THOMSON REUTERS
PRACTICAL LAW™

Trends in Privacy and Data Security: 2020

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

Status: **Published on 22 Feb 2021** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/w-028-6134**
Request a free trial and demonstration at: **us.practicallaw.tr.com/about/freetrial**

An Article addressing key privacy and data security developments in 2020 and likely trends for 2021, including federal and state regulation and enforcement. This Article also discusses private litigation related to data breaches, biometrics, and other privacy-related causes and recent developments in state data breach notification and other privacy and cybersecurity laws, with an emphasis on COVID-19 impacts, the California Consumer Privacy Act (CCPA), and trends in industry self-regulation and international data protection laws and enforcement.

COVID-19 impacts, the California Consumer Privacy Act (CCPA) coming into force, and the invalidation of the EU-US Privacy Shield already made 2020 an especially active year for privacy and data security risks and obligations. December then brought discovery of an unprecedented cyberattack affecting government agencies, critical infrastructure entities, and others. The highly sophisticated attack, likely perpetrated by nation-state sponsored hackers, exploited SolarWinds Orion, enterprise network management software that many organizations use to monitor and support their information technology (IT) infrastructures. Hackers compromised the SolarWinds development and build environment, adding malware to software updates that some 18,000 customer organizations received. The malware left those organizations vulnerable to hard-to-detect targeted network attacks and infiltration.

The SolarWinds attack is a startling reminder of evolving and novel cyber threats and the importance of companies and vendors conducting thorough diligence before finalizing and throughout the life of material software, hardware, and IT service agreements (for more on the attack and supply chain risk management, see the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Supply Chain Compromise website).

Given the bizarre, trying year that was 2020, organizations must keep up with the dynamic and increasing legal obligations governing privacy and data security, understand how they apply, monitor risks and attack trends, and manage their compliance to minimize exposure. This article reviews important privacy and data security developments in 2020 and highlights key issues for the year ahead. Specifically, it addresses:

- Implications of the COVID-19 global pandemic (see COVID-19 Pandemic).
- Developments concerning the California Consumer Protection Act (CCPA) (see California Consumer Privacy Act (CCPA) Developments).
- 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 (see International Developments), including the fallout from the invalidation of the EU-US Privacy Shield as a mechanism for cross-border data transfers (see ECJ Opinions and Schrems II).
- Trends likely to gain more traction in 2021 (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.

COVID-19 Pandemic

The COVID-19 pandemic impacted almost every aspect of daily life, forcing the temporary closure of many offices, schools, and businesses and altering the way government functions and provides services.

On March 13, 2020, US President Trump declared the COVID-19 outbreak a national emergency, making a variety of laws and executive powers available to federal and state government and public health agencies (85 Fed. Reg. 15337, 2020 WL 1272563 (Mar. 18, 2020)). Organizations had to navigate a quickly changing legal and regulatory landscape across industries. Some of the key issues subject to new or updated guidance included:

- Security vulnerabilities raised by the abrupt shift to near universal remote working (see Remote Environments).
- Privacy issues implicated by remote schooling (see Student and Child Privacy).
- Robocalls and permitted exceptions under the Telephone Consumer Protection Act (TCPA) (see Emergency Robocalls).
- Novel contact tracing technologies and apps (see Contact Tracing Technologies).
- Health information sharing under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and related regulations (see Health Information Sharing).

For more on handling personal data under pandemic conditions, see Practice Note, COVID-19: Data Privacy & Security Guidance on Handling Personal Data During a Pandemic (Global) Tracker.

Remote Environments

Businesses that abruptly shifted to a remote workforce faced new or expanded cybersecurity risks that surfaced with the new way of working. This change prompted:

- The Federal Trade Commission (FTC) to publish a post providing businesses with tips for minimizing security risks when hosting or joining online videoconferences.
- The National Institute of Standards and Technology (NIST) to publish blog posts on telework security basics and virtual meeting security.
- The Financial Industry Regulatory Authority (FINRA) to release a Cybersecurity Alert describing measures organizations may use to strengthen their cybersecurity controls in a remote work situation.
- CISA and the UK's National Cyber Security Centre to release a joint statement advising that cyber criminals were honing their phishing and malware attacks to exploit remote workers and newly deployed access infrastructure.

Organizations also confronted a series of pandemic-related workplace and health privacy issues (for more on managing these employment issues, see Employment Global Coronavirus Toolkit and Benefits, Share Plans & Executive Compensation Global Coronavirus Toolkit).

Student and Child Privacy

The pandemic made educational institutions adapt to new ways of handling student data, guided by:

- The FTC's guidance under the Children's Online Privacy Protection Act of 1998 (COPPA) urging schools to understand:
  - how ed tech operators and other providers may collect, use, and disclose students' personally identifiable information (PII); and
  - steps for ensuring proper consents and uses.
- The US Department of Education's Student Privacy Policy Office's FAQ on when schools may disclose a student's educational records to public health authorities without consent under the Family Educational Rights and Privacy Act (FERPA). The FAQ also discusses how a school may, in a limited manner, disclose a student's COVID positive status in certain situations.

Emergency Robocalls

Health care providers and public health authorities' need to communicate information about the pandemic raised issues under the TCPA, prompting the Federal Communications Commission (FCC) to:

- Rule that the pandemic constituted an emergency under the TCPA, permitting hospitals, health care providers, state or local health officials, and other government officials to make calls and send text messages without prior consent where the communications:
  - are informational; and
  - relay pandemic-related health and safety risks.

  (FCC, *In re Rules & Regulations Implementing the Telephone Consumer Protection Act of 1991*, 2020 WL 1491502 (Mar. 20, 2020).)
- Clarify that the emergency exception extended to calls made and text messages transmitted to positive-testing individuals with information on post-recovery plasma donations (FCC, Clarification on Emergency COVID-19 Related Calls, DA 20-793, 2020 WL 4362569 (July 28, 2020)).

Improper robocalls also rose during the pandemic. The FTC sent letters to Voice over Internet Protocol (VoIP) service providers and other companies:

- Warning against permitting COVID-related scam robocalls into the US.
- Threatening enforcement, including instructions to carriers to block all provider traffic.

(FTC, Robocall Warning Letters).

Contact Tracing Technologies

Technology companies harnessed mobile phone capabilities to help public health authorities with digital contact tracing and social distancing, raising privacy concerns. In April 2020, Google and Apple jointly released Privacy-Preserving Contact Tracing Technology or the Exposure Notification System that uses Bluetooth pseudonymized beacons between phones in proximity and individual positive test result reports to avoid collecting location data and minimize privacy risks. Some states have released free contact tracing apps based on the Exposure Notification System, including:

- Virginia (COVIDWISE).
- A group of northeast states (COVID Alert).
- A group of west coast states (Exposure Notification Express).

However, a lack of public awareness and lingering privacy concerns curtailed widespread use.

A group of state attorneys general sent a letter to the major app platforms requesting increased oversight of apps claiming to help with contact tracing or exposure notifications. The attorneys general noted that some apps may not adequately protect consumer privacy, including those that use GPS tracking, support in-app purchases, or are not affiliated with any public health or legitimate research institutions.

Kansas passed its Contact Tracing Privacy Act, which:

- Prohibits using mobile phone location data to identify or track an individual's movement.
- Imposes certain obligations on contact tracing personnel.
- Places other limits on collecting, using, and retaining contact tracing information.

(K.S.A. 48-961.)

