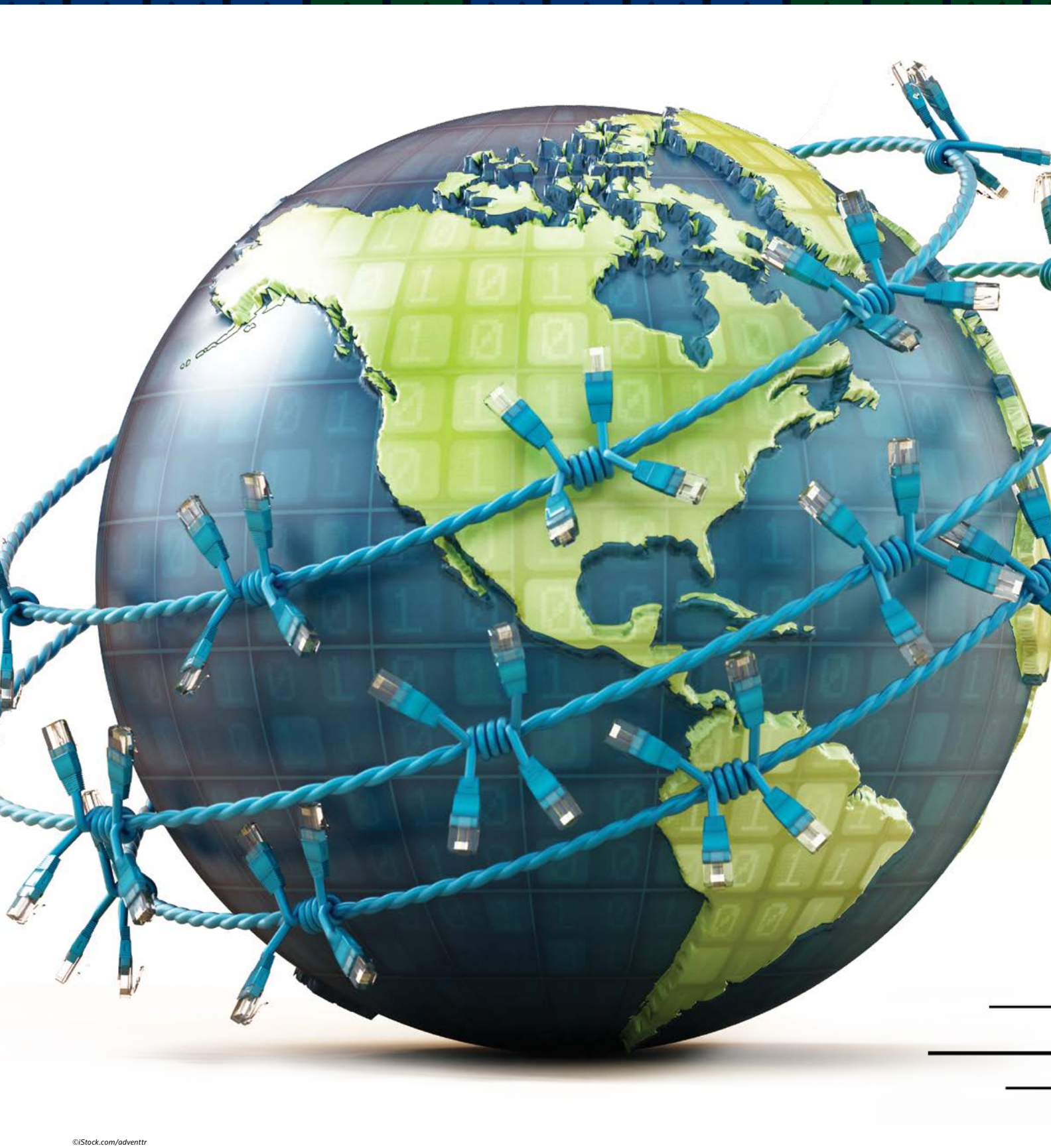

©iStock.com/adventtr

TRENDS IN PRIVACY AND DATA SECURITY

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

JEFFREY D. NEUBURGER
PARTNER
PROSKAUER 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.

Companies must keep up with the dynamic and increasing legal obligations governing privacy and data security, understand how they apply, monitor security risks and cyberattack trends, and manage their compliance to minimize risks. This article reviews important privacy and data security developments in 2019 and highlights key issues for the year ahead. Specifically, it addresses recent:

- Federal regulation and enforcement actions.
- State regulation and enforcement actions.
- Private litigation.
- Federal and state legislation.
- International developments likely to affect US companies.
- Trends likely to gain more traction in 2020.

