



TRENDS IN PRIVACY AND DATA SECURITY



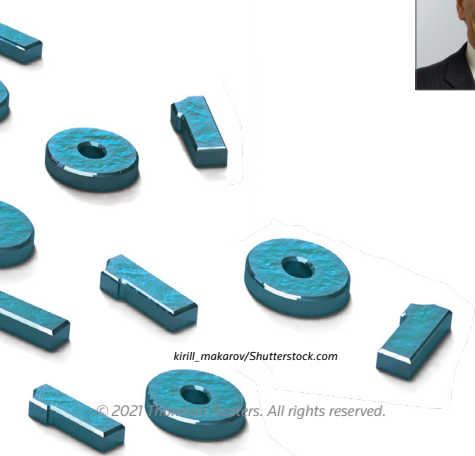
Privacy and cybersecurity remain top priorities for regulators and companies alike, as the threats posed by large-scale data breaches and other cyber incidents show no signs of waning. Companies and their counsel must monitor privacy and data security-related enforcement trends, new laws and regulations, and key emerging issues to mitigate risks and minimize potential liability, especially in the wake of changing work habits due to the COVID-19 pandemic.



JEFFREY D. NEUBURGER

PARTNER
PROSKAUER ROSE LLP

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



kirill_mokarov/Shutterstock.com

© 2021 Proskauer Rose LLP. All rights reserved.

The impacts of the COVID-19 pandemic, the California Consumer Privacy Act of 2018 (CCPA) coming into force, and the invalidation of the EU-US Privacy Shield made 2020 an especially active year for privacy and data security risks and obligations. Adding to the activity in this area, December 2020 brought the discovery of an unprecedented cyberattack affecting government agencies, critical infrastructure entities, and other bodies. The highly sophisticated attack, likely perpetrated by nation-state sponsored hackers, exploited SolarWinds Orion, an enterprise network management software package 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 the significant risks of evolving and novel cyber threats and how important it is for companies and vendors to conduct thorough diligence before finalizing and throughout the term of material software, hardware, and IT service agreements. (For more on the attack and supply chain risk management, see US Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), Supply Chain Compromise, available at [cisa.gov](https://www.cisa.gov).)

The unique events of 2020 have highlighted the need for organizations to keep up with the dynamic and increasing legal obligations governing privacy and data security, understand how these legal obligations 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 pandemic on privacy and data security.
- Developments concerning the CCPA.
- Federal and state guidance, regulations, and enforcement actions.
- Private litigation.
- The international fallout from the European Court of Justice's (ECJ's) invalidation of the EU-US Privacy Shield as a mechanism for cross-border data transfers.
- Trends likely to gain more traction in 2021.



Search [Trends in Privacy and Data Security: 2020](#) for the complete online version of this resource, which includes information on new federal and state legislation, state regulations, industry self-regulatory efforts, and other international developments in privacy and data security.

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

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 the government functions and provides services.

On March 13, 2020, former 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 (Proclamation 9994, Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak, 85 Fed. Reg. 15337, 2020 WL 1272563 (Mar. 13, 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.
- Privacy issues implicated by remote schooling.
- Robocalls and permitted exceptions under the Telephone Consumer Protection Act of 1991 (TCPA).
- Novel contact tracing technologies and apps.

Additionally, the US Department of Health and Human Services (HHS) took several steps during the pandemic to relax certain privacy requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and related regulations.



Search [COVID-19: Data Privacy & Security Guidance on Handling Personal Data During a Pandemic \(Global\) Tracker](#) for more on handling personal data under pandemic conditions.