Health Information Sharing

The US Department of Health and Human Services (HHS) took several steps during the pandemic to relax certain HIPAA privacy requirements. For example, HHS issued:

- A bulletin announcing a limited HIPAA sanctions waiver for sharing patient information with family, emergency personnel, and public health officials for treatment purposes or to prevent a serious health threat.
- An announcement that it intended to exercise its enforcement discretion and not impose penalties for certain HIPAA Privacy Rule violations against providers or their business associates for business associates' good faith uses and disclosures of protected health information (PHI) for public health and health oversight activities during the pandemic.
- Guidance on how covered entities may disclose PHI about an infected individual to paramedics and first responders in compliance with HIPAA.
- A notification that it intended to exercise its HIPAA enforcement discretion and not impose penalties against covered health care providers for good faith use of widely available communications apps for telehealth during the pandemic. HHS later clarified in a FAQ that providers must use non-public facing remote communication products that typically employ end-to-end encryption and individual access controls.
- A declaration under the Public Readiness and Emergency Preparedness Act (PREP Act) providing liability immunity to covered entities using medical countermeasures against COVID-19 and authorization to health care personnel using telehealth to administer covered countermeasures for patients in a state other than the state where they are already permitted to practice using telehealth technology.

California Consumer Privacy Act (CCPA) Developments

The CCPA took effect on January 1, 2020. However, the scope of organizations' obligations and risk exposure remain in flux, due largely to:

- The ongoing rulemaking process (see Final CCPA Regulations).
- Lawsuits under the CCPA's private right of action, which are just beginning (see CCPA Litigation).

- California voters' approval of the California Privacy Rights Act (Proposition 24) (CPRA), which amends the CCPA in important ways (see CPRA).

The legislature also passed several CCPA amendments in 2020, including an extension of the employee personal information and business-to-business communication exemptions until January 1, 2022, which the CPRA instead extended to January 1, 2023 (see CPRA; for more on CCPA amendments, see Practice Note, CCPA Proposed Amendments and Other California Privacy-Related Legislation Tracker: Enacted CCPA Amendments).

For more on the CCPA, see California Consumer Privacy Act (CCPA) Toolkit.

Final CCPA Regulations

The California Attorney General (CAG) released final CCPA implementing regulations, effective August 14, 2020, after extensive proposal and commenting activities. The regulations (Cal. Code Regs., tit. 11, §§ 999.300 to 999.337) clarify the law's requirements, for example, by:

- Requiring every covered business to provide a compliant privacy policy (Cal. Code Regs., tit. 11, § 999.304).
- Prescribing how businesses must satisfy notice requirements at or before the time of collection, including just-in-time notice when they collect personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect (Cal. Code Regs., tit. 11, § 999.305(a)(4)).
- Specifying:
  - the content and means for providing right to opt-out of personal information sales notices; and
  - methods for businesses' handling of consumers' requests to know and requests to delete.

  (Cal. Code Regs., tit. 11, §§ 999.306 and 999.312 to 313).

For more on the final regulations, see Legal Update, Final CCPA Regulations Approved. Even after finalizing the regulations, the CAG has continued to further refine them, offering proposed regulatory changes in December 2020 to clarify the consumer opt-out process and provide a uniform opt-out button design. For more, see Legal Update, Fourth Set of Proposed Modifications to CCPA Regulations Released for Comment.

CCPA Litigation

2020 brought the first lawsuits under the CCPA's private right of action, which permits claims for unauthorized access, theft, or disclosure of nonencrypted and nonredacted personal information due to a business's failure to implement reasonable security practices and procedures (Cal. Civ. Code § 1798.150(a)(1)).

For example, consumers brought a proposed class action against children's retailer Hanna Andersson LLC concerning a 2019 data breach, in what was reportedly the first data breach-related action to plead CCPA claims. The retailer ultimately reached a $400,000 proposed settlement to resolve the cases. (Order Granting Motion for Preliminary Approval of Class Settlement, *In re Hanna Andersson & Salesforce.com Data Breach Litig.*, No. 20-812 (N.D. Cal. Dec. 29, 2020).) Other cases continue to move through the courts.

CPRA

The CPRA, which voters approved on November 3, 2020, amends and generally expands the CCPA's scope, for example by:

- Establishing the California Privacy Protection Agency (CPPA), which will:
  - assume rulemaking authority for CCPA and CPRA regulations; and
  - share enforcement authority with the CAG.
- Defining a new category of sensitive personal information.
- Changing and expanding some current and creating new consumers' rights, including rights to:
  - correct inaccurate personal information;
  - opt out of sharing personal information; and
  - restrict sensitive information processing.
- Treating some forms of sharing personal information similarly to selling personal information under the CCPA.
- Defining "contractors," which resemble service providers under the CCPA and requiring certain contract terms.
- Prohibiting obtaining consent using dark patterns, which are user interface features designed to subvert or impair users' autonomy, decision-making, or choice.
- Potentially reducing the CCPA's scope, for example by:
  - increasing the threshold for covered business to those that alone or in combination annually buy, sell, or share the personal information of 100,000 or more consumers, from the CCPA's 50,000; and
  - expressly allowing loyalty or rewards programs consistent with the law.

- Expanding the circumstances when organizations must minimize their activities involving personal information (data minimization).
- Requiring certain organizations to perform annual independent cybersecurity audits and submit annual privacy risk assessments to the CPPA.

The CPRA becomes operative on January 1, 2023, applies only to personal information collected on or after January 1, 2022, with some exceptions, and delays enforcement until July 1, 2023. For more on the CPRA, see Article, Expert Q&A: The California Privacy Rights Act of 2020 (CPRA).

Federal Guidance, Regulation, and Enforcement

Several federal agencies issued guidance and took privacy and data security enforcement actions in 2020, including:

- The FTC (see FTC).
- The HHS (see HHS).
- The Department of Commerce and NIST (see Department of Commerce and NIST).
- The FCC (see FCC).
- The Securities and Exchange Commission (see SEC).
- Various other agencies (see Other Federal Regulatory Developments).

Federal agencies also continued to partner with state enforcement efforts, especially in higher-profile multistate actions (see Multistate Enforcement Actions).

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 Guidance

In 2020, the FTC sought public comments on possible changes to its Health Breach Notification Rule, which requires vendors of personal health records and related entities to notify consumers following a breach involving unsecured information (16 C.F.R. §§ 318.1 to 318.9).

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

- **Artificial intelligence (AI).** In April, the FTC published a blog post on AI and automated decision-making, advising companies to:
  - avoid deceiving consumers on how they use automated tools;
  - be transparent when collecting sensitive data and testing an AI system to ensure it does not create a discriminatory impact on protected classes; and
  - ensure that any AI tools use that involves providing consumers' data to others to make decisions about access to credit, employment, insurance, or other covered transactions complies with the Fair Credit Reporting Act (FCRA).
- **Social media bots.** In July, the FTC released a report outlining beneficial and potentially deceptive bot uses on social media, including using bots for click fraud, fake followers, misinformation, harassment, or to distribute malware. The report also discussed the agency's legal authority to counteract the spread of harmful social media bots under the FTC Act. (See Legal Update, FTC Issues Report to Congress on Social Media Bots and Deceptive Advertising.)
- **Do not call registry.** In October, the FTC released its National Do Not Call Registry Data Book for Fiscal Year 2020, which analyzes the more than 3.9 million Do Not Call complaints the agency received.

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. Key 2020 actions more generally demonstrate that companies should:

- **Ensure that privacy and data security practices match promises.** For example, the FTC reached settlements with:
  - a Canadian smart lock maker that allegedly deceived consumers by falsely claiming that its internet-connected smart locks were designed to be "unbreakable" and that it took reasonable steps to secure the data it collected from users (*In re Tapplock, Inc.*, 2020 WL 2745379 (F.T.C. May 18, 2020)); and
  - a videoconferencing company that allegedly made misleading claims about its encryption and cloud storage practices (*In re Zoom Video Comm'cns, Inc.*, 2020 WL 6589816 (F.T.C. Nov. 9, 2020); see Legal Update, FTC Settlement Requires Zoom to Enhance Information Security Program.)

For more on FTC enforcement concerning organizations' misrepresentations about their data security practices, see Practice Note, FTC Data Security Standards and Enforcement.