Local governments are also showing an increased interest in privacy and data security, especially concerning consumer protection, law enforcement and other uses for facial recognition, and smart city technologies. In late 2019, a federal court ruling allowed Chicago to proceed in a data breach action brought under a local city ordinance. The court accepted the city's argument that it has local interests and standing to pursue the action. (*City of Chicago v. Marriott Int'l, Inc.*, 2019 WL 6829101 (D. Md. Dec. 13, 2019).)

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

FEDERAL REGULATION AND ENFORCEMENT

Several federal agencies issued guidance and took privacy and data security enforcement actions in 2019, including:

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

Federal agencies, including the FTC and the Department of Justice, also continued to partner with state-level authorities, especially in higher-profile multistate actions.

Search Trends in Privacy and Data Security: 2019 for the complete online version of this resource, which includes information on regulatory and enforcement activity by other federal agencies, as well as industry self-regulation efforts.

FTC

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

Search FTC Data Security Standards and Enforcement for more on the FTC's authority and standards.

FTC Guidance

In 2019, the FTC continued to blog and explain its existing guidance, taking further action and releasing notable guidance on:

- **Children's privacy practices.** In July 2019, the FTC issued a broad request for comments on its current Children's Online Privacy Protection Act of 1998 (COPPA) Rule. It later extended the comment period through early December 2019, following an October 2019 workshop exploring whether to update the regulations and considering:
  - the growth of child-directed content on social media and video-sharing platforms;
  - the implications of interactive television and gaming, chatbots, and other interactive media; and
  - the increased use of education technology.

  (84 Fed. Reg. 35842-01 (July 25, 2019); 84 Fed. Reg. 56391-01 (Oct. 22, 2019).)
- **Reasonable data security practices.** The FTC issued an early 2020 blog post summarizing several trends and improvements in its 2019 data security actions, including:
  - more prescriptive safeguards requirements;
  - increased accountability for third-party assessors; and
  - board-level engagement and compliance certifications.

  (See Andres Smith, FTC Bureau of Consumer Protection, New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers (Jan. 6, 2020), available at *ftc.gov*.)
- **Financial institutions' privacy and data security practices.** In March 2019, the FTC issued separate requests for comments on proposed changes to its Gramm-Leach-Bliley Act (GLBA) Safeguards Rule and Privacy Rule, later extending the comment period on its extensive Safeguards Rule proposals, which are similar to recent New York Department of Financial Services (NYDFS) cybersecurity requirements (84 Fed. Reg. 13158-01 (Apr. 4, 2019); 84 Fed. Reg. 13150-01 (Apr. 4, 2019); 84 Fed. Reg. 24049-02 (May 24, 2019)).
- **Unsolicited commercial email.** The FTC reviewed and chose to keep unchanged its regulations implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) (84 Fed. Reg. 13115-01 (Apr. 4, 2019)).
- **Broadband privacy.** The FTC issued orders to several broadband providers to examine how they collect, retain, use, and disclose information about consumers and their devices (see Press Release, FTC, FTC Seeks

to Examine the Privacy Practices of Broadband Providers (Mar. 26, 2019), available at *ftc.gov*).

- **Robocall violations.** Responding to consumer complaints about unwanted robocalls to mobile phones, the FTC and various law enforcement agencies initiated Operation Call It Quits, bringing multiple actions against companies and individuals responsible for unwanted calls.

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.

Search Equifax to Pay $575 Million to Settle Data Breach Claims with FTC, CFPB, and State AGs and Facebook Agrees to Settle Privacy Claims with the FTC and SEC for information on widely reported cases in this area.

The FTC's 2019 actions demonstrate that companies should:

- **Ensure that privacy and data security practices match promises.** For example, the FTC reached settlements with:
  - an online rewards website that promised to implement a comprehensive information security program to settle allegations that it failed to take reasonable steps to protect personal data, despite promises that the site utilizes the latest security and encryption techniques (*In the Matter of Grago, Jr. d/b/a ClixSense.com*, 2019 WL 3001880 (F.T.C. June 19, 2019));
  - a smart home products manufacturer that agreed to implement a comprehensive software security program to settle alleged misrepresentations that it secured its wireless routers and internet-connected cameras using "advanced network security" despite reported cyber vulnerabilities (*FTC v. D-Link Systems, Inc.*, 2017 WL 4150873 (N.D. Ca. 2017) (Proposed Stipulated Order for Injunction and Judgment filed July 2, 2019)); and
  - a personal email management provider, regarding allegations that it made false statements about the extent of its data mining and data sharing of a subset of users' email message content (for more information, search FTC Settlement Targets Misrepresentations on Parent Company's Data Collection and Use on Practical Law).
- **Provide transparency and usage controls for monitoring apps.** A developer of three "stalking" apps used to monitor other individuals' mobile device activity agreed to settle allegations that it did not take reasonable steps to ensure its apps were used only for legitimate purposes, required bypassing device controls, and failed to secure the personal information it collected. The company agreed to take specific measures to limit the apps' uses and implement a comprehensive information security program. (For more information, search FTC Settlement Requires "Stalker App" Developers to Ensure Legitimate Use and Protect Personal Information on Practical Law.)
- **Protect children by complying with COPPA obligations.** For example, the FTC reached settlements with:
  - Google, Inc. and its video sharing platform YouTube, LLC for a record $170 million regarding allegations that they collected persistent identifiers from child-directed channel viewers, but failed to notify parents and obtain consent. The settlement also requires YouTube to provide channel owners a mechanism to designate their child-directed content and annual COPPA-compliance training to its employees. (For more information, search FTC and NY AG Announce $170 Million YouTube Settlement Over Alleged COPPA Violations on Practical Law.);
  - the operators of fashion-related social website i-DressUp.com for $35,000 and promises to comply with COPPA parental notice and consent requirements and implement reasonable security measures to protect collected data (*U.S. v. Unixiz, Inc.*, No. 19-2222 (N.D. Cal. Proposed Stipulated Order Apr. 24, 2019)); and
  - the operators of video social network app Musical.ly (now known as TikTok) for a then-record $5.7 million regarding allegations that they collected children's personal information without parental notice and consent, and failed to delete personal information at parents' request (for more information, search FTC Obtains Largest Monetary Settlement in a COPPA Case on Practical Law).
- **Maintain reasonable data security safeguards to protect personal information maintained on behalf of clients.** The FTC emphasized service provider accountability and pressed companies to maintain a comprehensive information security program when it settled with:
  - an auto dealer software provider that allegedly failed to protect dealer-stored personal information, leading to the breach of a backup database containing 12.5 million consumers' unencrypted personal information (for more information, search FTC Settlement Requires Information Security Program and Independent Evidence-Based Assessments on Practical Law); and
  - a multi-level marketing services provider over allegations that it failed to employ reasonable, low-cost security safeguards, allowing hackers to access clients' personal information (*In re Infotrax Systems, L.C.*, 2019 WL 7582773 (F.T.C. Dec. 30, 2019)).
- **Avoid misrepresenting privacy practices or misusing credit reports.** The FTC settled allegations that a mortgage broker violated the Fair Credit Reporting Act (FCRA) and other laws by disclosing consumers' personal information in response to negative reviews on Yelp. The broker agreed to pay $120,000 and avoid misrepresenting its privacy practices or misusing credit reports. (For more information, search FTC and

The California Attorney General released proposed regulations to implement the California Consumer Privacy Act and provide compliance guidance for businesses, including an Initial Statement of Reasons that offers an overview on the rationale and guiding principles behind the regulations.

Mortgage Broker Reach Settlement Over Personal Information Disclosures in Yelp Review Responses on Practical Law.)

- **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 over ten companies and sent warning letters to others throughout the year and into early 2020.

HHS

HHS's Office for Civil Rights (OCR) provides guidance and takes enforcement actions under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and related regulations.

HHS Guidance

In 2019, HHS:

- Released and later extended the comment period on proposed rule changes intended to improve electronic health information interoperability and patient access while supporting privacy (84 Fed. Reg. 7610-01 (Mar. 4, 2019)).
- Proposed exceptions to its regulations implementing the Physician Self-Referral Law, known as the Stark Law, and the Federal Anti-Kickback Statute to support donations of cybersecurity technology and related services (84 Fed. Reg. 55694-01 (Oct. 17, 2019); 84 Fed. Reg. 55766-01 (Oct. 17, 2019)).
- Increased its penalty amounts under the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 following its April 2019 reinterpretation of the Health Information Technology for Economic and Clinical Health (HITECH) Act that resulted in lower annual maximums for less severe violations (84 Fed. Reg. 59549 (Nov. 5, 2019)).
- Provided updated guidance on several topics, including disclosing protected health information (PHI) for care coordination, managing malicious insider threats, and recognizing direct liability for business associates under the HIPAA rules.