REMOTE WORK 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 guidance from:

- The Federal Trade Commission (FTC), which published a blog post providing businesses with tips for minimizing security risks when hosting or joining online videoconferences (FTC, Video Conferencing: 10 Privacy Tips for Your Business (Apr. 16, 2020), available at [ftc.gov](https://www.ftc.gov)).
- The National Institute of Standards and Technology (NIST), which published blog posts on telework security basics and virtual meeting security (NIST, Telework Security Basics (Mar. 19, 2020) and Preventing Eavesdropping and Protecting Privacy on Virtual Meetings (Mar. 17, 2020), available at [nist.gov](https://www.nist.gov)).
- The Financial Industry Regulatory Authority (FINRA), which released an alert describing measures organizations can use to strengthen their cybersecurity controls in a remote work situation (FINRA, Cybersecurity Alert: Measures to Consider as Firms Respond to the Coronavirus Pandemic (COVID-19) (Mar. 26, 2020), available at [finra.org](https://www.finra.org)).

- DHS's CISA and the UK's National Cyber Security Centre (NCSC), which released a joint statement advising that cyber criminals were honing their phishing and malware attacks to exploit remote workers and newly deployed access infrastructure (CISA and NCSC, AA20-099A, COVID-19 Exploited by Malicious Cyber Actors (Apr. 8, 2020), available at us-cert.cisa.gov).

Organizations also confronted a series of pandemic-related workplace and health privacy issues (for a collection of resources to assist counsel in managing pandemic-related employment issues, search [Employment Global Coronavirus Toolkit](#) and [Benefits, Share Plans & Executive Compensation Global Coronavirus Toolkit](#) on Practical Law).

STUDENT AND CHILD PRIVACY

The pandemic made educational institutions adapt to new ways of handling student data. To assist in this effort:

- The FTC issued guidance under the Children's Online Privacy Protection Act of 1998 (COPPA) urging schools to understand:
 - how ed tech operators and other providers might collect, use, and disclose students' personally identifiable information (PII); and
 - the steps for ensuring proper consents and uses.
 (FTC, COPPA Guidance for Ed Tech Companies and Schools During the Coronavirus (Apr. 9, 2020), available at ftc.gov; for more on COPPA, search [Children's Online Privacy: COPPA Compliance](#) on Practical Law.)
- The US Department of Education's (DOE's) Student Privacy Policy Office released information addressing frequently asked questions (FAQs) 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 FAQs also discuss how a school may, in a limited manner, disclose a student's COVID-positive status in certain situations. (DOE, Student Privacy Policy Office, FERPA & COVID-19 FAQs (Mar. 2020), available at studentprivacy.ed.gov).



Search [Student Privacy: Education Service Provider Requirements](#) for more on key student privacy requirements applicable to third-party educational service providers that use, maintain, share, or dispose of student-related data.

EMERGENCY ROBOCALLS

The need for health care providers and public health authorities 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 the Matter of 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, Consumer & Governmental Affairs Bureau, 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, Coronavirus Warning Letters to Companies, Robocall Warning Letters, available at ftc.gov.)

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 an 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. For example:

- Virginia released the COVIDWISE app (Virginia Department of Health, COVIDWISE, available at vdh.virginia.gov).
- Certain northeastern states, including New York and New Jersey, released regional COVID Alert apps (for example, Press Release, New York State, Governor Cuomo and Governor Murphy Launch Exposure Notification Apps to Help Stop the Spread of COVID-19 (Oct. 1, 2020), available at governor.ny.gov).
- Certain west coast states released the Exposure Notification Express app (for example, Press Release, Office of Governor, Washington and Oregon Join California in Pilot Project Using Google and Apple Exposure Notification Technology to Slow the Spread of COVID-19 (Sept. 16, 2020), available at gov.ca.gov).

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

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. (Letter from the National Association of Attorneys General to Sundar Pichai and Tim Cook (June 16, 2020), available at [ag.ks.gov](#).)

Additionally, 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.)

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.
- Lawsuits under the CCPA's private right of action, which are beginning to be filed.
- California voters' approval of the California Privacy Rights Act (Proposition 24) (CPRA), which amends the CCPA in important ways.

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. The CPRA extends the exemptions until January 1, 2023 (see below *CPRA*). (For more on the CCPA amendments, search [CCPA Proposed Amendments and Other California Privacy-Related Legislation Tracker](#) on Practical Law.)



Search [California Consumer Privacy Act \(CCPA\) Toolkit](#) for a collection of resources to help counsel understand and meet the requirements of the CCPA and CPRA.