- **Protect children by complying with COPPA obligations.** For example, the FTC reached settlements with:
  - a children's app developer concerning allegations it allowed third-party ad networks to collect persistent identifiers that tracked app users without verifiable parental consent (Proposed Stipulated Order for Permanent Injunction and Civil Penalty Judgment, *United States v. Hyperbeard, Inc.*, No. 20-3683 (N.D. Cal. June 4, 2020)); and
  - a Swiss-based digital game developer concerning allegations it falsely claimed that it was a member of the Children's Advertising Review Unit's COPPA safe harbor program even though its membership terminated in 2015 (*In re Miniclip, S.A.*, 2020 WL 3819205 (F.T.C. June 29, 2020)).

  For more on COPPA enforcement, see Practice Note, Children's Online Privacy: COPPA Compliance: COPPA Federal and State Enforcement Actions.
- **Reasonably secure health and other sensitive data.** A travel emergency service settled allegations that it failed to take reasonable steps to secure health data and sensitive consumer information by leaving personal data in an unsecured online database, deceptively displaying a "HIPAA Compliance" seal on its web pages, and failing to adequately notify customers following a potential breach. (*In re SkyMed Int'l Inc.*, No. C-4732 (F.T.C. Jan. 26, 2021).)
- **Properly oversee third-party vendors' security practices.** The FTC settled with Ascension Data & Analytics, LLC concerning allegations the company violated the Gramm-Leach-Bliley Act's Safeguards Rule (16 C.F.R. §§ 314.1 to 314.5) by failing to ensure that its vendor adequately secured mortgage holders' personal data (see Legal Update, FTC Agrees to Settle with Ascension Over Alleged Vendor Oversight Failures).
- **Comply with consumer records requests under the FCRA.** For example, the FTC reached a $220,000 settlement to resolve FCRA violation claims against a national retailer that allegedly refused to provide complete transaction records to consumers suffering identity theft (Stipulated Order for Permanent Injunction, Other Equitable Relief, and Civil Penalty, *United States v. Kohl's Dep't Stores, Inc.*, No. 20-859 (E.D. Wis. June 10, 2020); see Legal Update, FTC Settles Claims Kohl's Failed to Give Identity Theft Victims FCRA Required Information.)
- **Perform reasonable diligence to prevent illegal robocalls**. The FTC settled its first consumer protection case against a VoIP service provider, partnering with the State of Ohio to reach an agreement with the provider and an affiliated company for $1.9 million, plus additional individual penalties, concerning claims that they helped support fraudulent credit card interest rate relief. The VoIP provider agreed:
  - not to provide services to clients paying with stored value cards or cryptocurrency;
  - to perform due diligence on potential clients; and
  - to block spoofed and other calls from suspicious numbers.

  (FTC: Globex Telecom and Associates Will Pay $2.1 Million, Settling FTC's First Consumer Protection Case Against a VoIP Service Provider (Sept. 22, 2020).)
- **Make accurate representations about their cross-border data transfer practices.** The FTC continued its stepped up enforcement of companies' allegedly false or misleading statements about their participation in the EU-US Privacy Shield, the Swiss-US Privacy Shield, and the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system. The FTC settled allegations with multiple companies and sent warning letters to others throughout the year. (See, for example, Decision and Order, *In re NTT Global Data Ctrs. Ams., Inc.*, No. 182 3189 (F.T.C. Oct. 28, 2020); Decision and Order, *T&M Protection Res., LLC*, No. 192 3092 (F.T.C. Mar. 16, 2020); Decision and Order, *In re Ortho-Clinical Diagnostics, Inc.*, No. 192 3050 (F.T.C. July 8, 2020).)

HHS

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

HHS Guidance

In 2020, HHS:

- Finalized amendments to regulations protecting substance use disorder treatment patient records that improve coordination across health care providers (42 C.F.R. §§ 2.1 to 2.67; see SAMHSA: Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule). HHS plans to further revise these regulations consistent with the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) (Pub. L. No. 116-136).

- Jointly released a ransomware advisory with the FBI and CISA in October warning of an increased threat of cybercrime and ransomware attacks against US hospitals and health care providers.
- Finalized rules to address electronic health records interoperability and information blocking, increasing care coordination and individuals' access to their health data and establishing standard application programming interface (API) requirements, consistent with the 21st Century Cures Act (Pub. L. No. 114-255) (85 Fed. Reg. 25510-01 (May 1, 2020); 85 Fed. Reg. 25642-01 (May 1, 2020))
- Proposed changes to the HIPAA Privacy Rule aiming to further improve care coordination and individuals' access to their protected health information (PHI) and provide covered entities with more flexibility in some limited circumstances (86 Fed. Reg. 6446-01 (Jan. 21, 2021)).

HHS Enforcement Activity

OCR settled several notable HIPAA enforcement actions in 2020, highlighting that companies should:

- **Conduct a thorough data security risk analysis and implement effective safeguards**. Several organizations agreed to settle potential HIPAA violations and implement corrective action plans for incidents involving third-party misconduct, including:
  - Premera Blue Cross, which agreed to pay $6.85 million following a phishing incident leading to a network intrusion, resulting in the disclosure of more than 10.4 million individuals' PHI (see Legal Update, Cyber-Attackers' Theft of Over Ten Million Individuals' PHI Leads to $6.85 Million HIPAA Settlement);
  - Lifespan Health System Affiliated, which agreed to pay $1.04 million for alleged violations following the theft of an unencrypted laptop (see Legal Update, In $1 Million HIPAA Settlement, HHS Emphasizes Business Associate and Encryption Compliance);
  - Aetna Life Insurance Company, which agreed to pay $1 million pertaining to three data breaches that involved public access to individuals' plan-related documents and PHI impermissibly disclosed through envelopes' windows (see Legal Update, HIV-Related Disclosures (and More) Lead to $1 Million HIPAA Settlement);
  - HIPAA business associate, CHSPSC LLC, agreed to pay $2.3 million stemming from a data breach that used compromised administrative credentials to expose more than six million individuals' PHI (see Legal Update, Hacker's Theft of Over Six Million Individuals' PHI Leads to $2.3 Million HIPAA Settlement); and
  - Athens Orthopedic Clinic PA, which agreed to pay $1.5 million following a hacking incident involving stolen credentials and unauthorized access to their electronic health records (see Legal Update, Hacker Group's Impermissible Access to ePHI Leads to $1.5 Million HIPAA Settlement).
- **Support required patient access to PHI.** HHS continued increased enforcement under its Right of Access Initiative throughout 2020, culminating in its twelfth related action in November. The initiative continues with HHS already announcing further settlements with additional covered entities in early 2021.
- **Ensure termination of former employees' network access.** The City of New Haven, Connecticut agreed to pay $202,400 and implement a corrective action plan after a former employee apparently accessed patients' PHI by returning to the workplace eight days after termination and logging into its systems using her still-active credentials (see Legal Update, Terminated Employee's Unauthorized Access to HIPAA PHI Sparks HHS Investigation).

In early 2021, the US Court of Appeals for the Fifth Circuit issued a potentially wide-reaching decision for disputes involving civil money penalties levied against HIPAA covered entities when it vacated a $4.3 million assessment (see Legal Update, Fifth Circuit: HHS's HIPAA Enforcement Was "Arbitrary, Capricious, and Contrary to Law").

Department of Commerce and NIST

The Department of Commerce has issued guidance on and entered into renegotiations concerning a new cross-border data transfer mechanism following the invalidation of the EU-US Privacy Shield (see ECJ Opinions and Schrems II). The Department's NIST component maintained its leadership role in setting cybersecurity and privacy standards.

Notable 2020 NIST activities included:

- Starting the year off publishing version 1.0 of its eagerly anticipated NIST Privacy Framework, which follows the structure of its influential NIST Cybersecurity Framework (see Legal Update, NIST Releases Privacy Framework).

