Arthimexdes/Shutterstock.com

TRENDS IN PRIVACY AND DATA SECURITY

As hacking and other cyber threats reached new heights in 2016 and captured worldwide attention, data privacy and cybersecurity remained top priorities for regulators and companies alike.

JEFFREY D. NEUBURGER
PARTNER
PROSKAUER ROSE LLP

Jeff is co-head of the firm's Technology, Media & Telecommunications Group, a member of the Privacy & Cybersecurity Group, and editor of the firm's New Media and Technology Law blog. His practice focuses on technology, media, and advertising-related business transactions and counseling, including the use of emerging technology and distribution methods in business.

As in the past several years, privacy and data security issues continued to garner attention from regulators, industry sectors, and consumers in 2016. Cybersecurity risks were a major focus, driven in large part by high-profile cyber attacks involving the presidential election that federal experts attributed to Russian hackers. Faced with growing vulnerabilities and more complex technologies, federal agencies increased their regulatory and enforcement efforts in the past year.

Companies and their counsel must stay aware of changes in this rapidly evolving area to meet emerging legal and marketplace expectations. To help manage risk, they must understand the dynamic legal framework and ensure their privacy policies and procedures are kept up to date.

This article reviews noteworthy privacy and data security developments in 2016 and highlights key issues for the year ahead. In particular, it addresses recent:

- Federal regulation and enforcement actions.
- State regulation and enforcement actions.
- Private litigation.
- Federal and state legislation.
- Cybersecurity issues and guidance.
- International developments likely to affect US companies.
- Trends likely to gain more prominence in 2017.

Search US Privacy and Data Security Law: Overview for more on the patchwork system of federal and state laws regulating privacy and data security, as well as common law principles and self-regulatory programs.

FEDERAL REGULATION AND ENFORCEMENT

The increase in activity by federal agencies in 2016 reflected growing concerns in privacy and data security and emphasized the overlapping, sector-specific nature of US laws. Agencies taking notable regulatory and enforcement actions included:

- The Federal Trade Commission (FTC).
- The Federal Communications Commission (FCC).
- The Department of Health and Human Services (HHS).

Search Trends in Privacy and Data Security: 2016 for the complete, online version of this resource, which includes information on regulatory and enforcement activity by the Consumer Financial Protection Bureau, the Department of Commerce, and the Securities and Exchange Commission, among others, as well as industry self-regulation efforts in the financial industry, the digital advertising industry, and the payment card industry.

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 2016, the FTC released guidance for companies on:

- **Big data analytics.** The FTC released *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues* to help companies ensure that their big data programs avoid exclusionary or discriminatory outcomes. The report emphasizes laws that might apply to big data analytics, including:
  - the Fair Credit Reporting Act (FCRA);
  - the FTC Act; and
  - equal opportunity laws.
- **Ransomware dangers.** The FTC held a workshop examining ransomware threats and steps for companies to take if they experience an attack. The FTC urged companies to prevent and prepare for these malicious software incidents, and stressed that failure to remediate vulnerabilities known to be exploited by ransomware could violate FTC Act Section 5. (For more on ransomware attacks, search Cybersecurity Tech Basics: Ransomware: Overview.)
- **Data breach response.** The FTC released *Data Breach Response: A Guide for Business* to assist companies in preparing for and responding to data breaches. The guide highlights notification requirements under various federal and state laws and provides a model data breach notification letter. (For more on data breach response, search Breach Notification.)

Additionally, the FTC issued a statement explaining that the National Institute of Standards and Technology (NIST) Cybersecurity Framework is consistent with the FTC's reasonableness standard and approach to data security enforcement (see below *Cybersecurity*).

FTC Enforcement Activity

Companies should routinely monitor the FTC's enforcement actions, especially in the absence of comprehensive federal data privacy law. The FTC's 2016 actions demonstrate that companies should:

- **Review privacy policies and verify compliance with commitments made.** A cloud-based electronic health record company settled charges that it misled consumers by soliciting doctor reviews without clearly disclosing that those reviews would be posted on the internet and could include patients' sensitive personal information (*In re Practice Fusion, Inc.*, FTC No. 142-3039, 2016 WL 4446476 (Decision and Order Aug. 15, 2016)). A digital advertising company also settled charges that it misled consumers by tracking their online activities using supercookies, or mobile carrier-injected unique identifiers, even after consumers took suggested steps to opt out (*In re Turn Inc.*, FTC No. 152-3099, 2016 WL 7448417 (settlement announced Dec. 20, 2016)).
- **Ensure that data security practices match claims made.** A Taiwan-based computer hardware maker settled charges that security flaws in its routers put consumers' home networks at risk and insecure cloud services led to the compromise of thousands of consumers' connected data storage devices (*In re ASUSTeK Computer, Inc.*, FTC No. 142-3156, 2016 WL 4128217 (Decision and Order July 18, 2016)).
- **Protect children's privacy when collecting app users' personal information.** A Singapore-based mobile advertising company agreed to pay $950,000 in civil penalties and settle charges that it deceptively tracked the geolocations of hundreds of millions of consumers, including children, to target advertising. The FTC also alleged that the company violated the Children's Online Privacy Protection Act (COPPA) by collecting geolocation data from child-targeted apps without obtaining appropriate parental consent. (Stipulated Order, *U.S. v. InMobi Pte Ltd.*, No. 16-3474 (N.D. Cal. June 22, 2016).) (For more on COPPA compliance, search Children's Online Privacy: COPPA Compliance.)