FINAL CCPA REGULATIONS

The California Attorney General (CAG) released final CCPA implementing regulations, effective August 14, 2020, after extensive proposal and commenting activities (Cal. Code Regs., tit. 11, §§ 999.300 to 999.337; for more information, search [Final CCPA Regulations Approved](#) on Practical Law). 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 (California Department of Justice, Text of Modified Regulations, available at [oag.ca.gov](#); for more information, search [Fourth Set of Proposed Modifications to CCPA Regulations Released for Comment](#) on Practical Law).

CCPA LITIGATION

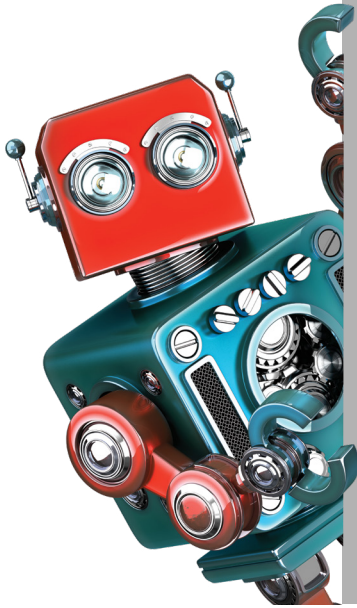
2020 brought the first lawsuits under the CCPA's private right of action, which permits claims for unauthorized access, theft, or disclosure of nonencrypted and nonredacted personal information due to a business's failure to implement reasonable security practices and procedures (Cal. Civ. Code § 1798.150(a)(1)).

For example, consumers brought a proposed class action against children's retailer Hanna Andersson LLC over 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 case (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 and will become operative on January 1, 2023, amends and generally expands the CCPA's scope. For example, the CPRA:


- Establishes the California Privacy Protection Agency (CPPA), which will:
 - assume rulemaking authority for CCPA and CPRA regulations; and
 - share enforcement authority with the CAG.
- Defines a new category of sensitive personal information.
- Provides for new and expands some current rights for consumers, including the right to:
 - correct inaccurate personal information;
 - opt out of sharing personal information; and
 - restrict sensitive information processing.
- Treats some forms of sharing personal information similarly to selling personal information under the CCPA.
- Defines "contractors," which resemble service providers under the CCPA, and requires certain contract terms.
- Prohibits obtaining consent through dark patterns, which are user interface features designed to subvert or impair users' autonomy, decision-making, or choice.
- Potentially reduces the CCPA's scope 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 (the threshold under the CCPA is 50,000 or more); and
 - expressly allowing loyalty or rewards programs consistent with the law.
- Expands the circumstances when organizations must minimize their activities involving personal information (data minimization).



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.

- Requires certain organizations to perform annual independent cybersecurity audits and submit annual privacy risk assessments to the CPPA.


The CPRA applies only to personal information collected on or after January 1, 2022, with some exceptions, and delays enforcement until July 1, 2023.

 Search [Expert Q&A: The California Privacy Rights Act of 2020](#) for more on how the CPRA amends and expands the CCPA.

FEDERAL GUIDANCE, REGULATION, AND ENFORCEMENT

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

- The FTC.
- HHS.
- The US Department of Commerce and NIST.

 Search [Trends in Privacy and Data Security: 2020](#) for the complete online version of this resource, which includes information on regulatory and enforcement activity by the FCC, the Securities and Exchange Commission, and other federal agencies.

FTC

The FTC is the primary federal agency regulating consumer privacy and data security. It derives its authority to protect consumers against unfair or deceptive trade practices from Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45).

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

FTC Guidance

In 2020, the FTC sought public comments on possible changes to its Health Breach Notification Rule (16 C.F.R. §§ 318.1 to 318.9), which requires vendors of personal health records and related entities to notify consumers following a breach involving unsecured information (Press Release, *FTC Seeks Comment as Part of Review of Health Breach Notification Rule* (May 8, 2020), available at [ftc.gov](#)).

