genetic information, updated its notice requirements, and altered the timing obligations for notification under some circumstances (see State Q&A, Data Breach Notification Laws: Maryland).
- Pennsylvania's SB 696 updated its notice requirements and expanded its personal information definition to include certain medical and health insurance information and a user name or email address in combination with a password or security question and answer that allows access to an online account (see Legal Update, Pennsylvania Amends Data Breach Notification Law).

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

Other Privacy and Cybersecurity-Related Laws

Other notable state and local data privacy laws that were newly enacted or updated in 2022 address:

- **Children's and student privacy.** California passed the California Age-Appropriate Design Code Act, effective July 1, 2024, imposing new legal obligations on companies providing online services, products, or features that children under 18 are likely to access. The

law requires covered businesses to adopt privacy-by-design and privacy-by-default measures for their online services. For more information on this law, see Legal Update, California Passes the Age-Appropriate Design Code Act to Protect Children's Privacy. An industry group has challenged the law (see Complaint for Declaratory & Injunctive Relief, *NetChoice, LLC v. Bonta*, No. 22-08861 (N.D. Cal. Dec. 14, 2022)). Several states also updated their student privacy laws, including:

  - California, which enacted the Student Test Taker Privacy Protection Act, restricting educational test proctoring services' data practices (see Legal Update, California Enacts Changes to Student and Mental Health Privacy Laws);
  - Maryland, which amended its Student Data Privacy Act to alter definitions to further protect certain student data and to re-establish the Student Data Privacy Council (see Legal Update, Maryland Amends Student Data Privacy Law); and
  - Minnesota, which enacted the Student Data Privacy Act, governing public school technology providers' student data practices and limiting provider and government access to students' school-issued devices (see Legal Update, Minnesota Enacts Student Data Privacy Act).

- **Employee privacy.** New Jersey enacted AB 3950, which prohibits employers from knowingly using a tracking device in a vehicle used by an employee without written notice (see Legal Update, New Jersey Law Requiring Employers to Provide Notice Before Tracking Employee-Operated Vehicles to Take Effect).
- **Genetic information.** Wyoming amended its genetic information privacy law to include enhanced notice, consent, and consumer rights requirements for direct-to-consumer genetic testing companies (see Legal Update, Wyoming Amends Genetic Data Privacy Law).
- **Health care privacy.** California passed AB 2089, amending its Confidentiality of Medical Information Act to apply to digital mental health services, such as mobile apps and websites (see Legal Update, California Enacts Changes to Student and Mental Health Privacy Laws).
- **IoT security.** California amended its law imposing security requirements on IoT devices to provide a safe harbor for connected device manufacturers that participate in a labeling scheme that conforms with certain NIST criteria (see Legal Update, California Amends Connected Devices Law and Creates a Safe Harbor for IoT Devices Meeting NIST Labeling Criteria).
- **Right of publicity.** Louisiana passed SB 426, which grants individuals property rights in the commercial exploitation of their names, signatures, and likenesses and other aspects of their identities (see Legal Update, Louisiana Enacts New Right of Publicity Statute).
- **Robocalls.** Ohio enacted SB 54, strengthening its anti-robocall laws and giving its Attorney General the power to enforce federal telemarketing laws at the state level (see Legal Update, Ohio Enacts New Robocall Legislation).

Industry Self-Regulation and Guidance

Industry self-regulation and guidance from independent organizations remained important components of the privacy and data security landscape in 2022 across various sectors.

For example:

- The Children's Advertising Review Unit (CARU), one of the self-regulatory units of BBB National Programs:
  - issued a compliance warning for child-directed advertising in the metaverse, reminding advertisers to avoid blurring advertising and non-advertising content, clearly disclose endorsements and influencer claims, and use clear and conspicuous disclosures understandable to children (see CARU: Compliance Warning Regarding Advertising Practices Directed to Children in the Metaverse (Aug. 23, 2022)); and
  - announced its compliance efforts with app operators to correct alleged COPPA and CARU guidelines violations, including insufficient age screening processes and privacy notices, lack of verifiable parental consent, and non-compliant advertising displays (for example, see CARU: Children's Advertising Review Unit Finds Outright Games in Violation of COPPA and CARU's Advertising and Privacy Guidelines; Company Agrees to Corrective Actions (July 6, 2022)).
- The BBB National Programs' Digital Advertising Accountability Program (DAAP) issued a compliance warning on device or user fingerprinting and cross-app data, reminding companies that its standards are applicable regardless of the technology they use to serve targeted advertising (see DAAP: BBB National Programs' Privacy Watchdog Issues Compliance Warning for "Fingerprinting" Cross-App Data Collection Practices (Feb. 8, 2022)).
- The BBB National Programs' Center for Industry Self-Regulation and its Teen Age Privacy Program (TAPP)

published a new operational framework designed to help companies develop digital products and services that consider the potential of risks and harms to teenage consumers and ensure that businesses collect teen data responsibly (see TAPP: A Roadmap for Considering Teen Privacy & Safety).