- **Review cross-border data transfer practices.** A US-based hand-held vaporizer manufacturer resolved claims that it deceived consumers about its participation in and certification status for the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR) system (*In re Very Incognito Techs., Inc.*, FTC No. 162-3034, 2016 WL 3626839 (Decision and Order June 21, 2016)). The FTC also issued warning letters to 28 companies that claimed to have APEC CBPR system certification but did not appear to be in compliance with its requirements (see Press Release, FTC, FTC Issues Warning Letters to Companies Claiming APEC Cross-Border Privacy Certification (July 14, 2016)). Enforcement activity related to cross-border data transfers will likely grow in light of the new EU-US Privacy Shield Framework announced in 2016 (see below *EU-US Privacy Shield*).

Companies also should note that the FTC adjusted the maximum civil penalties under various laws it enforces. For example, effective August 1, 2016, the FTC increased the maximum per violation civil penalty under FTC Act Section 5 from $16,000 to $40,000. In early 2017, the FTC made an additional inflation-based adjustment, raising the maximum per violation civil penalty to $40,654. (16 C.F.R. § 1.98.)

Limitations on FTC Authority

Companies facing enforcement actions challenged the FTC's authority with some success in the past year, specifically in cases involving:

- **The common carrier exception.** In *FTC v. AT&T Mobility LLC*, the US Court of Appeals for the Ninth Circuit held that the FTC could not challenge a mobile broadband carrier's "data throttling" reductions of speed to customers who were grandfathered into its unlimited data plans as an unfair or deceptive trade practice. The court held that FTC Act Section 5's common carrier exception applied based on AT&T's status as a regulated carrier, not whether the activities at issue were common carrier services at the time. (835 F.3d 993, 997-1003 (9th Cir. 2016).) The common carrier exception limits the FTC's ability to enforce its privacy and data security standards against FCC-regulated broadband internet service providers (ISPs) (see below *FCC*).
- **The statutory interpretation of "unfair" practices.** In *LabMD, Inc. v. FTC*, the US Court of Appeals for the Eleventh Circuit stayed enforcement of the FTC's final order in this long-running data security action pending appeal. The FTC order requires LabMD to implement a comprehensive information security program despite its defunct status and limited remaining use of consumer data. The court questioned both the FTC's broad statutory interpretation of unfair practices under the FTC Act and its reasonableness in concluding that LabMD's actions were likely to have caused substantial consumer injury. (*LabMD, Inc. v. FTC*, 2016 WL 8116800, at *2-4 (11th Cir. Nov. 10, 2016); *In re LabMD, Inc.*, 2016 WL 4128215, at *29-32 (F.T.C. July 28, 2016).)

FCC

The FCC regulates telecommunications carriers' privacy and data security practices under Section 222 of the Communications Act of 1934, which imposes customer data handling obligations (47 U.S.C. § 222). Additionally, the FCC has regulatory and enforcement authority under the Telephone Consumer Protection Act of 1991 (TCPA), which restricts the manner by which businesses may contact consumers' telephones and fax machines and provides consumers with opt-out mechanisms (47 U.S.C. § 227).

Search Direct Marketing for more on the FCC's authority and standards.

Notably, the FCC's 2015 Open Internet Order reclassified broadband internet access as a telecommunications, or common carrier, service under Title II of the Communications Act. The FCC provided temporary Section 222 forbearance, pending the adoption of broadband-focused privacy rules in a separate rulemaking.

Broadband Consumer Privacy Rules

In late 2016, the FCC adopted new privacy regulations for carriers, including broadband ISPs. The new rules require ISPs to:

- Provide customers with notice and choice regarding the personal information that they collect and how they will use

The common carrier exception limits the FTC's ability to enforce its privacy and data security standards against FCC-regulated broadband internet service providers (ISPs).

and share it. The rules require different forms of customer consent, including opt-in and opt-out approvals, based on information sensitivity.

- Take reasonable security measures to protect customer information.
- Notify customers and the FCC and, in some cases, the Federal Bureau of Investigation (FBI) and the US Secret Service, if a data breach occurs.
- Avoid take-it-or-leave-it broadband service offerings that require customers to surrender privacy rights.
- Support heightened disclosure and affirmative consent requirements for offers that provide customers with financial incentives, such as lower monthly rates, in exchange for rights to use personal information.