HHS Enforcement Activity

OCR settled several notable HIPAA enforcement actions in 2019, highlighting that companies should:

- **Review media and public communications policies.** For example:
  - Elite Dental Associates, Dallas, P.C. agreed to pay $10,000 to settle potential violations regarding PHI disclosures it allegedly made in response to patient reviews on Yelp (for more information, search Disclosure of Patients' PHI on Yelp Leads to $10,000 HIPAA Settlement on Practical Law); and
  - Jackson Health System agreed to pay $2.15 million over privacy incidents, including PHI disclosures to the media and lost paper records containing PHI (for more information, search Social Media Disclosure of

NFL Player's PHI (and Other Violations) Lead to $2.15 Million in HIPAA Penalties on Practical Law).

- **Conduct a thorough risk analysis and implement effective safeguards.** For example:
  - Touchstone Medical Imaging, LLC agreed to pay $3 million regarding an allegedly publicly available FTP server containing over 300,000 patients' PHI (for more information, search PHI Visible Via Google Search Leads to $3 Million HIPAA Settlement on Practical Law);
  - Medical Informatics Engineering, Inc. agreed to pay $100,000 over a data breach in which hackers allegedly used a compromised user ID and password to access approximately 3.5 million individuals' PHI;
  - University of Rochester Medical Center agreed to pay $3 million related to alleged failures to encrypt PHI on mobile devices and media; and
  - Texas Health and Human Services Commission agreed to pay $1.6 million related to PHI allegedly exposed on a public server (for more information, search Applying Its Updated Penalties Analysis, HHS Imposes $1.6 Million in HIPAA Civil Money Penalties on Practical Law).
- **Properly notify HHS of data breaches.** For example, Sentara Hospitals agreed to pay $2.175 million after an apparent difference of interpretation regarding breach notification obligations that resulted from a mailing error (for more information, search HIPAA Breach Notification Failure Leads to $2.175 Million Settlement on Practical Law).
- **Support required patient access to PHI.** For example, in the first patient access enforcement action and resolution agreement under HHS's Right of Access Initiative, Bayfront Health St. Petersburg agreed to pay $85,000 and update its practices following a mother's complaint that she was unable to timely obtain medical records about her unborn child.

DEPARTMENT OF COMMERCE AND NIST

The Department of Commerce issued (and continues to update) post-Brexit guidance for companies that use the EU-US Privacy Shield to support cross-border data transfers. NIST maintained its leadership role in setting cybersecurity and privacy standards for public and private sector entities.

Notable NIST activities in 2019 included:

- Releasing the initial draft and, in early 2020, Version 1.0 of its Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management (available at *nist.gov*), which:
  - helps companies develop privacy engineering practices to better protect personal information, meet compliance obligations, and communicate with stakeholders; and
  - leverages structural and other lessons learned from the widely adopted NIST Cybersecurity Framework, with similar core, profiles, and implementation tiers components (for more information, search The NIST Cybersecurity Framework on Practical Law).
- Publishing the final version of its NIST Big Data Interoperability Framework (available at *bigdatawg.nist.gov*), which addresses requirements for data security and privacy protections that companies should include in big data programs and tools.
- Releasing comment drafts and standards guidance on various cybersecurity topics, including:
  - improving the security of interdomain traffic exchange and mitigating DDoS attacks;
  - creating a zero trust architecture network strategy;
  - following a systems security approach to building cyber resilient systems;
  - using blockchain-based data management to help secure smart manufacturing;
  - protecting internet of things (IoT) devices;
  - securing medical imaging archives; and
  - adopting secure software development practices.

STATE REGULATION AND ENFORCEMENT

STATE REGULATORY DEVELOPMENTS

Key 2019 developments at the state level include:

- In August 2019, attorneys general from all 50 states and the District of Columbia, and 12 voice service providers, agreed to adopt the Anti-Robocall Principles and cooperate in stopping unwanted robocalls. The principles include a commitment from the service providers to implement STIR/SHAKEN technical standards for call authentication.
- In October 2019, the California Attorney General (CAG) released proposed regulations to implement the California Consumer Privacy Act (CCPA) and provide compliance guidance for businesses, including an Initial Statement of Reasons that offers an overview on the CAG's rationale and guiding principles behind the regulations. The CAG released revised proposed regulations in February 2020. The proposed CCPA regulations generally address:
  - how businesses should provide notice to consumers of their rights;
  - how businesses should handle consumer opt-outs and other requests;
  - how businesses should verify a consumer's identity;
  - what additional information should be in businesses' privacy policies;
  - what limitations businesses should place on their service providers; and
  - how businesses can comply with the CCPA's anti-discrimination provisions while offering financial incentives to consumers who do not opt out of the sale of their personal information.

  (For more information, search California Consumer Privacy Act (CCPA) Toolkit on Practical Law.)