- Releasing a new revision, further updates, and supporting materials for its widely used Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations.
- Updating its key federal contractor data security standard, NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, which provides guidance to agencies on securing controlled unclassified information in various settings, including when using external service providers. Agencies often apply the standard when engaging contractors.
- Publishing its revised NIST Special Publication 800-181 Workforce Framework for Cybersecurity (NICE Framework), which helps organizations improve methods to identify, recruit, develop, and retain cybersecurity talent.
- Releasing NIST Special Publication 1800-11 Data Integrity: Recovering from Ransomware and Other Destructive Events, which helps organizations develop strategies to identify and protect their assets against ransomware and other major cyber events.
- Providing cybersecurity guidance for the hospitality industry, including offering solutions on securing property management systems and connections to internal and external systems.
- Publishing reports on Internet of Things (IoT) security, an IoT Device Cybersecurity Capability Core Baseline, and Foundational Cybersecurity Activities for IoT Device Manufacturers, which provide recommendations to help manufacturers address IoT cybersecurity in their product development processes.

FCC

The Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) (Pub. L. No. 116-105), enacted in 2019, gave the FCC additional tools to combat unwanted robocalls and scam calls under the TCPA. In 2020, the agency adopted rules that:

- Require all voice service providers to implement the Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) caller ID authentication standards to combat malicious caller ID spoofing (*In re Call Authentication Tr. Anchor*, No. 20-67, 2020 WL 1634553, at *1 (F.C.C. Mar. 31, 2020); see Legal Updates, FCC Requires Voice Service Providers to Use STIR/SHAKEN to Combat Spoofed Robocalls and FCC Adopts New Rules to Clarify STIR/SHAKEN Implementation to Combat Spoofed Robocalls).
- Permit voice service providers to block calls from numbers associated with illegal one-ring scams (*In re Protecting Consumers from One-Ring Scams*, No. CG20-93, 2020 WL 7068399 (F.C.C. Nov. 30, 2020)).
- Restrict non-telemarketing robocalls to consumers' home phones (*In re Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991*, No. CG02-278, 2020 WL 7873750 (F.C.C. Dec. 30, 2020)).
- Require terminating voice service providers to police their networks to block illegal robocalls (*In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, No. CG17-59, 2020 WL 7873751 (F.C.C. Dec. 30, 2020)).
- Provide safe harbors to protect phone companies from liability for unintended or inadvertent blocking of wanted calls if the provider:
  - uses reasonable analytics to block illegal or unwanted robocalls; or
  - blocks call traffic from bad actor upstream voice service providers that were on notice to stop their illegal calls.

  (*In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, No. CG17-59, 2020 WL 4187350 (F.C.C. July 17, 2020).)

In 2020, the FCC also highlighted two related consumer privacy issues:

- **Call spoofing.** The FCC:
  - proposed a record $225 million fine against telemarketers for making approximately one billion spoofed robocalls to consumers, including those on the Do Not Call List (see Legal Update, FCC Proposes Record $225 Million Fine Against Telemarketers for Making 1 Billion Spoofed Robocalls);
  - issued a $37.5 million forfeiture order for making millions of illegally spoofed telemarketing calls in violation of the Truth in Caller ID Act (47 U.S.C. § 227(e)); and
  - fined a California telemarketer nearly $10 million for making more than 47,000 spoofed robocalls leveling false accusations against a local political candidate, in violation of the Truth in Caller ID Act (see Legal Update, FCC Fines California Telemarketer Nearly $10 Million for Spoofed Election-Related Robocalls).
- **TCPA robocall restrictions.** The FCC issued a reconsideration order clarifying that the TCPA's restrictions requiring prior express consent for robocalls apply to federal and state government contractors but not to the federal or state governments themselves (*In re Rules & Regulations Implementing the Tel. Consumer*

Prot. Act of 1991, No. CG02-278, 2020 WL 7383274 (F.C.C. Dec. 14, 2020)).

The FCC was also active against the perceived national security threat posed by Chinese telecom company and 5G equipment vendor Huawei Technologies Company, for example by:

- Designating Huawei a "covered company," precluding US carriers from using FCC Universal Service Funds to purchase, obtain, maintain, improve, modify, or otherwise support Hauwei equipment or services. (*In re Protecting Against Nat'l Sec. Threats to the Commc'ns Supply Chain Through FCC Programs - Huawei Designation*, No. DA20-690, 2020 WL 3566005 (F.C.C. June 30, 2020), affirmed by *In re Protecting Against Nat'l Sec. Threats to the Commc'ns Supply Chain Through FCC Programs - Huawei Designation*, No. FCC20-179, 2020 WL 7351129 (F.C.C. Dec. 11, 2020).)
- Ordering US carriers to remove and replace designated security risk network assets, such as Huawei equipment and services, under the Secure and Trusted Communications Networks Act of 2019 (Pub. L. No. 116-124) (*In re Protecting Against Nat'l Sec. Threats to the Commc'ns Supply Chain Through FCC Programs*, No. FCC20-176, 2020 WL 7351126 (F.C.C. Dec. 11, 2020)).

SEC

The SEC issued guidance on data security and risk management for public companies in 2020. Notable resources from the Office of Compliance Inspections and Examinations (OCIE) included:

- Examination observations on market participants' cybersecurity and operational resiliency practices. The report highlights specific examples of effective cybersecurity program practices and procedures (Legal Update, SEC Publishes Cybersecurity and Resiliency Observations).
- A risk alert on increasingly sophisticated ransomware attacks against SEC registrants and their service providers. The alert offers tips on security measures and encourages organizations to monitor CISA alerts about evolving tactics and techniques used by threat actors (SEC: OCIE, Cybersecurity: Ransomware Alert (July 10, 2020)).

Other Federal Regulatory Developments

Other key federal agencies and entities active in privacy and data security for 2020 include:

- The Office of the Comptroller of the Currency (OCC), which:
  - assessed an $80 million penalty against a financial institution for its failure to establish effective risk assessment processes and network security controls for cloud operations (see Legal Update, OCC Settles with Capital One Over Information Security Failures), with the event prompting a class action (*In re Capital One Customer Data Security Breach Litig.*, 2020 WL 5629790 (E.D. Va. Sept. 18, 2020) (denying motion to dismiss)); and
  - in early 2021, with other banking regulators, proposed heightened cyber incident reporting obligations (see Legal Update, Federal Banking Agencies Propose Requirements for Computer Security Incident Notification).
- The Consumer Financial Protection Bureau (CFPB), which:
  - issued an advance notice of proposed rulemaking requesting information on consumer access to financial records under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act); and
  - reached a $1.3 million settlement with payday lender Cottonwood Financial, Ltd. that allegedly violated the FCRA by not maintaining adequate policies for the accuracy and integrity of the information it furnished to consumer reporting agencies (*Cottonwood Fin. Ltd., d/b/a Cash Store*, 2020 WL 8182126 (C.F.P.B. Apr. 1, 2020)).
- CISA, which continued to offer cybersecurity advisories and released its CISA 5G Strategy aiming to:
  - ensure the security and resilience of 5G technology;
  - engage with the private sector on governance and technical guidance;
  - expand situational awareness of 5G supply chain risks; and
  - collaborate with national laboratory and technology centers to evaluate key existing 5G components for security vulnerabilities.
- The Department of the Treasury, which issued ransomware-related advisories, including:
  - an Office of Foreign Assets Control (OFAC) advisory warning that organizations, such as financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, that facilitate ransomware payments to hackers may face scrutiny for potential violations of anti-money laundering and sanctions regulations; and

  - a Financial Crimes Enforcement Network (FinCEN) advisory on financial intermediaries' role in processing of ransomware payments.

  (See Legal Update, US Department of Treasury Issues Warning on Facilitating Ransomware Payments.)

- The Government Accountability Office (GAO), which released reports on:
  - facial recognition technology, suggesting Congress consider strengthening the consumer privacy framework surrounding facial recognition to reflect technological changes; and
  - student data security, examining cybersecurity breaches that compromised K-12 student data from July 2016 through early May 2020 and the vulnerabilities exploited.
- The White House, which issued several executive orders with a privacy or data security nexus, including:
  - guidance for federal agencies and private sector organizations when developing regulatory and non-regulatory approaches regarding artificial intelligence (AI) (Office of Management and Budget (OMB), Draft Guidance for Regulation of Artificial Intelligence Applications (Jan. 7, 2020); OMB, Guidance for Regulation of Artificial Intelligence Applications (Nov. 17, 2020));
  - Executive Order 13905, Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services, concerning cyber resilience of critical infrastructure systems if a disruption to GPS or other position, navigation and timing services occurs; and
  - Executive Order 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, outlining principles for government artificial intelligence (AI) use for purposes other than national security.