The new data security requirements are effective March 2, 2017. However, the new notice and choice rules and breach notification rules contain information collection requirements that are pending approval by the Office of Management and Budget. (81 Fed. Reg. 87274 (Dec. 2, 2016).) Changes in FCC commissioners under the new administration are likely to drive further review and reconsideration (see below *Looking Forward*).

TCPA Order

The FCC recently clarified its rules under the TCPA related to informational calls from schools and utilities. The ruling declares that robocalls and automated texts are permitted when they are sent by:

- Schools contacting student family wireless phones for:
  - emergency purposes, including situations that affect the health and safety of students and faculty, regardless of prior express consent; and
  - purposes closely related to the school's mission, where the call or text recipient has provided the school with the number.
- Utility companies contacting customers about matters closely related to utility service, such as a service outage.

(*Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, 31 F.C.C. Rcd. 9054 (Aug. 4, 2016).)

FCC Enforcement Activity

The FCC settled an investigation with Verizon Wireless regarding the company's practice of inserting unique identifier headers (UIDH), or supercookies, into its customers' mobile internet traffic without their knowledge or consent for targeted advertising. Verizon Wireless paid a $1.35 million fine under the settlement and it must:

- Adopt a three-year compliance plan.
- Notify consumers about its targeted advertising programs.
- Obtain customers' opt-in consent before sharing UIDH with third parties.
- Obtain customers' opt-in or opt-out consent before sharing UIDH internally within Verizon Communications Inc. and its subsidiaries.

(*In re Cellco P'ship*, 31 F.C.C. Rcd. 1843 (Mar. 7, 2016).)

HHS

HHS provided guidance on several privacy and data security-related topics in the past year, and its Office for Civil Rights (OCR) investigated and took action against multiple organizations for failing to comply with regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Search HIPAA and Health Information Privacy Compliance Toolkit for a collection of resources to assist companies in complying with HIPAA regulations.

HHS Guidance

Useful resources issued by HHS in 2016 include:

- *Guidance on HIPAA & Cloud Computing*, which presents various questions and answers to help covered entities and business associates understand their obligations when using cloud-based services.
- *Fact Sheet: Ransomware and HIPAA*, which describes attack prevention and recovery from a healthcare perspective, including the preventive role that HIPAA compliance plays, and how to manage data breach notification obligations in response to a ransomware attack.
- *Postmarket Management of Cybersecurity in Medical Devices*, which provides guidance for industry and Food and Drug Administration (FDA) staff to use in managing cybersecurity vulnerabilities for marketed and distributed medical devices (for more information, search FDA Releases Guidance for Medical Device Cybersecurity).

HHS Enforcement Activity

OCR settled several notable enforcement actions in the past year, underscoring issues involving:

- Continuing gaps in risk analysis.
- Inadequate business associate oversight.
- Unencrypted computers and mobile devices.

For example, OCR entered into:

- A $2.14 million settlement and corrective action plan with St. Joseph Health (SJH) Cancer Care following SJH's report to OCR that protected health information was publicly accessible through internet search engines for over a year. OCR's investigation found that SJH failed to perform an appropriate enterprise-wide risk analysis and had retained default server settings, exposing the data of 31,800 individuals. (See Press Release, OCR, $2.14 Million HIPAA Settlement Underscores Importance of Managing Security Risk (Oct. 18, 2016).)
- A $5.55 million record-setting settlement and extensive corrective action plan with Advocate Health Care Network based on multiple, ongoing HIPAA violations and three separate data breach reports in less than four months, affecting approximately four million individuals (see Press Release, OCR, Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million (Aug. 4, 2016)).
- A $2.7 million settlement and corrective action plan with Oregon Health & Science University to address multiple HIPAA failures, including the lack of an enterprise-wide risk

analysis or a proper business associate agreement with a cloud services provider (see Press Release, OCR, Widespread HIPAA Vulnerabilities Result in $2.7 Million Settlement with Oregon Health & Science University (July 18, 2016)).

Additionally, in 2016, OCR:

- Began Phase 2 of its HIPAA Audit Program to review the policies and procedures adopted by covered entities and their business associates to meet selected elements of HIPAA regulations.
- Announced its intent to more widely investigate data breaches that affect fewer than 500 individuals through its regional offices.
- Increased its maximum civil monetary penalties for HIPAA violations (for more information, search HHS Increases Penalties for HIPAA Noncompliance, Effective August 1).

Search HIPAA Enforcement: Penalties and Investigations for more on procedures used by HHS to enforce HIPAA regulations.

STATE REGULATION AND ENFORCEMENT

Key regulatory developments at the state level in 2016 include:

- New cybersecurity rules for the financial services sector in New York.
- Various privacy and data security-related resources issued in California.
- Several single-state enforcement actions.
- A few high-profile multi-state enforcement actions.