- The New York State Department of Health implemented a notification (OHIM DAL 19-01 (Aug. 12, 2019)) outlining a new protocol that health care providers should use to inform the state of cyber incidents.
- The Maryland Insurance Administration released Bulletin 19-14 (Aug. 29, 2019), available at *insurance.maryland.gov*, requiring health insurers, HMOs, managed care organizations, and third-party administrators to notify them of a data breach if the company's investigation determines a likelihood that personal information has been or will be misused.

SINGLE-STATE ENFORCEMENT ACTIONS

State attorneys general and other agencies continued to pursue privacy and data security enforcement actions in 2019, including in:

- California, where the CAG announced a $935,000 settlement with Aetna Inc. regarding a vendor mailing error that sent letters with oversized clear windows revealing that recipients take HIV-related medication (Press Release, Cal. Office of the Att'y Gen., Attorney General Becerra Announces $935,000 Settlement with Aetna over Allegations that it Revealed Californians' HIV Status (Jan. 30, 2019), available at *oag.ca.gov*).
- Massachusetts, which settled with:
  - CoPilot Provider Support Services Inc. for $120,000 and an agreement to update security policies following its alleged failure to provide timely notice of a data breach (Press Release, Mass. Office of the Att'y Gen., Healthcare Services and IT Provider Resolves Data Breach Affecting Nearly 1,900 Massachusetts Residents (July 2, 2019), available at *mass.gov*); and
  - online sock retailer Bombas LLC for $85,000 regarding a data breach and compelled the retailer to maintain a written information security program and institute reasonable safeguards for customers' personal information (Press Release, Mass. Office of the Att'y Gen., Online Sock Retailer Resolves Claims of Violating Data Security Laws (Aug. 12, 2019), available at *mass.gov*).
- New York, which settled with:
  - Bombas LLC for $65,000 and an agreement to bolster its data security policies over claims the online sock retailer failed to protect customers' personal information and provide timely notice of its data breach (Press Release, N.Y. Office of the Att'y Gen., Attorney General James Announces $65,000 Settlement With Online Retailer Bombas LLC Over Consumer Data Breach (June 6, 2019), available at *ag.ny.gov*); and
  - dating app operator Online Buddies, Inc. for $240,000 and promises to improve its user information safeguards following claims that the app failed to secure "private" and nude photos and the mobile device data of its LGBTQIA+ users (Press Release, N.Y. Office of the Att'y Gen., Attorney General James Announces Settlement With Dating App For Failure To Secure Private And Nude Photos (June 28, 2019), available at *ag.ny.gov*).
- Pennsylvania, which settled with travel website providers Orbitz Worldwide LLC and Expedia, Inc. for $110,000 and promises to strengthen security practices, including complying with the Payment Card Industry Data Security Standard (PCI DSS), following a 2018 data breach and allegations of privacy policy misrepresentations concerning safeguards for customers' personal information (Press Release, Pa. Office of the Att'y Gen., AG Shapiro Announces Settlement with Orbitz and Expedia in Data Breach Affecting Pennsylvania Consumers (Dec. 13, 2019), available at *attorneygeneral.gov*).
- Vermont, which settled with New England Municipal Resource Center for $30,000 and commitments to improve its information security program and employee training over data security allegations regarding its municipal management software, including failing to encrypt sensitive information (Press Release, Vt. Office of the Att'y Gen., Attorney General Donovan Settles with Supplier of Software to Vermont Cities and Towns (May 23, 2019), available at *ago.vermont.gov*).

MULTISTATE ENFORCEMENT ACTIONS

The trend of multistate and federal-state cooperation in privacy enforcement continued in 2019. For example:

- Healthcare software providers Medical Informatics Engineering Inc. and NoMoreClipboard, LLC agreed to pay $900,000 and improve their data security practices in a settlement with 16 state attorneys general in a novel multistate HIPAA lawsuit, stemming from a breach of PHI affecting more than 3.9 million individuals (Press Release, Ariz. Office of the Att'y Gen., AG Brnovich Announces Settlement in First-Ever Multistate HIPAA-Related Data Breach Lawsuit (June 4, 2019), available at *az.ag.gov*).
- Premera Blue Cross agreed to pay $10 million and ensure its data security program complies with HIPAA to resolve allegations that its failure to secure PHI resulted in a data breach affecting more than 10.4 million consumers (for more information, search State Attorneys General Secure $10 Million Settlement in Multistate HIPAA Data Breach Lawsuit on Practical Law).
- Equifax Inc. agreed to pay at least $575 million and bolster its information security program in a settlement with the FTC and 50 states regarding allegations that the company's cybersecurity failures resulted in the 2017 mega breach that affected 147 million people (for more information, search Equifax to Pay $575 Million to Settle Data Breach Claims with FTC, CFPB, and State AGs on Practical Law).
- In a potential trend-setting application of the False Claims Act, Cisco Systems, Inc. entered into an

$8.6 million federal and multistate agreement to settle allegations that the video security software it sold to various government agencies had cyber vulnerabilities (Mark Chandler, Cisco Blogs, Executive Platform, A Changed Environment Requires a Changed Approach (July 31, 2019), available at *blogs.cisco.com*).