State Regulation and Enforcement

State Regulations

Key 2020 regulatory developments at the state level included:

- The CAG's release of final CCPA regulations (see Final CCPA Regulations).
- New York's updated student data protection regulations taking effect, which require school districts, state-supported schools, and their vendors to develop best practices-based cybersecurity programs to protect personal information (8 NYCRR §§ 121.1 to 121.14).

Single-State Enforcement Actions

Key single-state enforcement actions in 2020 focused primarily on:

- Data breaches and security vulnerabilities (see Data Breaches and Security Failures).
- Location tracking practices (see Location Tracking Practices).
- Biometric information privacy and use (see Biometrics Privacy).
- Children's privacy (see Children's Privacy).

Data Breaches and Security Failures

State regulators continued to focus their enforcement efforts on large-scale data breaches and inadequate privacy and security safeguards, including:

- California, which reached a $250,000 settlement with the operator of Glow, Inc., a women's fertility app, following an investigation of privacy and security lapses that put women's highly sensitive personal and health information at risk (see Legal Update, California AG Resolves Fertility App Privacy Breach Investigation).
- Indiana, which opted not to join a 2019 multistate settlement with Equifax, Inc. concerning its 2017 breach, instead reaching a $19.5 million settlement with the company (*State of Indiana v. Equifax, Inc.*, No. 49D01-1905-PL-018398 (Ind. Super. Ct. Apr. 14, 2020)).
- New Jersey, which reached a $235,000 settlement with supermarket retailer Wakefern Food Corp. stemming from a 2016 data breach caused by the retailer's inadequate data disposal practices (Consent Order, *In re Wakefern Food Corp.* (N.J. Dept. of Law Oct. 9, 2020)).
- New York, which:
  - filed its first action under the New York State Department of Finance Services (NYDFS) Cybersecurity Regulations (23 NYCRR §§ 500.0 to 500.23) against First American Title Insurance Company alleging that a vulnerability in the company's systems exposed hundreds of millions of documents (see Article, Expert Q&A on Lessons Learned from the First NYDFS Cybersecurity Enforcement Action);
  - reached an agreement with videoconferencing company Zoom Video Communications, Inc. to implement a comprehensive data security program, resolving an investigation into the company's security vulnerabilities and privacy practices, following an agreement with the New York City Department of Education (DOE) for enhanced Zoom protections; and
  - reached a $650,000 settlement with franchisor Dunkin' Brands, Inc. resolving a lawsuit concerning

the company's failure to respond to 2015 cyberattacks that compromised tens of thousands of customers' online accounts (Consent Order, *New York v. Dunkin' Brands, Inc.*, No. 451787/2019 (N.Y. Sup. Ct. Sept. 22, 2020)).

Location Tracking Practices

State authorities took aim at location tracking practices, including:

- Arizona, which brought suit against Google LLC under its state consumer protection law concerning the company's location data collection practices, including allegedly collecting users' location information even when they turn off the Location History setting (Complaint, *Arizona v. Google LLC*, No. 2020-6219 (Ariz. Super Ct. May 27, 2020)).
- California, which reached a settlement with the operator of The Weather Channel (TWC) mobile phone app, resolving a 2019 lawsuit that was one of the first state enforcement actions to address mobile device location data collection (*California v. TWC Prod. & Tech., LLC*, No. 19STCV00605 (Cal. Super., L.A. Cty., Stipulation Aug. 14, 2020)). The state filed suit before the CCPA took effect and before both the Apple and Android mobile platforms adopted increasingly restrictive developer policies on location data sharing.

Biometrics Privacy

State authorities increasingly recognized the sensitivity and privacy concerns surrounding biometric data. For example, on March 10, 2020, Vermont Attorney General T.J. Donovan filed suit in state court against facial recognition company Clearview AI. Vermont's complaint:

- Notes that Clearview is a registered data broker (9 V.S.A. §§ 2430 to 2431; see Legal Update, Vermont Enacts First Data Broker Law).
- Alleges violations of the state's consumer protection and data broker laws concerning the techniques it uses to acquire images (Vt. AG: Attorney General Donovan Sues Clearview AI for Violations of Consumer Protection Act and Data Broker Law (Mar. 10, 2020)).

Vermont later prevailed on the company's initial motion to dismiss (*State v. Clearview AI, Inc.*, No 226-3-20 Cncv (Vt. Super. Ct. Sept. 10, 2020)).

Children's Privacy

Various states pursued children's privacy enforcement efforts, including:

- New Mexico, which brought claims against Google, alleging that its G Suite education software collected students' personal information for commercial purposes without first obtaining parental consent in violation of COPPA and state law. A district court dismissed the claims, finding that Google used schools as intermediaries or the parent's agent in the notice-and-consent process, consistent with FTC guidance. (*New Mexico ex rel. Balderas v. Google, LLC*, 2020 WL 5748353 (D.N.M. Sept. 25, 2020) (on appeal to the US Court of Appeals for the Tenth Circuit).)
- Washington, which reached a $100,000 settlement (suspended from $500,000) with social media platform operator Super Basic, LLC concerning the platform's practice of permitting children to create accounts, collecting their personal information, and allowing third-party advertisers to collect their data, without first obtaining parental consent (Consent Order, *Washington v. Super Basic, LLC* (Wash. Super. Ct. June 23, 2020)).

Multistate Enforcement Actions

The trend of multistate and federal-state cooperation in privacy enforcement continued in 2020. For example:

- Anthem, Inc., agreed to pay $39.5 million and enact a series of data and information security measures in a settlement with 42 states and the District of Columbia concerning a 2014 data breach that compromised 78.8 million customers' personal information (N.Y. AG: Attorney General James Helps Secure $39.5 Million After Anthem's 2014 Data Breach (Sept. 30, 2020)).
- CHS/Community Health Systems, Inc. and its subsidiary, CHSPSC LLC, agreed to pay $5 million and implement and maintain a comprehensive security program in a settlement with 28 states concerning a 2014 data breach that impacted approximately 6.1 million individuals (N.C. AG: Attorney General Josh Stein Announces $5 Million Settlement with Community Health Systems (Oct. 8, 2020)).
- Home Depot USA, Inc. agreed to pay $17.5 million and implement various measures to strengthen its information security program, including employing a chief information security officer, in a settlement with 45 states and the District of Columbia concerning a 2014 data breach affecting approximately 40 million consumers nationwide (Cal. AG: Attorney General Becerra Announces $17.5 Million Settlement Against Home Depot Over Credit Card Data Breach (Nov. 24, 2020)).
- DISH Network L.L.C. agreed to pay $210 million and comply with strict telemarketing restrictions in a settlement of the long-running dispute with the US

Department of Justice (DOJ) and California, Illinois, North Carolina, and Ohio for violations of the FTC's Telemarketing Sales Rule (TSR) (DOJ: DISH Network to Pay $210 Million for Telemarketing Violations (Dec. 7, 2020)).

- The online retailer CafePress, LLC reached a $2 million settlement with seven states concerning a 2019 data breach that affected 22 million users (N.Y. AG: Attorney General James Announces $2 Million Agreement with CafePress After Data Breach (Dec. 18, 2020)).

Private Litigation

Private litigation highlights and trends for 2020 focused on:

- Data breach-related actions (see Data Breach Litigation).
- Biometrics (see Biometrics Privacy Litigation).
- Cases brought under the TCPA (see TCPA Cases).
- Other privacy and data security-related topics (see Other Notable Cases).

Data Breach Litigation

Standing remained a key issue in 2020 for data breach actions in federal courts. For example, courts found that plaintiffs were unable to satisfy the injury-in-fact required to sustain Article III standing where there was no evidence that the plaintiff's information was used fraudulently or improperly accessed (see, for example, *Hartigan v. Macy's, Inc.*, 2020 WL 6523124, at *4 (D. Mass. Nov. 5, 2020); *Stasi v. Inmediata Health Grp. Corp.*, 2020 WL 2126317, at *4-9 (S.D. Cal. May 5, 2020)).