NEW YORK REGULATIONS

The New York Department of Financial Services (NYDFS) proposed extensive cybersecurity regulations, but later updated them and delayed their implementation to March 1, 2017, following industry comments, with transition periods of up to two years for compliance with some requirements (23 NYCRR 500). Under the new regulations, banks, insurance companies, and other financial services organizations that NYDFS regulates must:

- Establish and maintain a cybersecurity program.
- Adopt a written cybersecurity policy that addresses specified areas, including:
  - third-party service provider management;
  - technical controls; and
  - incident response.
- Perform periodic risk assessments.
- Designate a chief information security officer.
- Comply with additional requirements, including:
  - conducting annual penetration tests;
  - maintaining audit trails;
  - training personnel;
  - ensuring secure data disposal; and
  - notifying regulators of cybersecurity events.

(See Press Release, NYDFS, Governor Cuomo Announces First-in-the-Nation Cybersecurity Regulation Protecting Consumers

and Financial Institutions from Cyber-Attacks to Take Effect March 1 (Feb. 16, 2017).)

CALIFORNIA RESOURCES

The California Attorney General issued several new resources in the past year, including:

- A set of guidelines, *Ready for School: Recommendations for the Ed Tech Industry to Protect the Privacy of Student Data*, which encourages education technology providers to focus on information that is useful for educational purposes and limit the collection and use of student data (for more on California's student privacy laws, search Student Privacy: Education Service Provider Requirements).
- The annual California Data Breach Report, which includes an extensive discussion and recommendations on reasonable data security practices under California law, and an endorsement of the Center for Internet Security's 20 Critical Security Controls (for more information, search California AG Releases 2016 Data Breach Report).
- An online form to help consumers report websites, apps, and other online services that violate the California Online Privacy Protection Act (CalOPPA) by failing to post adequate privacy policies or keep the commitments that they make (for more on CalOPPA, search California Privacy and Data Security Law: Overview).

SINGLE-STATE ENFORCEMENT ACTIONS

State attorneys general continued to pursue privacy enforcement actions in 2016, including actions in:

- New York, which:
  - settled for $100,000 and commitments to improve data security with EZcontactsUSA.com, after the company overstated its website security practices and failed to notify affected customers of a data breach that potentially exposed over 25,000 credit card numbers and other cardholder data (see Press Release, NY Office of the AG, AG Schneiderman Announces $100K Settlement With E-Retailer After Data Breach Exposes Over 25K Credit Card Numbers (Aug. 5, 2016)); and
  - investigated and settled for $3.1 million with a state contractor that transmitted personal data of over 16 million people to an offshore subcontractor, in violation of certain data protection provisions in its contract (see Press Release, NY Office of the AG, AG Schneiderman & IG Leahy Scott Obtain Groundbreaking Agreement with Government Contractor that Illegally Outsourced New York Jobs to India (Mar. 24, 2016)).
- Texas, which settled with app developer Juxta Labs, Inc., the maker of a popular teen-focused app. The company agreed to comply with COPPA, delete previously collected personal information of children under age 13, and pay a $30,000 civil penalty. (See Press Release, AG of Texas, AG Paxton Settles Suit with App Company Collecting Children's Information (Oct. 3, 2016).)
- Vermont, which entered into a settlement with Entrinsik to provide more explicit warnings about the files its software creates, after a Vermont college experienced a security breach that potentially exposed 14,000 Social Security numbers following its ordinary use of the company's browser-based reporting tool (see Press Release, Vermont Office of the AG, Attorney General Enters Unique Data Security Settlement with Software Developer (Oct. 12, 2016)).

MULTI-STATE ENFORCEMENT ACTIONS

2016 also saw the continuing trend of multi-state and federal-state cooperation in privacy enforcement. For example:

- Software company Adobe Systems Inc. settled with 15 states for $1 million and commitments to improve its security practices, regarding a 2013 data breach that potentially exposed approximately 500,000 individuals' personal information, including payment card data (see Press Release, NC Dep't of Justice, Adobe to Pay $1 Million for Data Breach, Bolster Security, AG Cooper Says (Nov. 14, 2016)).
- Owners of the dating site AshleyMadison.com settled with the FTC, 13 states, and the District of Columbia for $1.6 million and an agreement to institute a comprehensive information security program, on charges that they misled consumers and failed to protect the personal information of over 36 million users (for more information, search AshleyMadison.com Owners Agree to Pay $1.6 Million to Settle FTC and State Data Breach Charges).

PRIVATE LITIGATION

Privacy and data security issues continued to be an active area of private litigation in the past year. Some highlights include:

- The US Supreme Court's decision in *Spokeo, Inc. v. Robins*.
- Data breach-related actions.
- Suits stemming from emerging biometrics issues.
- Class actions under the Video Privacy Protection Act (VPPA).

Search Trends in Privacy and Data Security: 2016 for the complete, online version of this resource, which includes information on other notable privacy and data security-related decisions in 2016.

SPOKEO AND ITS IMPACT ON STANDING

The Supreme Court clarified its Article III standing standards in 2016, specifically in cases where plaintiffs allege statutory violations, as is common in privacy-related class actions. In *Spokeo*, the Supreme Court held that an action based on an alleged statutory violation, without a showing of concrete and particularized harm, does not satisfy the injury-in-fact requirement to establish standing.