PRIVATE LITIGATION

Standing remained a key issue for privacy-related litigation in 2019, especially in actions alleging procedural violations of the FCRA and the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Some notable cases include:

- *Kamal v. J. Crew Group, Inc.*, 918 F.3d 102 (3d Cir. 2019) (printing receipt with too many credit card digits is a technical violation without any concrete harm, and thus no standing conferred) (for more information, search Third Circuit Applies Spokeo to Find No Standing for FACTA Violation on Practical Law).
- *Jeffries v. Volume Servs. Am., Inc.*, 928 F.3d 1059 (D.C. Cir. 2019) (conferring standing where printing full credit card number exposed the plaintiff to increased risk, because the receipt "bore sufficient information for a criminal to defraud her").
- *Muransky v. Godiva Chocolatier, Inc.*, 922 F.3d 1175 (11th Cir. 2019), *vacated en banc* (939 F.3d 1278) (11th Cir. 2019) (initially conferring standing where receipt showed too many digits, because a violation of FACTA's truncation requirement could cause a marginal increase in the risk of harm).

Search Trends in Privacy and Data Security: 2019 for the complete online version of this resource, which includes information on US Supreme Court rulings, data breach-related actions, biometrics decisions, and cases involving the Telephone Consumer Protection Act of 1991 (TCPA) from the past year.

FEDERAL AND STATE LEGISLATION

Despite the lack of a viable comprehensive federal privacy bill, Congress debated multiple data security proposals, including those that would enhance cyber information sharing for state and local governments.

Search 2019-2020 Federal and State Privacy-Related Legislation Tracker for more on notable privacy-related legislation.

Ultimately, Congress only passed the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), which:

- Grants the Federal Communications Commission (FCC) increased enforcement powers and a longer statute of limitations to pursue illegal robocallers.
- Requires the FCC to conduct a rulemaking to support a private entity's voluntary sharing of information about robocall and spoofing violations.
- Obligates carriers to adopt the STIR/SHAKEN protocol.

Search TRACED Act Implementation Imposes New TCPA Penalties and Requirements Regarding Robocalls for more on the TRACED Act.

Despite the lack of a viable comprehensive federal privacy bill, Congress debated multiple data security proposals, including those that would enhance cyber information sharing for state and local governments. Ultimately, Congress only passed the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act).

States continued filling in the gap by enacting laws addressing consumer data privacy and cybersecurity, and extending their data breach notification laws.

KEY CHANGES IN STATE DATA PRIVACY LAW

Several states made notable changes in their data privacy laws, for example:

- **California.** While a new 2019 law requires CAG registration for data brokers (Cal. Civ. Code § 1798.99.80), CCPA-related activities are the focus. Further:
  - the state enacted multiple amendments clarifying the law's scope and requirements (for more information, search California Governor Signs CCPA and Data Breach Law Amendments on Practical Law);
  - the CAG released draft regulations (see above *State Regulatory Developments*); and
  - Californians for Consumer Privacy filed and the CAG released the title and summary for a 2020 ballot initiative to create a dedicated privacy protection agency in California and expand the CCPA's data protection rights and obligations (Press Release, Californians for Consumer Privacy, CA Attorney General Becerra Releases the Title and Summary for Initiative to Protect Consumer Privacy (Dec. 17, 2019), available at *caprivacy.org*).
- **Maine.** A new broadband privacy law imposes data protection obligations on internet service providers (ISPs) and prohibits them from using, selling, disclosing, or permitting access to a customer's personal information without express, opt-in consent, unless an exception applies. ISPs cannot impose a penalty or offer a discount based on the customer's decision. (For more information, search Maine's Governor Signs New Internet Privacy Law on Practical Law.)
- **Nevada.** SB 220 amended the state's online privacy law to allow consumers to prevent websites and online service providers from selling personally identifiable information that they collect. Under SB 220, sale means the exchange of covered information for money to a person who will then license or sell it, which is narrower and less ambiguous than the CCPA's definition. (For more information, search Nevada Gives Consumers 'Do Not Sell' Rights Under Online Privacy Law on Practical Law.)
- **New York.** S.4119 prohibits ambulance and first responder service providers from disclosing or selling patient information to third parties for marketing purposes (for more information, search New York Enacts Law to Stop Ambulance Services and First Responders from Selling Patient Information on Practical Law).
- **Utah.** HB 57 is the country's first law prohibiting law enforcement from accessing electronic information without first obtaining a search warrant (for more information, search Utah Enacts Electronic Privacy Law on Practical Law).