2020 data breach litigation also revealed:

- **Forensic breach assessment reports may not be protected by the work product doctrine.** A district court compelled production of a third-party cybersecurity breach assessment report where the court found that the defendant would have commissioned the incident response services in a substantially similar form even without the prospect of litigation. (*In re Capital One Consumer Data Sec. Breach Litig.*, 2020 WL 3470261, at *5 (E.D. Va. June 25, 2020).)
- **Language describing security vulnerabilities rather than "data breaches" may not sustain securities fraud claims.** The US Court of Appeals for the Ninth Circuit affirmed a district court's dismissal of a proposed class action brought by investors where the plaintiffs failed to show a "cogent and compelling inference" that PayPal's announcement that it found "security vulnerabilities" in the network of a new acquisition, rather than describing an actual security breach, was intentionally misleading. (*Eckert v. PayPal Holdings Inc.*, 831 F. App'x 366, 367 (9th Cir. 2020).)

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

- Kalispell Regional Healthcare, which agreed to pay $4.2 million, including credit monitoring services costs, following a 2019 phishing attack and data breach affecting 13,000 patients' PHI (*Henderson v. Kalispell Reg'l Healthcare*, No. CDV-19-0761 (Mont. Dist. Ct. Nov. 25, 2020)).
- Equifax, which agreed to pay:
  - $30.5 million to resolve claims by a class of financial institution plaintiffs stemming from a 2017 data breach, with most of the funds directed to data security measures (Final Order and Judgment, *In re: Equifax, Inc. Customer Data Sec. Breach Litig.*, No. 17-md-2800 (N.D. Ga. Nov. 16, 2020)); and
  - $149 million to resolve consolidated securities litigation brought by investors related to the 2017 data breach's effect on the company's stock (Stipulation and Order, *In re: Equifax, Inc. Customer Data Sec. Breach Litig.*, No. 17-cv-03463 (N.D. Ga. Feb. 3, 2020)).
- Google, which agreed to pay $7.5 million to resolve claims arising out of a 2018 software bug in its now-defunct Google+ social media platform that may have exposed up to 500,000 Google+ users' profile information (*In re Google Plus Profile Litig.*, 2021 WL 242887 (N.D. Cal. Jan. 25, 2021) (order granting final approval of class settlement)).

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

Biometric Information Privacy Act Litigation

Litigation under Illinois's Biometric Information Privacy Act (BIPA) (740 ILCS 14/1) remained robust in 2020, following the Illinois Supreme Court's 2019 ruling that BIPA does not require individuals to suffer 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).

Numerous BIPA actions have been filed against various entities, including businesses, social media platforms, cloud storage providers, and employers using biometric timekeeping systems (see, for example, Preliminary Approval Order, *Jones v. CBC Rest. Corp.*, No. 19-06736 (N.D. Ill. June 12, 2020) (preliminarily approving a $3.2 million class settlement of BIPA violations related to fingerprint collection for timekeeping purposes)).

Some notable decisions concerned:

- **Preemption.** One district court found that federal labor law preempted BIPA claims related to the collection and retention of employee fingerprints where a collective bargaining agreement was in place (*Fernandez v. Kerry Inc.*, 2020 WL 7027587, at *7 (N.D. Ill. Nov. 30, 2020)), while another district court rejected arguments that similar claims were preempted by the state Workers' Compensation Act (*Burlinski v. Top Golf USA Inc.*, 2020 WL 5253150, at *6 (N.D. Ill. Sept. 3, 2020)).
- **BIPA's patient-in-a-health care-setting exception.** A district court found that the BIPA exception for collecting patient biometric information in a health care setting does not extend to plasma donors selling plasma to a plasma donation center (*Marsh v. CSL Plasma, Inc.*, 2020 WL 7027720, at *5 (N.D. Ill. Nov. 30, 2020)).
- **Unlawful data retention policies as a basis for Article III standing.** In a pair of decisions, the US Court of Appeals for the Seventh Circuit examined Article III standing issues surrounding whether a company's failure to develop, publicly disclose, and comply with data retention and destruction policies consistent with BIPA presents a concrete and particularized injury-in-fact of a legally protected privacy right, with slightly divergent results based on the specific claims made (*Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146, 1152-56 (7th Cir. 2020); *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617 (7th Cir. 2020); see Legal Update, Unlawful Retention of Biometric Data Under BIPA Supports Article III Standing: Seventh Circuit).

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 2020, including a steady stream of class settlements. Key litigated issued included:

- **The automatic telephone dialing system (ATDS) definition.** In December 2020, the Supreme Court heard arguments addressing 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 (compare, for example, *Duran v. La Boom Disco, Inc.*, 955 F.3d 279, 283-84 (2d Cir. 2020) (adopting a broad view of an ATDS to include devices that store and call telephone numbers that were not generated by a random or sequential number generator) with *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 464-65, 469 (7th Cir. 2020) (taking a narrow view and holding that the defendant's use of a customer feedback tool that selects numbers stored in a customer database to generate automated texts to those numbers did not amount to the use of an ATDS)).
- **The government debt exemption.** The Supreme Court invalidated the short-lived "government-debt exception," which permitted robocalls to collect debts owed to or guaranteed by the federal government, finding the exception was an unconstitutional content-based restriction on speech (*Barr v. Am. Assoc. of Political Consultants, Inc.*, 140 S. Ct. 2335, 2347-48 (2020); Legal Update, SCOTUS Strikes Down TCPA Government Debt Exception).
- **How to determine the level of deference courts should afford FCC interpretative rules.** On remand from the Supreme Court, the US Court of Appeals for the Fourth Circuit found that because the parties agreed that the FCC's ruling on the meaning of "unsolicited advertisement" in the TCPA was interpretive rather than legislative, four key standards should guide the district court when determining how much deference to give the FCC's interpretation (*Carlton & Harris Chiropractic, Inc. v. PDR Network, LLC*, 982 F.3d 258, 263-64 (4th Cir. 2020)).
- **Standing.** The US Court of Appeals for the Eleventh Circuit dismissed a plaintiff's claim for lack of standing based on failure to prove a cognizable injury where the plaintiff did not show that receiving a single prerecorded voicemail rendered their phone unavailable to receive legitimate calls or messages for any period of time (*Grigorian v. FCA US LLC*, 2020 WL 7238392, at *3 (11th Cir. 2020)).

- **A consumer's ability to revoke consent.** The Eleventh Circuit held that the TCPA does not permit consumers to unilaterally revoke their consent to receive automated calls or texts if they consented in a bargained-for contract to receive automated calls (*Medley v. Dish Network, LLC*, 958 F.3d 1063, 1069 (11th Cir. 2020)).

Other Notable Cases

Other notable privacy and data security-related litigation and settlements in 2020 included those addressing:

- **The Computer Fraud and Abuse Act (CFAA).** Key 2020 cases focused on:
  - whether someone exceeds authorized access for purposes of a CFAA violation if they access a computer for improper purposes or in violation of use restrictions (*Van Buren v. United States,* 140 S. Ct. 2667 (2020) (cert. granted; argued Nov. 30, 2020) (considering the CFAA's criminal provisions on unauthorized access); see, for example, *Royal Truck & Trailer Sales & Serv., Inc. v. Kraft*, 974 F. 3d 756, 759-61 (6th Cir. 2020) (considering what constitutes unauthorized access for CFAA civil liability); Legal Update, Sixth Circuit Requires More Than Misuse to Exceed Authorized Access Under CFAA);
  - whether scraping publicly available website data provides grounds for CFAA liability (*hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1003-04 (9th Cir. 2019), petition for cert. pending, No. 19-1116 (filed Mar. 9, 2020)); and
  - when the statute of limitations is triggered (*Radcliff v. Radcliff*, 2020 WL 7090687, at *6 (D.N.J. Dec. 4, 2020) (finding that the statute of limitations on the plaintiff's CFAA claims began when they learned that their account's or computer's integrity was impaired, not when they learned of the exact extent of the defendant's involvement in the intrusion)).