Significant to privacy-related actions, the *Spokeo* decision:

- Acknowledged that intangible harms can confer standing.
- Directed courts to consider history and Congressional intent in analyzing intangible harms.
- Cautioned that plaintiffs do not automatically satisfy the injury-in-fact requirement simply because a statute grants a right and purports to authorize private actions, especially in the case of technical or procedural violations.

(136 S. Ct. 1540, 1549-50 (2016).)

Spokeo has undeniably increased dismissals on standing grounds for suits based on technical violations of federal statutes.

Spokeo has undeniably increased dismissals on standing grounds for suits based on technical violations of federal statutes. For example:

- In *Hancock v. Urban Outfitters, Inc.*, the US Court of Appeals for the District of Columbia Circuit held that plaintiffs failed to allege a concrete harm and so lacked standing for their challenge to two retailers' zip code requests despite District of Columbia consumer protection laws that limit retailer data collection (830 F.3d 511, 514-15 (D.C. Cir. 2016)).
- In *Braitberg v. Charter Communications, Inc.*, the US Court of Appeals for the Eighth Circuit held that mere retention of a customer's personally identifiable information by a cable company is a procedural violation that does not amount to concrete harm (836 F.3d 925, 929-31 (8th Cir. 2016)).
- In *Meyers v. Nicolet Restaurant of De Pere, LLC,* the US Court of Appeals for the Seventh Circuit extended *Spokeo* to Fair and Accurate Credit Transactions Act claims by holding that a showing of injury apart from the statutory violation is required to obtain standing (843 F.3d 724, 727-29 (7th Cir. 2016)).

However, other courts have reached varying results since *Spokeo*. For example, in *Galaria/Hancox v. Nationwide Mutual Insurance Co.*, the US Court of Appeals for the Sixth Circuit allowed data breach-related claims to proceed, finding sufficiently substantial risk of harm based on the theft of personal information (2016 WL 4728027, at *3-5 (6th Cir. Sept. 12, 2016)).

Search The Injury-In-Fact Test Post-Spokeo and Third and Seventh Circuits Weigh In on Article III Standing After Spokeo for more examples of contrasting applications of *Spokeo* in recent privacy and data security actions.

Spokeo also presents challenges to TCPA plaintiffs, since many TCPA claims assert procedural violations. However, the Supreme Court's decision in *Campbell-Ewald Co. v. Gomez* that an unaccepted offer for complete relief does not moot a plaintiff's individual claim or putative class claims also prevents defendants from "picking off" TCPA class representatives (136 S. Ct. 663, 670-72 (2016)).

Search TCPA Litigation: Key Issues and Considerations for more on private litigation under the TCPA, including offers of judgment and mootness issues.

DATA BREACH LITIGATION

As discussed above, standing was a central issue in 2016 for federal data breach cases. Most courts continued to hold that data breach plaintiffs lacked standing under *Clapper v. Amnesty International USA* (133 S. Ct. 1138 (2013)) and, more recently, *Spokeo*. However, in *Lewert v. P.F. Chang's China Bistro, Inc.*, the Seventh Circuit held that *Clapper* did not foreclose claims concerning an increased risk of fraudulent charges and identity theft where personal information had been stolen, at least at the motion-to-dismiss stage (819 F.3d 963, 966-69 (7th Cir. 2016)). The Sixth Circuit then reached a similar result post-*Spokeo* in *Galaria/Hancox*.

Even where plaintiffs can clear the standing hurdle, some courts have dismissed data breach claims on other grounds, for example:

- **The economic loss doctrine.** In *Longenecker-Wells v. Benecard Services Inc.*, the US Court of Appeals for the Third Circuit barred claims brought by employees and customers of a prescription benefit administration provider following a data breach, finding that Pennsylvania's economic loss doctrine barred negligence claims and rejecting the plaintiffs' implied contract claims (658 Fed. Appx. 659, 661-63 (3d Cir. 2016)).
- **Standard of care evidence.** In *Silverpop Systems, Inc. v. Leading Market Technologies, Inc.*, a digital marketing services provider defeated negligence claims following a data breach because the claimant failed to establish an applicable data security standard of care in the provider's industry (641 Fed. Appx. 849 (Mem), 852 (11th Cir. 2016)).