- The Interactive Advertising Bureau (IAB) published a contractual framework to assist companies in complying with the five state data privacy laws that take effect in 2023 (see IAB: Multi-State Privacy Agreement (MSPA)).
- The National Advertising Initiative (NAI) released enhanced standards for precise location data tracking (see Legal Update, NAI Publishes Enhanced Standards on Tracking Sensitive Location Data).
- The Payment Card Industry Security Standards Council (PCI SSC) released version 4.0 of the PCI Data Security Standard (PCI DSS), with a defined transition period (see Practice Note, PCI DSS Compliance: PCI DSS Versions).

International Developments

The global momentum for enacting and enforcing comprehensive data protection laws and regulations also continued in 2022, with a sampling of activities that may affect US-based multinationals occurring in the following locations (**Note that global resources may only be available to users with an enhanced global subscription. For questions about access to content, please contact your Account Manager.**):

- **Canada.** Québec adopted Bill 64 in late 2021, which includes significant amendments to the 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, took effect September 22, 2022. For more information on Bill 64, see Québec Act Respecting the Protection of Personal Information in the Private Sector Compliance Toolkit.
- **The EU.** See EU Developments.
- **The UK.** See UK Developments.
- **Other countries.** New or updated data protection and cybersecurity laws or regulations also appeared in a variety of other countries and regions in 2022, including Australia, Cuba, Kenya, Oman, Switzerland, Uzbekistan, and Vietnam.

International Standards

In April, the US Department of Commerce (DOC) published a declaration from current Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR) System participating states on establishing the Global Cross-Border Privacy Rules Forum (Global CBPR Forum). The Global CBPR Forum's objectives include supporting cross-border data flows and promoting interoperability among different regulatory approaches to data privacy (see DOC: Global Cross-Border Privacy Rules Declaration).

In October, the International Standards Organization (ISO) announced an update to its widely used ISO/IEC 27001 information security standard (see ISO: ISO/IEC 27001: What's new in IT security? (Oct. 25, 2022)).

Cross-Border Data Transfers

Organizations that depend on standard contractual clauses (SCCs) to transfer personal data originating in the European Economic Area (EEA) to third countries under the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), including the US, were obligated to implement new SCCs by December 27. For guidance and steps to ensure compliance, see GDPR Cross-Border Transfers Checklist.

On March 25, the White House announced that the US and the European Commission (EC) had agreed in principle on a new Trans-Atlantic Data Privacy Framework (see Legal Update, White House Announces Trans-Atlantic Data Privacy Framework). In October, President Biden issued Exec. Order No. 14086, 87 Fed. Reg. 62,283 (Oct. 7, 2022) on Enhancing Safeguards For United States Signals Intelligence Activities that, along with newly issued DOJ regulations, supports further redress for individuals (see DOJ: Redress in the Data Protection Review Court). In December, the Office of the Director of National Intelligence (ODNI) announced additional redress support procedures (see ODNI: Intelligence Community Directive 126: Implementation Procedures for the Signals Intelligence Redress Mechanism Under Executive Order 14086).

Following those actions, the EC began the process of adopting an adequacy decision for the US that continues to progress, including issuing a draft decision (see Legal Update, European Commission launches adoption process for EU-US Data Privacy Framework). The new framework is not available for companies' use unless and until the EC formally adopts the adequacy decision. For more resources on cross-border data transfers, see Cross-Border Personal Data Transfers Toolkit.

EU Developments

While perhaps the biggest news for many US companies concerned the updated Trans-Atlantic Data Privacy Framework (see Cross-Border Data Transfers), other 2022 privacy and data security policy developments in EU law included:

- The Directive of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (Directive 2022/2555) (NIS 2 Directive), which was published in the Official Journal, triggering a January 16, 2023, effective date, although member states have until October 2024 to implement the updated measures. The NIS 2 Directive broadens the scope of covered sectors under the prior NIS 1 Directive and aims to enhance cybersecurity and further standardize implementation across member states. For details on the NIS 2 Directive, see Practice Note, NIS 2 Directive: overview.
- Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives 2019/1937 and 2020/1828 (Digital Markets Act), which entered into force on November 1, 2022. The Digital Markets Act:
  - bans certain anticompetitive practices used by large platforms acting as gatekeepers; and
  - includes certain privacy-related provisions, such as prohibitions on preventing users from uninstalling preinstalled software or apps or processing users' personal data outside of the gatekeeper's core platform for targeted advertising purposes without effective consent.