The FTC also continued to issue blog posts and notable guidance on artificial intelligence, social media bots, and the Do Not Call registry.

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 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); for more information, search [FTC Settlement Requires Zoom to Enhance Information Security Program](#) on Practical Law).

- **Protect children by complying with COPPA obligations.** For example, the FTC reached settlements with:
 - a children's app developer over 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 3, 2020), available at [ftc.gov](#)); and
 - a Swiss-based digital game developer over 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, search [Children's Online Privacy: COPPA Compliance](#) on Practical Law.)

- **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), available at [ftc.gov](#)).
- **Properly oversee third-party vendors' security practices.** The FTC settled with Ascension Data & Analytics, LLC over 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 (for more information, search [FTC Agrees to Settle with Ascension Over Alleged Vendor Oversight Failures](#) on Practical Law).
- **Comply with consumer records requests under the Fair Credit Reporting Act (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 who were victims of 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), available at [ftc.gov](#); for more information, search [FTC Settles Claims Kohl's Failed to Give Identity Theft Victims FCRA-Required Information](#) on Practical Law).
- **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, over claims that they helped support fraudulent credit card interest rate relief. The VoIP provider agreed to:

- not provide services to clients who pay with stored value cards or cryptocurrency;
- perform due diligence on potential clients; and
- 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), available at [ftc.gov](#).)

- **Make accurate representations about cross-border data transfer practices.** The FTC continued its enhanced 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 Cross-Border Privacy Rules 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, *In re Ortho-Clinical Diagnostics, Inc.*, No. 192 3050 (F.T.C. July 8, 2020); Decision and Order, *T&M Prot. Res., LLC*, No. 192 3092 (F.T.C. Mar. 16, 2020), available at [ftc.gov](#).)

HHS

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



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

HHS Guidance

In 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 Substance Abuse and Mental Health Services Administration (SAMHSA), Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule (July 13, 2020), available at [samhsa.gov](#)). HHS plans to further revise these regulations consistent with the Coronavirus Aid, Relief, and Economic Security Act (Pub. L. No. 116-136).
- Jointly released a ransomware advisory with the Federal Bureau of Investigation and CISA warning of an increased threat of cybercrime and ransomware attacks against US hospitals and health care providers (CISA, Ransomware Activity Targeting the Healthcare and Public Health Sector (Oct. 28, 2020), available at [us-cert.cisa.gov](#)).
- 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 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 (for more information, search [Cyber-Attackers' Theft of Over Ten Million Individuals' PHI Leads to \\$6.85 Million HIPAA Settlement, In \\$1 Million HIPAA Settlement, HHS Emphasizes Business Associate and Encryption Compliance, and HIV-Related Disclosures \(and More\) Lead to \\$1 Million HIPAA Settlement](#) on Practical Law).
- **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 (Press Release, HHS, OCR Settles Twelfth Investigation in HIPAA Right of Access Initiative (Nov. 19, 2020), available at [hhs.gov](#)). The initiative continues with HHS 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 (for more information, search [Terminated Employee's Unauthorized Access to HIPAA PHI Sparks HHS Investigation](#) on Practical Law).

In early 2021, the Fifth Circuit issued a potentially wide-reaching decision for disputes involving civil monetary penalties levied against HIPAA covered entities when it vacated a \$4.3 million assessment (for more information, search [Fifth Circuit: HHS's HIPAA Enforcement Was "Arbitrary, Capricious, and Contrary to Law"](#) on Practical Law and see page 9 in this issue).

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 (Department of Commerce, FAQs – EU-U.S. Privacy Shield Program Update (Aug. 20, 2020), available at [privacyshield.gov](#); see below *International Developments*). NIST maintained its leadership role in setting cybersecurity and privacy standards. Notable 2020 NIST activities included:

- Publishing version 1.0 of its eagerly anticipated NIST Privacy Framework, which follows the structure of its influential NIST Cybersecurity Framework (for more information, search [NIST Releases Privacy Framework on Practical Law](#)).
- 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 (available at [csrc.nist.gov](#)).
- Updating its key federal contractor data security standard (NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, available at [csrc.nist.gov](#)), 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.