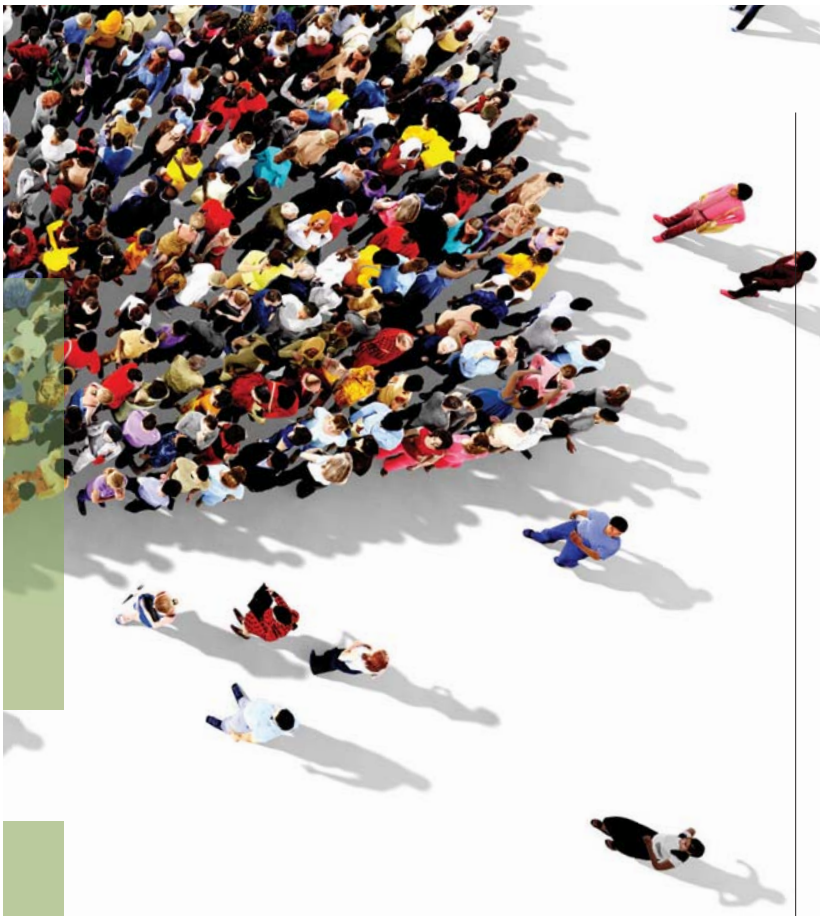
Search Key Issues in Consumer Data Breach Litigation for more on applicable law and theories of recovery in data breach cases.

Search Expert Q&A: Standing in Data Breach Class Actions for more on *Clapper* and its progeny.

BIOMETRICS LITIGATION

Private actions related to biometrics privacy and data security grew in the past year, as expected with the increasing commercial use of biometrics. Illinois's Biometric Information Privacy Act (BIPA) (740 ILCS 14/1) currently drives most actions, for example:

- Facebook, Inc. lost its first battle in consolidated class actions claiming the company's Tag Suggestions program violates BIPA's notice and consent requirements when it applies facial recognition to uploaded photos. The California district court:



- declined to enforce a California choice of law provision in Facebook's terms of use;
- held that the plaintiffs stated a claim under BIPA; and
- at this stage, declined to apply BIPA's photographs exception to Facebook's online processing.

(*In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1166, 1170-72 (N.D. Cal. 2016).)

- L.A. Tan Enterprises, Inc., a tanning salon operator and franchisor, settled an Illinois state BIPA action for $1.5 million regarding its customer fingerprint scanning practices that affected approximately 37,000 class members over three years. The company also agreed to comply with BIPA's requirements. (Stipulation of Class Action Settlement at 12-13, *Sekura v. L.A. Tan Enters., Inc.*, No. 15-CH-16694 (Ill. Cir. Ct. Cook Cnty. June 20, 2016).)

Search Biometrics Litigation: An Evolving Landscape for more on emerging issues in biometrics law and litigation.

VPPA CASES

In 2016, federal courts continued to address who qualifies as a consumer and what constitutes personally identifiable information (PII) under the VPPA, while considering *Spokeo*'s impact. Important decisions included:

- *Yershov v. Gannett Satellite Information Network, Inc.*, in which the US Court of Appeals for the First Circuit:
  - ruled that the plaintiff's download and use of a free mobile app made him a subscriber under the VPPA; and
  - affirmed that the device identifier, geolocation, and video history data the app disclosed to a third-party data analytics company constituted PII.

(820 F.3d 482, 486-90 (1st Cir. 2016).)

- *In re Nickelodeon Consumer Privacy Litigation*, in which the Third Circuit:
  - adopted a sliding scale test to determine when disclosure of different data elements could reasonably lead to an individual's identification;
  - ruled that information is not PII unless it readily permits an ordinary person to identify a specific individual's video watching behavior, unlike the digital identifiers at issue, including IP addresses, device identifiers, and browser fingerprints that on their own are not PII; and
  - distinguished *Yershov* by noting that geolocation data would fall closer to identifying an individual on its sliding scale.

(827 F.3d 262, 279-90 (3d Cir. 2016).)

FEDERAL AND STATE LEGISLATION

Congress considered bills, made inquiries, and held many privacy and data security-related hearings in 2016, especially on cybersecurity issues. However, as in other recent years, it took few legislative actions, leaving most issues that fall outside current regulatory authority to the states and industry.