  For more information on the Digital Markets Act, see Legal Update, Digital Markets Act enters into force on 1 November 2022.
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act), which was published in the Official Journal, triggering a November 16, 2022, effective date, although most provisions do not apply until February 2024. The Digital Services Act:
  - aims to increase transparency and accountability for online platforms and improve mechanisms for removing illegal content; and
  - contains some privacy-related provisions, including banning dark patterns that manipulate users' choices and strengthening certain transparency requirements for online advertising.

  For more information on the Digital Services Act, see Legal Update, Digital Services Act published in Official Journal. To track further guidance, see Digital Services Act: legislation tracker.

Following the *Schrems II* ruling in 2020 that invalidated the Privacy Shield, the French data protection authority (*Commission Nationale de l'informatique et des Libertés* (CNIL)) and other EU data protection authorities (DPAs) received complaints questioning companies' use of Google Analytics on their websites. In February 2022, the CNIL found that these personal data transfers to the US are illegal under the GDPR and should cease under current conditions (see CNIL: Use of Google Analytics and data transfers to the United States: the CNIL orders a website manager/operator to comply (Feb. 10, 2022)). Some other EU DPAs made similar findings. In July, the CNIL released guidance about how companies can make their websites' use of analytics tools GDPR-compliant (see CNIL: Google Analytics and data transfers: how to make your analytics tool compliant with the GDPR? (July 20, 2022)). Google also issued a blog post about Google Analytics 4 updates, including those that further address user privacy (see Google: Prepare for the future with Google Analytics 4 (Mar. 16, 2022)). In December, the Spanish DPA (*Agencia Española de Protección de Datos* (AEPD)) deviated from the other DPAs, rejecting a similar complaint, at least under the facts presented (AEPD: Decision No. E/10529/2021 (Dec. 15, 2022) (in Spanish)).

The European Data Protection Board and member states' DPAs continued to publish a wide variety of resources, offering additional targeted guidance on the GDPR and various issues and technologies. For details regarding GDPR guidance, see GDPR European Data Protection Board Guidance Tracker and GDPR Data Protection Authority Guidance Tracker by Country (EEA).

The DPAs' enforcement priorities in 2022 generally focused on transparency, non-compliant digital marketing, consent issues, and data security controls, resulting in a variety of fines and remediation demands, including a noteworthy investigation and fine related to the data processing operations of a social media service. For more on GDPR enforcement trends, see Practice Note, GDPR Enforcement Charts (EEA).

For more information on GDPR issues and compliance, especially for US-based companies, see GDPR Resources for US Practitioners Toolkit.

UK Developments

The UK government released a voluntary code of practice for app store operators and app developers with minimum privacy and data security requirements, which includes a cyber vulnerability disclosure process (see UK: Code of practice for app store operators and app developers (Dec. 9, 2022); see also Legal Update, Government publishes new code of practice for app store operators and developers).

The UK Information Commissioner's Office (ICO) released updated guidance in 2022 on:

- Transfer risk assessments, which businesses must undertake when transferring personal data to entities located in countries the UK deems inadequate, including the US (see ICO: International data transfers; see also Legal Update, ICO updates guidance on international data transfers).
- The Privacy and Electronic Communications Regulations (PECR), which provide rules on digital marketing messages, cookies, and consumer privacy regarding communication networks and location data (see ICO: What are PECR?; see also Legal Update, ICO publishes updated PECR guidance).
- Binding corporate rules (BCRs), noting the ICO's simplified approval process (see ICO: Guide to Binding Corporate Rules; see also Legal Update, ICO simplifies UK Binding Corporate Rules approval process).

The ICO imposed several significant penalties for data protection violations in 2022, including those against:

- TikTok Inc. and TikTok Technologies UK Ltd, provisionally for GBP27 million, based on allegations that the company may have breached UK data protection law and failed to protect children's privacy when using the TikTok platform (see Legal Update, ICO issues TikTok with notice of intent to fine £27 million).
- Clearview AI, Inc. for GBP7.5 million for allegedly using UK individuals' images scraped from publicly available internet content without their consent (see Legal Update, ICO fines Clearview AI Inc over £7.5 million and orders data deletion). Other European DPAs took similar actions against Clearview. However, the company has claimed that they are not subject to European law.