STATE ENFORCEMENT

Notable state activity related to privacy and data security in 2020 included single-state enforcement actions as well as multistate and federal-state cooperation in privacy enforcement.

SINGLE-STATE ENFORCEMENT ACTIONS

Single-state enforcement actions in 2020 focused primarily on:

- Data breaches and security vulnerabilities.
- Location tracking practices.
- Biometric information privacy and use.
- 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 (for more information, search [California AG Resolves Fertility App Privacy Breach Investigation](#) on Practical Law).
- Indiana, which opted not to join a 2019 multistate settlement with Equifax, Inc. over 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); see In. Office of the Att'y Gen., 2017 Equifax Security Breach: 2020 Equifax Settlement, available at [in.gov](#)).
- 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 (see Consent Order, *In re Wakefern Food Corp.* (N.J. Dept. of Law Oct. 9, 2020), available at [nj.gov](#)).

- 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 (for more information, search [Expert Q&A on Lessons Learned from the First NYDFS Cybersecurity Enforcement Action](#) on Practical Law);
 - 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 (N.Y. Office of the Att'y Gen., Letter Agreement Between Zoom and the NYAG (May 7, 2020), available at [ag.ny.gov](#); United Federation

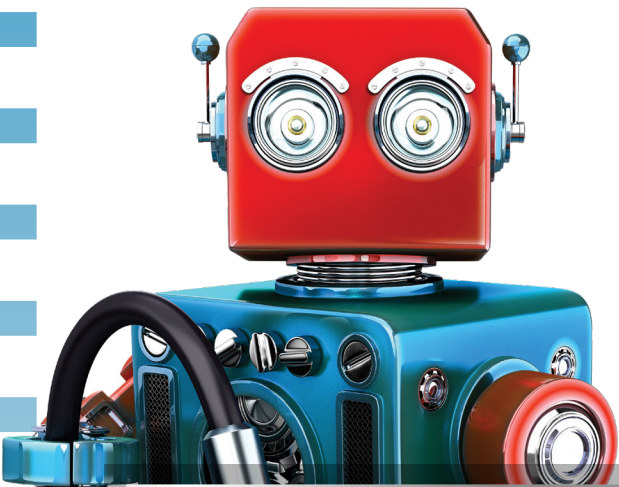
of Teachers, DOE Employees Can Use Zoom Again (May 6, 2020), available at [uft.org](#)); and

- reached a \$650,000 settlement with franchisor Dunkin' Brands, Inc., resolving a lawsuit over 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), available at [ag.ny.gov](#)).

Location Tracking Practices

State authorities took aim at location tracking practices, including:

- Arizona, which brought suit against Google LLC under Arizona's state consumer protection law based on the company's location data collection practices, including allegedly collecting users' location information even when they turn off the Location History setting on their mobile devices (Complaint, *Arizona v. Google LLC*, No. 2020-6219 (Ariz. Super Ct. May 27, 2020), available at [azag.gov](#)).
- 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 (Joint Stipulation and Order Regarding Settlement and Dismissal of the Case with Prejudice, *California v. TWC Prod. & Tech., LLC*, No. 19STCV00605 (Cal. Super., L.A. Cty, 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.



STANDING REMAINED A KEY ISSUE IN 2020 FOR DATA BREACH ACTIONS IN FEDERAL COURTS. FOR EXAMPLE, COURTS FOUND THAT PLAINTIFFS COULD NOT 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.

Biometrics Privacy

State authorities increasingly recognized the sensitivity and privacy concerns surrounding biometric data. For example, on March 10, 2020, the Vermont Attorney General 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; for more information, search [Vermont Enacts First Data Broker Law](#) on Practical Law).
- Alleges violations of the state's consumer protection and data broker laws over the techniques Clearview uses to acquire images (Vt. Office of the Att'y Gen., Attorney General Donovan Sues Clearview AI for Violations of Consumer Protection Act and Data Broker Law (Mar. 10, 2020), available at [ago.vermont.gov](#)).