  For more on the CFAA, see Practice Note, US Privacy Litigation: Overview: Computer Fraud Abuse Act (CFAA).
- **The scope of electronic storage under the Stored Communications Act (SCA).** The Ninth Circuit found that fact issues on whether the plaintiff's law firm work emails were in electronic storage for backup purposes, as required for SCA protection, precluded summary judgment on an SCA claim alleging unauthorized access to the emails. The court rejected any distinction between the protection afforded to "service copies" immediately accessible to a user and "storage copies" that are less conveniently accessible. (*Clare v. Clare*, 982 F.3d 1199, 1202-03 (9th Cir. 2020).) For more on the SCA, see Practice Note, US Privacy Litigation: Overview: Electronic Communications Privacy Act (ECPA).
- **The federal criminal identity theft statute (18 U.S.C. § 1028A).** The US Court of Appeals for the Fifth Circuit upheld a Medicare fraud and aggravated identity theft conviction under the infrequently invoked federal criminal identity theft statute (*United States v. Dubin*, 982 F.3d 318, 324, 325-27 (5th Cir. 2020)).
- **The Driver's Privacy Protection Act (DPPA).** A company reached an injunctive relief only class settlement and promised to institute new business practices to resolve DPPA claims concerning selling Department of Motor Vehicles crash reports at the direction of its law enforcement agency customers (Proposed Settlement Agreement and Release, *Gaston v. LexisNexis Risk Sols. Inc.*, No. 16-00009 (W.D.N.C. Nov. 3, 2020)). For more on the DPPA, see Practice Note, US Privacy Litigation: Overview: Driver's Privacy Protection Act (DPPA).
- **The data protection obligations for fintech data aggregators' collection and use of personal information.** Several lawsuits in 2020 focused on fintech companies' data collection and use, alleging that these providers collect, use, and sell access to consumers' financial transaction data without meaningful notice or choice or proper safeguards (see, for example, Complaint, *Wesch v. Yodlee Inc.*, No. 20-05991 (N.D. Cal. Aug. 25, 2020); Amended Complaint, *In re Plaid Privacy Litig,* No. 20-03056 (N.D. Cal. Aug. 5, 2020)).
- **Standing based on potential injuries.** Standing remained a key issue for privacy litigation in 2020, including cases involving, for example, security vulnerabilities (*Flynn v. FCA US LLC*, 2020 WL 1492687, at *5 (S.D. Ill. Mar. 27, 2020) (finding the plaintiff lacked standing in a case against a car maker and an electronics manufacturer over an alleged design defect that may theoretically allow hackers to remotely assume control of vehicles)). For more on standing, see Practice Note, US Privacy Litigation: Overview: Standing and Injury-in-Fact in Privacy Litigation.

Federal Legislation

Congress again failed to pass a comprehensive privacy legislation in 2020, despite debating multiple bills, primarily failing to reach agreement on the extent of federal preemption of state laws and the inclusion of a private right of action. For more on notable privacy-related legislation, see Practice Note, Federal Privacy-Related Legislation Tracker.

Ultimately, Congress:

- Reauthorized the US SAFE WEB Act (Pub. L. No. 116-173), which permits the FTC to take certain collaborative actions against cross-border online fraud through 2027.
- Passed the Internet of Things Cybersecurity Improvement Act of 2020 (Pub. L. No. 116-207), which directs NIST to establish and maintain cybersecurity and vulnerability management standards for federally procured IoT devices. These standards are likely to widely influence private sector practices given the federal government's purchasing power.

State Legislation

Many state legislatures are currently considering bills to provide their residents with stronger consumer privacy and data protections. For more on comprehensive data protection proposals, see Practice Note, State Omnibus Privacy Legislation Tracker.

In the absence of comprehensive federal legislation, states focused their efforts on, for example:

- **Data breach notification.** Reacting to mega breaches and other cybersecurity issues, some states amended their existing data breach notification laws in 2020, generally extending them, for example:
  - the District of Columbia, which amended its law to expand its personal information definition and notice requirements, require organizations to provide 18 months of identity theft prevention services following certain data breaches, and use reasonable security safeguards (see Legal Update, District of Columbia Passes Amendment to Data Security Breach Law); and
  - Vermont, which amended its law to expand its personal information definition and make related notice clarifications (S.110).

  For more details on state data breach notification laws, see State Q&A Tool, Data Breach Notification Laws.
- **Facial recognition and biometric identifying technology.** Several states and cities passed limits or prohibitions on facial recognition technology use, including:
  - Boston, Massachusetts' ban on city use of facial recognition technology, including law enforcement;
  - Portland, Oregon's ban on private sector facial recognition technology use in public spaces, with some exceptions, complementing its related ordinance banning government use (see Legal Update, Portland, Or. Bans Private Entity Use of Face Recognition Technologies in Public Spaces);
  - Maryland's law prohibiting employers from using certain facial recognition services during an applicant's interview for employment without consent (Md. House Bill 1202);
  - New York's prohibition on using biometric identifying technology in schools until July 1, 2022 and after further study (A6787D);
  - Vermont's moratorium on law enforcement use of facial recognition (S.124); and
  - Washington's imposing privacy and antidiscrimination safeguards on state and local governmental facial recognition technology use (SB 6280).
- **The insurance industry.** Several states enacted insurance data security laws, generally following the National Association of Insurance Commissioners (NAIC) Model Insurance Data Security Law (MDL-668), including Indiana, Louisiana, and Virginia. For more, see Practice Note, NAIC Model Data Security Law and State-Specific Implementations. Florida also passed a genetic privacy bill that prohibits life and long-term care insurers from canceling, limiting, or denying coverage, or basing premium rates genetic information (HB 1189).
- **The right to publicity.** New York passed a law that:
  - expands state statutory publicity rights to include deceased personalities and performers domiciled in New York at the time of their death (consistent with constitutional protections for free speech);
  - restricts the use of "digital replicas" of performers without consent; and
  - provides a private right of action for the nonconsensual release of a digitally enhanced sexually explicit depiction of an individual, such as deep fake videos.

  (S5959D.)
- **Student privacy.** Vermont passed a student privacy law that prohibits certain targeted advertising and data profiling using data collected from K-12 educational applications and sharing or selling of student data (Vt. State Bill 110). For more on state student privacy, see Practice Notes, Student Privacy: Education Service Provider Requirements: State Student Privacy Laws and Student Privacy State Laws for Education Service Providers Chart: Overview.

Industry Self-Regulation and Guidance

Industry self-regulation and guidance from independent organizations remained important components of the

privacy and data security landscape in 2020 across various sectors.

For example:

- The Payment Card Industry Security Standards Council (PCI SSC), which is a self-regulatory organization that manages the PCI Data Security Standard (PCI DSS), published incident response guidance, including tips for finding a PCI forensic investigator (PCI SSC, Responding to a Cardholder Data Breach (2020)).
- The Network Advertising Initiative (NAI), a regulatory association for the digital advertising industry, released guidance on sharing personal information, such as location data, for purposes other than tailored advertising including contact tracing, public health initiatives, or for law enforcement purposes (NAI, Best Practices: Using Information Collected for Tailored Advertising or Ad Delivery and Reporting for Non-Marketing Purposes (June 2020)).
- The Digital Advertising Alliance and its enforcement partner, the Council of Better Business Bureaus, reported several inquiries under its accountability program and took actions against, for example:
  - Pinsight Media+ Inc., which agreed to provide enhanced notice of third-party geolocation data collection for interest-based advertising (IBA) in its weather apps (DAA Accountability Program, Formal Review Case No. 118-2020 (Sept. 10, 2020)); and
  - Compare.com Insurance Agency, LLC, which agreed to enhance its notice of third-party data collection on its website for IBA purposes (DAA Accountability Program, Formal Review Case No. 113-2020 (June 18, 2020)).