Looking Forward

Data privacy compliance remains a priority and challenge for many organizations, with a special focus on the GDPR, the CCPA/CPRA, and compliance preparations for the emerging Colorado, Connecticut, Utah, and Virginia laws (see State Regulation and Enforcement and State Legislation). Companies must also continue to track the FTC's evolving priorities, which its latest reports, enforcement actions, blog posts, and rulemaking efforts indicate a continued and, in some areas, increasing focus on:

- Children's privacy.
- Location and health care data privacy.
- Business models and related activities that the FTC has termed commercial surveillance under its open ANPR (see FTC Regulations and Guidance).
- Data breach response.
- Dark patterns.
- Potential discrimination or other adverse effects from automated systems and AI, including the agency's use of algorithmic disgorgement as an enforcement remedy.

Privacy-related litigation will likely remain robust in many areas, including biometric privacy under Illinois's BIPA, wiretapping suits related to the use of session replay software, and complaints over the collection and use of sensitive health and location data without adequate notice and consent.

As already seen in early 2023 legislative activities, states are likely to continue:

- Filling the gap in data privacy law, given the low likelihood of federal legislation passing in a divided Congress.
- Considering laws and regulations to strengthen cybersecurity.

To monitor current state legislation, see State Consumer Privacy Legislation Tracker.

Additional privacy and data security issues likely to get particular attention in 2023 include:

- **New hope for EU-US 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 their lawful options under the GDPR. In a bit of good news, it appears that the EC may adopt a final adequacy decision for the Trans-Atlantic Data Privacy Framework in 2023, giving US companies the opportunity to eventually certify their participation in the framework. However, uncertainty remains following an early 2023 draft motion from the European Parliament (EP) Committee On Civil Liberties, Justice and Home Affairs urging EC rejection

(see EP: Draft Motion for a Resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework (Feb. 14, 2023)). A legal challenge to the framework, if adopted, is also likely.

- **Cryptocurrency and digital assets remain an enviable target of cybercriminals.** With turmoil in the cryptocurrency industry following the collapse of a well-known payment platform, crypto lender, and exchange, cybercriminals are employing phishing techniques, deepfakes, and other scams to try to defraud consumers into giving up their digital wallet credentials. Hackers have also continued to target online trading platforms and digital wallet applications, looking for software vulnerabilities to steal valuable digital currencies (one recent report noted that $3.8 billion was stolen from cryptocurrency businesses in 2022). Attackers have also orchestrated elaborate spoofed crypto offerings to scam unsuspecting victims. Holders of crypto and digital assets, as well as platforms, must maintain careful safeguards and control procedures to prevent theft or intrusions. Given the administration's and certain state regulators' (such as the NYDFS) focus on anti-money laundering (AML) compliance, there will likely be increased oversight and regulation of virtual currency exchanges, decentralized autonomous organizations (DAOs), and even platform developers whose protocols may be used for illicit purposes.
- **Metaverse offers new possibilities but new cyber hazards.** The grand concept of the metaverse as the next iteration of the mobile internet and a major part of both digital and real life has not yet arrived, but borderless virtual worlds and platforms are coming. With these services, thorny questions arise about applicable privacy laws, potential cyber threats and scams, and children's privacy protection.
- **Focus on children's privacy.** The UK rolled out its age-appropriate design code in 2021, and California followed in 2022, with its law slated to take effect July 1, 2024, making this a crucial time for compliance activities (see Other Privacy and Cybersecurity-Related Laws). On the federal front, a bill to update COPPA and raise the age of minors under its protection to 16 has received bipartisan support, making children's privacy a prominent issue for 2023. State attorneys general may also be active again regarding child privacy enforcement issues.
- **Managing sector-specific and online cyber risks.** Sophisticated cyber intrusions from non-US hackers and ransomware attacks, fueled by cybercrime-as-a-service marketplaces, remain a serious concern. The Ukraine conflict has only exacerbated the potential cyberthreats from abroad, with many organizations dedicating more resources to their own and their vendors' cybersecurity practices. On the regulatory side, there may be more regulation limiting ransomware payments. Federal authorities discourage the practice, and Florida and North Carolina restrict state entities from complying with ransom demands. 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 supply chain providers remain priority targets for bad actors. Additional high-risk attack targets include utilities and critical infrastructure, state and county agencies, sports betting and online gambling platforms and user accounts, and fintech and crypto-related applications.