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), available at [ago.vermont.gov](#)).



Search [Biometrics in the Workplace](#) for information on the regulation and use of biometrics in the workplace.

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 Tenth Circuit).)
- Washington, which reached a \$100,000 settlement (suspended from \$500,000) with social media platform operator Super Basic, LLC over 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 Decree, *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 (Press

Release, N.Y. Office of the Att'y Gen., Attorney General James Helps Secure \$39.5 Million After Anthem's 2014 Data Breach (Sept. 30, 2020), available at [ag.ny.gov](#)).

- 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. Office of the Att'y Gen., Attorney General Josh Stein Announces \$5 Million Settlement with Community Health Systems (Oct. 8, 2020), available at [ncdoj.gov](#)).
- 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 (Press Release, Ca. Office of the Att'y Gen., Attorney General Becerra Announces \$17.5 Million Settlement Against Home Depot Over Credit Card Data Breach (Nov. 24, 2020), available at [oag.ca.gov](#)).
- 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 (Press Release, DOJ, DISH Network to Pay \$210 Million for Telemarketing Violations (Dec. 7, 2020), available at [justice.gov](#)).
- 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. Office of the Att'y Gen., Attorney General James Announces \$2 Million Agreement with CafePress After Data Breach (Dec. 18, 2020), available at [ag.ny.gov](#)).

PRIVATE LITIGATION

Private litigation highlights and trends for 2020 focused on:

- Data breach-related actions.
- Biometrics.
- The TCPA.
- Various other privacy and data security-related topics.

DATA BREACH LITIGATION


Standing remained a key issue in 2020 for data breach actions in federal courts. For example, courts found that plaintiffs could not 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)).

Additionally, 2020 data breach litigation 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 in a complaint describing security vulnerabilities rather than “data breaches” may not sustain securities fraud claims.** 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)).

A steady stream of data breach-related class settlements also continued through the past year, 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 subsequent 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. 17-2800 (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. 17-03463 (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)).

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

BIOMETRIC INFORMATION PRIVACY ACT LITIGATION

Litigation under the Illinois 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 (for more information, search [Illinois Supreme Court Rules Biometric Information Privacy Act Lawsuits Do Not Require Actual Injury](#) on Practical Law).

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 exception for patients in a health care setting.** 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 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. Dakota Integrated Sys., LLC*, 980 F.3d 1146, 1152-56 (7th Cir. 2020); *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020); for more information, search [Unlawful Retention of Biometric Data Under BIPA Supports Article III Standing: Seventh Circuit](#) on Practical Law).

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

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

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. TCPA litigation continued apace in 2020, including a steady stream of class settlements. Key litigated issues included:

- **The automatic telephone dialing system (ATDS) definition.** In December 2020, the Supreme Court heard arguments addressing a circuit split over 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 exception.** 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); for more information, search [SCOTUS Strikes Down TCPA Government Debt Exception](#) on Practical Law).
- **How to determine the level of deference courts should afford FCC interpretative rules.** On remand from the Supreme Court, 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 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. Dec. 9, 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)).



Search [Telephone Consumer Protection Act: Overview](#) and [TCPA Litigation: Key Issues and Considerations](#) for more on TCPA litigation.