International Developments

2020 reflected a growing trend in global momentum for comprehensive data protection laws and regulations, including:

- The enactment of:
  - Brazil's General Personal Data Protection Law (LGPD), in many ways similar to the EU General Data Protection Regulation (EU) 2016/679) (GDPR);
  - amendments to New Zealand's Privacy Act, which add additional data breach reporting requirements and data transfer limitations; and
  - new data protection laws in other countries, including Egypt, Jamaica, and Thailand.
- Proposed comprehensive data protection laws in China, India, Indonesia, and Pakistan.
- The Canadian Parliament's initial efforts to overhaul the Personal Information Protection and Electronic Documents Act (PIPEDA).

In addition to navigating evolving data protection laws, multinational companies must also consider the impact from other important 2020 developments, including:

- New European Court of Justice (ECJ) data protection opinions, primarily its seminal decision in *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* (Case No. C-311/18) EU:C:2020:559 (July 16, 2020) (Schrems II), which invalidated the EU-US Privacy Shield (see ECJ Opinions and Schrems II).
- Continued enforcement efforts by European data protection authorities (see European Enforcement).
- Post-Brexit cross-border data issues and enforcement efforts (see Looking Forward).

ECJ Opinions and *Schrems II*

The ECJ's July 16, 2020 decision in *Schrems II* invalidated the EU-US Privacy Shield based 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 the GDPR's adequate protection requirements. 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.

On November 10, 2020, the European Data Protection Board (EDPB) published draft recommendations to guide data exporters (EDPB, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data (Nov. 10, 2020)). For more on this guidance, see Article, EDPB Supplementary Measures Recommendations and German DPA Guidance Post Schrems II.

In January 2021, the EDPB and the European Data Protection Supervisor (EDPS) adopted Joint Opinion 2/2021 on the European Commission's draft SCCs for the transfer of personal data to third countries. For more, see Legal Update, EDPB and EDPS adopt joint opinions on European Commission's draft sets of standard contractual clauses. The European Commission's adoption of a final version of the SCCs is expected in early 2021.

Regulators and data protection authorities across the EU have also issued statements and guidance for compliant cross-border data transfers. For more on this guidance, see Practice Note, EU Cross-Border Data Transfers: Regulatory Guidance Post Schrems II Tracker.

The *Schrems II* decision offers no compliance grace period and represents the second ECJ ruling to overturn an established personal data EU-US transfer mechanism, following its 2015 *Schrems I*decision that invalidated the EU-US Safe Harbor. Companies that relied on the Privacy Shield must immediately reassess and implement other recognized cross-border data transfer mechanisms to ensure their compliance, such as:

- Binding corporate rules.
- SCCs.
- A derogation under GDPR Article 49, such as explicit consent.

Following the ruling, both the Department of Commerce and the FTC advised that participants must continue to honor their Privacy Shield obligations as they consider other transfer mechanisms (see Privacy Shield Framework Website; FTC, Prepared Remarks of Chairman Joseph J. Simons (Aug. 5, 2020); see also US Commerce Department, Privacy Shield FAQs (Aug. 20, 2020); Legal Update, Department of Commerce Updates Privacy Shield FAQs).

The ECJ also issued several other significant online privacy opinions this year that may affect multinational companies, including decisions on:

- The conditions for valid consent in an offline context (see *Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* (Case No. C-61/19) (EU:C:2020:901 (Nov. 11, 2020); Legal Update, Conditions for Valid Consent in an Offline Context (ECJ)).
- The conditions under which national authorities may process communications metadata, such as traffic and location data, for crime prevention or to safeguard national security (see *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs* (Case No. C-623/17) EU:C:2020:790 (Oct. 6, 2020)).

Post-Brexit UK Data Protection

The EU and UK reached a Trade and Cooperation Agreement that contains an interim bridging mechanism allowing the continued free flow of personal data from the EU to the UK for six months after the Brexit transition period ended on December 31, 2020. The extension offers stability while the EU considers an adequacy decision for the UK. In February 2021, the European Commission released a draft adequacy decision, which requires some formal approvals before coming into effect. Absent an adequacy decision:

- The EU considers the UK a third country.
- Companies wishing to transfer personal data from the EU to the UK, such as for processing or other purposes, must adopt an acceptable cross-border data transfer mechanism before doing so.

European Enforcement

Organizations continue to navigate the data protection obligations imposed by the General Data Protection Regulation (GDPR). European regulators' enforcement priorities generally focused on transparency and data security controls.

European data protection authorities (DPAs) brought some notable enforcement actions under the GDPR, including:

- The Croatian DPA's EUR20 million fine on a credit institution that failed to comply with more than 2,500 data subject access requests.
- The Italian DPA's:
  - EUR12.25 million fine on Vodaphone Italia SpA for processing personal data for telemarketing purposes without consent, using inadequate security practices, and other GDPR violations; and
  - EUR 27.8 million fine on TIM S.p.A. for making promotional phone calls without consent and other GDPR failures.
- The Spanish DPA's EUR5 million fine on Banco Bilbao Vizcay Argentaria S.A. for failing to provide required information in its privacy policy and processing client data without a valid legal basis.
- The Irish DPA's EUR450,000 fine on Twitter International Company for failing to adequately document and timely notify the DPA of a data breach.

For more on GDPR compliance, see GDPR Resources for US Practitioners Toolkit.

The French DPA also took action against Google LLC and Google Ireland under national law, imposing a total of EUR100 million fines concerning certain advertising cookie practices.

In the UK, the Information Commissioner's Office (ICO) imposed several significant penalties for data security violations following major data breaches, including against:

- Cathay Pacific, for £500,000.
- British Airways, for £20 million.

Looking Forward

Data privacy compliance issues will remain a priority for organizations, with a special focus on the GDPR, the CCPA, CPRA preparation, and additional state and local regulations. Companies must hone their compliance procedures and carefully watch enforcement and private litigation trends, including:

- Adapting with the changing regulatory environment after the CPPA begins to exercise its rulemaking and enforcement power.
- Tracking the new administration's FTC enforcement priorities, which appears to include looking into technology companies' use of facial recognition and the potentially discriminatory effects of algorithms.

States are likely to continue filling the gap in data privacy regulation, as already seen in early 2021 legislative season activities, given the somewhat low likelihood of federal privacy legislation in the face of other pressing national priorities.

Additional privacy and data security issues likely to get particular attention in 2021 include:

- **Adopting reliable cross-border data transfer mechanisms.** Given the invalidation of the Privacy Shield and the coming expiration of the EU-UK bridging mechanism, multinational companies must assess their options for lawful cross-border data transfers throughout 2021.
- **Focusing on mobile privacy.** Location data has become more valuable to marketers and other commercial entities, but consumer consent for its collection is under increased scrutiny in the face of more stringent privacy laws, mobile platform developer policies, and increased oversight by the FTC and state authorities. Organizations must take care when collecting this type of data to ensure consent is adequate and that their collection practices are not deemed deceptive or unfair.
- **Monitoring sector-specific and local cyber risks.** As the SolarWinds cyberattack and other cyber intrusions of sophisticated networks have shown, no company's system is immune from attack. However, certain sectors that hold especially valuable personal data, such as financial services and health care, and widely used third-party software services will remain priority targets for bad actors. CISA has also noted its expectation that malicious cyber actors will continue to target K-12 educational institutions in 2021, exploiting the remote learning environment to level ransomware attacks, steal data, and otherwise disrupt distance learning services. Additional 2021 high-risk attack targets include the COVID-19 vaccine supply chain, remote work assets, insecure IoT devices, health care entities, including digital health records, cryptocurrency services, and legal cannabis business ventures.
- **Navigating new applications of AI technologies.** Various industries are quickly moving from testing to operational pilot AI programs that analyze and make decisions from consumer data and assist organizations to bolster their cybersecurity defenses. As AI technology becomes more widespread, it continues to raise privacy and ethical concerns about discriminatory outcomes. The federal government is likely to continue its effort to foster public trust in AI technology in 2021 and beyond.