Two important federal developments include the enactment of:

- **The Judicial Redress Act of 2015.** This law grants some foreign citizens the right to bring actions under the Privacy Act of 1974, and provides redress opportunities essential to the EU-US Privacy Shield Framework (Pub. L. No. 114-126; see below *EU-US Privacy Shield*).
- **The 21st Century Cures Act.** This law, among other things:
  - instructs HHS to provide additional HIPAA resources and guidance regarding appropriate uses and disclosures of protected health information; and
  - removes many health-related mobile apps from the Food, Drug, and Cosmetic Act's definition of a medical device, taking them outside the FDA's regulatory scope (for more information, search Obama Signs 21st Century Cures Act into Law).

(Pub. L. No. 114-255.)

States continued to build on their patchwork of privacy and data security laws in the past year. Several states revised their data breach notification laws, for example, to:

- Expand the definition of personal information to include encrypted data if the encryption key or security credential is compromised (see, for example, Cal. Civ. Code §§ 1798.29, 1798.82; 815 Ill. Comp. Stat. Ann. 530/5; Neb. Rev. Stat. § 87-802).
- Provide certain exemptions for covered entities subject to HIPAA (see, for example, 815 Ill. Comp. Stat. Ann. 530/50).
- Require notice to the state attorney general (see, for example, 815 Ill. Comp. Stat. Ann. 530/12; Neb. Rev. Stat. § 87-803).

- Expand the definition of unauthorized person to include an information holder's employees who acquire personal information and intentionally misuse it for unlawful purposes (see, for example, Tenn. Code Ann. § 47-18-2107).

Search Data Breach Notification Laws: State Q&A Tool to search and compare data breach notification laws across multiple jurisdictions.

Search Trends in Privacy and Data Security: 2016 for the complete, online version of this resource, which includes information on new student data privacy laws and other 2016 state law developments.

CYBERSECURITY

Cybersecurity risks gained widespread attention in 2016 due in large part to high-profile election year cyber attacks that federal experts attributed to Russian hackers in a joint Department of Homeland Security (DHS) and FBI report (DHS and FBI, Joint Analysis Report on Grizzly Steppe – Russian Malicious Cyber Activity (Dec. 29, 2016)). The global financial messaging network SWIFT also endured significant events, and several high-profile online services sustained major distributed denial-of-service (DDoS) attacks driven by armies of compromised internet of things (IoT) devices. Data breach reports continued across the public and private sectors, while ransomware attacks against large and small organizations reached new heights.

Most cyber attacks remain rooted in either social engineering, including phishing and other email-based methods that introduce malicious software (malware) or otherwise compromise an organization's environment, unaddressed vulnerabilities in software and configurations, or both.

Search Cybersecurity Tech Basics: Hacking and Network Intrusions: Overview, Cybersecurity Tech Basics: Malware and End User Attacks: Overview, and Cybersecurity Tech Basics: Ransomware: Overview for more on common types of cyber attacks.

Various agencies and industry groups provided guidance on cybersecurity issues, including strengthening cybersecurity practices, sharing information, and addressing IoT-related vulnerabilities.

PRINCIPLES AND BEST PRACTICES

NIST continued to foster a risk-based approach to cybersecurity by:

- Publishing *Small Business Information Security: The Fundamentals*, which provides guidance for small businesses on using the NIST Cybersecurity Framework.
- Releasing its draft Baldrige Cybersecurity Excellence Builder self-assessment tool to help organizations review how effectively they are using the NIST Cybersecurity Framework.
- Leading the National Initiative for Cybersecurity Education (NICE) and development of the NICE Cybersecurity Workforce Framework.

Search The NIST Cybersecurity Framework for more on implementing the NIST Cybersecurity Framework approach.

TOOLKITS

The following related Toolkits are available on Practical Law.

>> Simply search the resource title

- Privacy Compliance and Policies Toolkit
- Data Breach Toolkit
- Employee Privacy Compliance Toolkit
- Financial Privacy Compliance Toolkit
- HIPAA and Health Information Privacy Compliance Toolkit
- Information Security Toolkit
- Internet, Mobile, and Marketing Privacy Compliance Toolkit

The Obama administration also sustained its direct cybersecurity engagement in 2016 by issuing:

- Executive Order 13718 to establish a nonpartisan, NIST-coordinated Commission on Enhancing National Cybersecurity. In December 2016, the Commission released its *Report on Securing and Growing the Digital Economy*, which identifies six imperatives and recommendations for strengthening public and private sector cybersecurity practices.
- Presidential Policy Directive 41 (PPD-41), US Cyber Incident Coordination, which sets out principles and procedures to guide the federal response to significant cyber incidents. In January 2017, DHS issued an updated National Cyber Incident Response Plan as directed by PPD-41.