STATE DATA BREACH NOTIFICATION LAWS

Reacting to mega breaches and other cybersecurity issues, some states amended their existing data breach notification laws in 2019. For example:

- Arkansas amended its law by:
  - expanding the definition of personal information to include biometric data;
  - requiring notification to the attorney general if a breach affects more than 1,000 individuals; and
  - imposing specific data retention obligations for data breach documentation.

  (Ark. Code Ann. §§ 4-110-101 to 4-110-108.)
- California updated its law alongside its CCPA amendments by expanding the definition of personal information (Cal. Civ. Code §§ 1798.29 and 1798.82).
- Illinois amended its law to update its notification requirements, including requiring notice to the attorney general, if a breach affects more than 500 residents (815 ILCS 530/10).
- Indiana imposed data breach notification and certain data disposal requirements on loan brokers and processing companies (Ind. Code §§ 23-2.5-8-8 to 23-2.5-8-9).
- Maryland amended its law to prohibit:
  - a company that incurs a data breach involving data that is not its own from charging a fee to the data owner for providing information that the owner needs to make a breach notification; and
  - a data owner from using the breach information for purposes other than providing notification or data security.

  (Md. Code Ann., Com. Law § 14-3504(c).)
- Massachusetts updated its law requiring companies to:
  - provide additional information when giving notice to the attorney general, including whether the company maintains a written information security program;
  - offer 18 months of free credit monitoring if the breach discloses an individual's Social Security number;
  - notify residents affected by the breach on a "rolling" basis, as soon as practicable, and without reasonable delay; and
  - identify the parent or affiliated corporation in the notice to affected residents, if another person or corporation owns the company that experienced the data breach.

  (For more information, search Massachusetts Updates Breach Notification Law Requirements on Practical Law.)

- New Jersey amended its law to:
  - expand the definition of personal information; and
  - restrict email notifications to affected individuals when their email addresses are compromised.

  (N.J.S.A. 56:8-161 and 56:8-163.)
- New York enacted the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which amended its laws by:
  - expanding the definition of private information;
  - expanding the circumstances that trigger breach notification;
  - modifying breach notification form and content requirements;
  - increasing penalties; and
  - imposing proactive information security obligations.

  (For more information, search New York Amends Data Breach Notification, Information Security, and Identity Theft Prevention Obligations on Practical Law.)
- Oregon amended its law to clarify certain definitions and impose notification requirements on vendors that discover or have reason to know about security breaches (Or. Rev. Stat. §§ 646A.602 to 646A.622).
- Texas enacted the Texas Privacy Protection Act, which created the Texas Privacy Protection Advisory Council and amended its law by requiring notification:
  - without unreasonable delay and no later than 60 days after determination of a breach; and
  - to the Texas attorney general for breaches affecting more than 250 residents.

  (For more information, search Texas Enacts Privacy Protection Act on Practical Law.)
- Virginia amended its law by expanding the definition of personal information to include a passport number or military identification number (Va. Code Ann. § 18.2-186.6).
- Washington amended its law by expanding the definition of personal information and adding detailed notification requirements (for more information, search Washington Amends Data Breach Notification Law on Practical Law).

OTHER STATE CYBERSECURITY LAWS

Several states joined South Carolina in 2019 by enacting data security laws focused on the insurance industry and the sensitive data it handles, generally following the National Association of Insurance Commissioners (NAIC) Model Insurance Data Security Law (MDL-668). Specifically:

- Alabama (Ala. Code § 27-62-1 to 27-62-11).
- Connecticut (Section 230, 2019 Conn. Legis. Serv. P.A. 19-117 (HB 7424)).
- Delaware (18 Del. C. §§ 8601 to 8611).
- Mississippi (Miss. Code Ann. § 83-5-801 to 83-5-825).
- New Hampshire (N.H. RSA §§ 420-P:1 to 14).

Michigan and Ohio enacted their insurance data security laws days before the end of 2018 (MCL 500.550 to 500.565; Ohio R.C. 3965.01 to 3965.11), while New York already protects insurance-related data under its NYDFS regulations.

The early 2020 legislative season indicates that additional states will follow.

INTERNATIONAL DEVELOPMENTS

In 2019, international agreements, cross-border data transfer frameworks, new regulations, and related enforcement actions affected US companies with international reach. European laws and regulations continue to wield a strong influence. However, the year also saw a growing trend in data protection laws and regulations globally, including in the Asia-Pacific region, Brazil, and Kenya.