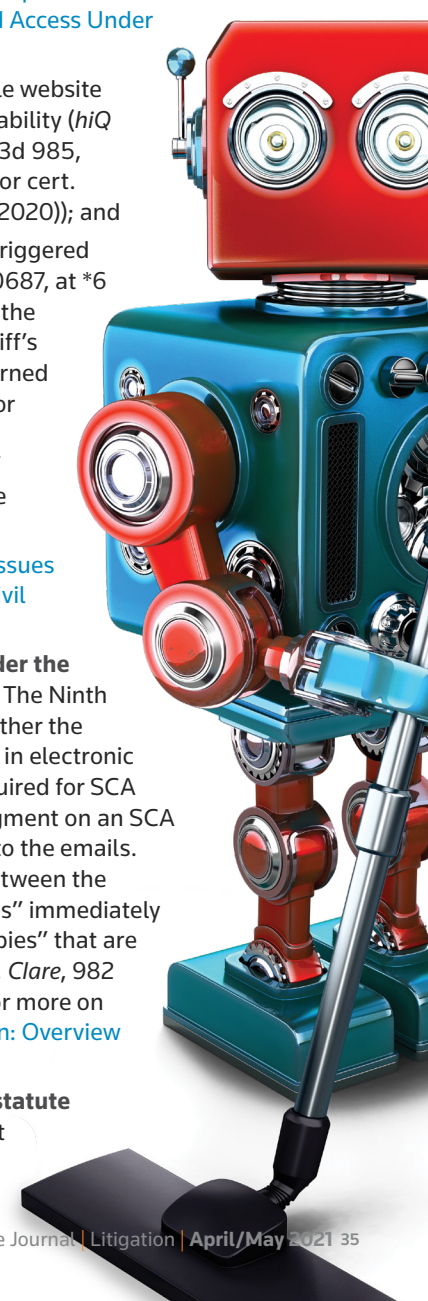
OTHER NOTABLE CASES

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

- **The Computer Fraud and Abuse Act (CFAA).** Key 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, 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); for more information, search [Sixth Circuit Requires More Than Misuse to Exceed Authorized Access Under CFAA](#) on Practical Law);
 - 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 the integrity of their account or computer was impaired, not when they learned of the exact extent of the defendant's involvement in the intrusion)).

(For more on the CFAA, search [Key Issues in Computer Fraud and Abuse Act Civil Litigation](#) on Practical Law.)

- **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, search [US Privacy Litigation: Overview](#) on Practical Law.)
- **The federal criminal identity theft statute (18 U.S.C. § 1028A).** 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, 324-27 (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 over 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, search [US Privacy Litigation: Overview](#) on Practical Law).
- **The data protection obligations for financial technology (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. 20-5991 (N.D. Cal. Aug. 25, 2020); Amended Complaint, *In re Plaid Privacy Litig.*, No. 20-3056 (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

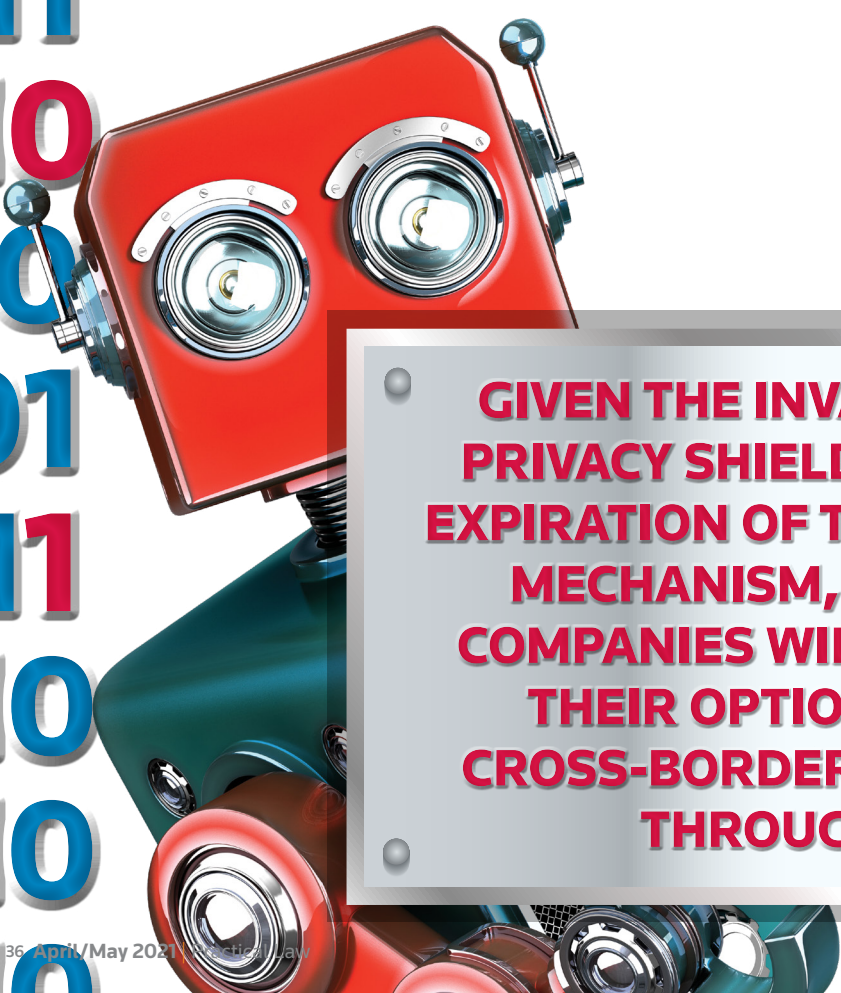
lacked standing in a case against a car maker and an electronics manufacturer over an alleged design defect that could theoretically allow hackers to remotely assume control of vehicles); for more on standing, search [US Privacy Litigation: Overview](#) on Practical Law).