CLOUD ACT

The US and the UK entered into the first Clarifying Lawful Overseas Use of Data (CLOUD) Act agreement that allows both countries' law enforcement agencies, under certain procedures, to demand electronic data directly from technology service providers in the other country (see Press Release, US Department of Justice, US and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online (Oct. 3, 2019), available at *justice.gov*).

GDPR

Data protection obligations for companies that collect and use information from individuals in the EU are undergoing a significant transition with the General Data Protection Regulation (GDPR), which took effect on May 25, 2018. This trend continued throughout 2019 as the EU and the rest of the world learned more about:

- The regulation's nuances and scope.
- European regulators' enforcement priorities, as shown in their initial enforcement actions, which generally focused on transparency and data security controls.

The European Commission (EC) published an impact assessment on the GDPR's first year, concluding that while work remains, member states mostly have set up the necessary legal framework and companies are building a compliance culture (see EC, Communication: Data Protection Rules as a Trust-Enabler in the EU and Beyond—Taking Stock (COM/2019/374) (July 24, 2019), available at *ec.europa.eu*).

The EU's European Data Protection Board (EDPB), which includes member states' data protection authorities (DPAs), provided guidance on key GDPR concepts and compliance obligations, including lawful bases for processing personal data under GDPR, Article 6(1) (EDPB, Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects, Version 2.0 (Oct. 8, 2019), available at *edpb.europa.eu*). Various DPAs also

continue to provide localized guidance at the member state level.

Search GDPR Resources for US Practitioners Toolkit for resources to assist counsel in advising US-based clients on the GDPR.

EU-US PRIVACY SHIELD

In 2019, EU and US officials cooperated on a third annual review of the EU-US Privacy Shield, and the US Senate confirmed the first permanent Privacy Shield Ombudsperson at the State Department. The EC published an October 2019 report, concluding that the US continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield. The FTC also continues to support EU confidence in the Privacy Shield through its enforcement activities.

Search Trends in Privacy and Data Security: 2019 for the complete online version of this resource, which includes information on notable European Court of Justice decisions, the APEC CBPR system, and Canada's treatment of cross-border data flows.

LOOKING FORWARD

Privacy and data security issues likely to get particular attention in 2020 include:

- **Data privacy compliance issues, with a special focus on the GDPR, Brexit, the CCPA, and additional state and local regulation.** With the CCPA becoming operative in 2020, counsel should expect companies to continue improving their compliance procedures and carefully watch enforcement and private litigation trends, including how targeted companies use their statutory opportunities to cure violations. Multinational companies should continue to track GDPR enforcement trends for insight on DPA priorities, especially as Brexit proceeds. At the same time, while there appears to be an earnest congressional desire to enact a comprehensive data privacy law, passage is still in doubt, leaving states to continue filling the gap in data privacy regulation. Without a federal privacy bill that preempts all or at least some state laws, companies are still left to comply with a disparate patchwork of laws and regulatory expectations. These expectations may not overlap in focus or methods but will likely continue, especially with US and global regulators empowered from their stepped up actions and record fines in 2019.
- **Biometrics privacy.** With more companies exploring consumer-facing technologies that use biometric authentication and more governments using facial recognition for surveillance or security purposes, the debate will likely continue over the legal, technical, and ethical issues surrounding these technologies. Counsel should expect continued litigation under Illinois's Biometric Information Privacy Act. More states, local governments, and even Congress may take up reasonable limitations on using facial recognition, following a handful of initial public sector bans in 2019.
- **Sector-specific and local cyber risks.** No company is immune from cyberattacks, which are often crimes of opportunity. However, certain sectors that hold especially valuable personal data, such as financial services and health care, will continue to be hackers' priority targets. Some commentators have suggested that emerging business areas, such as cryptocurrency, cannabis retailers, and mobile payment services, are also more likely targets. Local governments in 2019 suffered debilitating ransomware incidents, often due to a lack of cybersecurity resources and inadequate investments in technical controls and training. This trend is only likely to grow.
- **New applications of blockchain and artificial intelligence (AI) technologies.** Emerging blockchain technology may soon offer innovative approaches to identity management and other cybersecurity challenges, such as trusted information sharing, data tampering prevention, and even methods for fighting deepfake videos and other media. Balancing privacy and data security risks in blockchain applications will challenge early adopters. AI technology also offers innovative solutions, but raises ethical concerns. Counsel should expect these technologies to garner further attention as various industries move from concept and testing to launching operational pilot programs that analyze and make decisions from consumer data.

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