INTERNATIONAL DEVELOPMENTS

2020 reflected a growing trend in global momentum for comprehensive data protection laws and regulations. In addition to navigating evolving data protection laws, multinational companies must also consider the impact from other important 2020 developments, including the ECJ's seminal decision in *Data Protection Commissioner v. Facebook Ireland & Maximillian Schrems* (Case No. C-311/18, EU:C:2020:559 (July 16, 2020), available at curia.europa.eu) (*Schrems II*).

The ECJ's *Schrems II* decision 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 standard contractual clauses (SCCs) for the transfer of personal data from EU controllers to processors in third countries 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 adequate protection requirements of the EU General Data Protection Regulation (GDPR). Exporters may need to supplement SCCs with additional safeguards, such as technical measures, to ensure they meet GDPR standards. (For more on the GDPR, search [Overview of EU General Data Protection Regulation](#) on Practical Law.)



GIVEN THE INVALIDATION OF THE PRIVACY SHIELD AND THE COMING EXPIRATION OF THE EU-UK BRIDGING MECHANISM, MULTINATIONAL COMPANIES WILL NEED TO ASSESS THEIR OPTIONS FOR LAWFUL CROSS-BORDER DATA TRANSFERS THROUGHOUT 2021.

- 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.

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, Privacy Shield Program Overview, available at [privacyshield.gov](https://www.privacyshield.gov); FTC, Prepared Remarks of Chairman Joseph J. Simons (Aug. 5, 2020), available at [ftc.gov](https://www.ftc.gov); see also Department of Commerce, FAQs – EU-U.S. Privacy Shield Program Update (Aug. 20, 2020), available at [privacyshield.gov](https://www.privacyshield.gov); for more information, search [Department of Commerce Updates Privacy Shield FAQs on Practical Law](#)).



Search [Trends in Privacy and Data Security: 2020](#) for the complete online version of this resource, which includes information on other international developments, including notable ECJ decisions, post-Brexit UK data protection, an overview of European enforcement, and newly enacted or proposed data protection laws.

Search [EU Cross-Border Data Transfers: Regulatory Guidance Post Schrems II Tracker](#) for links to guidance from regulators and data protection authorities across the EU for compliant cross-border data transfers.

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 appear 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 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:

- **Cross-border data transfer mechanisms.** Given the invalidation of the Privacy Shield and the coming expiration of the EU-UK bridging mechanism, multinational companies will need to assess their options for lawful cross-border data transfers throughout 2021.
- **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 that consent is adequate and their collection practices are not deemed deceptive or unfair.
- **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 (CISA, Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data (Dec. 10, 2020), available at [us-cert.cisa.gov](https://www.cisa.gov/us-cert/2020/US-CERT-20-338)). Additional 2021 high-risk attack targets include the COVID-19 vaccine supply chain, remote work assets, insecure Internet of Things devices, health care entities, including digital health records, cryptocurrency services, and legal cannabis business ventures.
- **New applications of artificial intelligence (AI) technology.** 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. [🔗](#)

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