INFORMATION SHARING

Cybersecurity information sharing gained traction in the past year, aided by the Cybersecurity Information Sharing Act of 2015 (CISA). Many public and private sector organizations can benefit from sharing information on the threats they detect and the defensive measures they take. Some important information-sharing guidance was released in 2016 by:

- **DHS and the Department of Justice.** As required by CISA, these jointly issued guidelines and procedures govern cyber threat indicators federal entities receive and address how to share information through DHS's Automated Indicator Sharing capability, which was also made available in 2016 (for more information, search Department of Homeland Security and DOJ Issue Final CISA Guidance).
- **The Information Sharing and Analysis Organization (ISAO) Standards Organization.** Under 2015's Executive Order 13691, the ISAO Standards Organization published various resources, including voluntary guidelines for forming and maintaining ISAOs (see Press Release, ISAO Standards Organization, ISAO Standards Organization Releases Initial Voluntary Guidelines for ISAOs (Sept. 30, 2016)).
- **NIST.** In addition to the cybersecurity guidance and tools mentioned above, NIST published guidelines for organizations involved in information-sharing relationships (Chris Johnson, et al., *Guide to Cyber Threat Information Sharing*, NIST Special Publication 800-150 (Oct. 2016)).

Search Data Security Risk Assessments and Reporting for more on cybersecurity information-sharing programs.

IoT

The increased use of internet-connected devices, or the IoT, garnered more privacy and data security attention in 2016. Unfortunately, some device manufacturers continued to distribute and support IoT products with little or no built-in security, contrary to the FTC's recommendations and warnings. In October 2016, cyber attackers exploited these vulnerabilities to launch significant DDoS attacks that affected several high-profile websites and online services. The attacks reportedly used hundreds of thousands of malware-infected devices and prompted Congressional review.

Agencies and industry groups that provided IoT guidance include:

- **The National Telecommunications and Information Administration (NTIA).** The Department of Commerce's NTIA convened a meeting designed to develop a multistakeholder process to address security vulnerabilities and patching issues in IoT devices (see NTIA, Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching (2017), available at *ntia.doc.gov*).
- **Mobile telecommunications industry group GSMA.** This international group released privacy and data security guidelines targeted at IoT device developers, manufacturers, and service providers (for more information, search Mobile Industry Group Issues Internet of Things Privacy and Data Security Guidelines).
- **The Global Privacy Enforcement Network (GPEN).** At least 25 countries' data protection authorities participated in a privacy sweep of IoT devices by GPEN and reported findings that included many privacy and data security risks that they are considering for enforcement action (see Press Release, UK Info. Comm'r's Office, Privacy Regulators Study Finds Internet of Things Shortfalls (Sept. 22, 2016)).
- **DHS and NIST.** To help encourage IoT security throughout the device lifecycle, DHS published *Strategic Principles for Securing the Internet of Things* and NIST released Special Publication 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (for more information, search DHS and NIST Release New IoT Guidance).

Search The Internet of Things: Key Legal Issues for more on IoT issues and regulations.

INTERNATIONAL DEVELOPMENTS

In 2016, international agreements, such as the EU-US Privacy Shield Framework, and new regulations outside the US continued to shape the privacy practices of organizations with global reach.

Search Trends in Privacy and Data Security: 2016 for the complete, online version of this resource, which includes information on regulatory developments in Canada, Turkey, Russia, and China.

EU-US PRIVACY SHIELD

US and EU officials announced the adoption of the EU-US Privacy Shield Framework to replace the invalidated Safe Harbor program. The Privacy Shield supports cross-border personal information data transfers by businesses from EU member states to the US. The Department of Commerce began accepting self-certifications on August 1, 2016, and has over 1,500 organizations currently listed on its website.

Search Privacy Shield Self-Certification Checklist for steps to take when self-certifying to the EU-US Privacy Shield Framework.

Government surveillance concerns still cloud cross-border data transfers to the US. In July 2016, the EU's Article 29 Working Party, composed of member states' data protection authorities, announced that it would not contest the Privacy Shield program for at least one year. However, several European privacy groups, including Digital Rights Ireland, have challenged the Privacy Shield at EU General Court in other pending actions (see, for example, Case T-670/16, *Digital Rights Ireland v. Commission*; Case T-738/16, *La Quadrature du Net v. Commission*).

In early 2017, the US entered into a similar data transfer agreement with Switzerland (for more information, search US Enters Privacy Shield Data Transfer Agreement with Switzerland).

EU DEVELOPMENTS

The EU adopted the following two key pieces of privacy and data security legislation in 2016 that are likely to affect many multinational companies:

- **The General Data Protection Regulation (GDPR).** This replaces the EU Data Protection Directive and will apply in all member states beginning in May 2018. Businesses that operate in the EU should begin preparing for GDPR compliance now, because it differs from the prior Directive in many ways, including:
  - expanded territorial scope;
  - increased fines;
  - greater rights and control for data subjects, including a right to data portability;
  - more detailed conditions for using consent;
  - a requirement for many organizations to appoint a data protection officer; and
  - data breach notification obligations.
- **The Directive on Security of Network and Information Systems (NIS Directive).** This directive became effective in August 2016. Member states have 21 months from that time to transpose it into national law and six more months to

Organizations should review their information security and business continuity programs, while also considering whether their current cyberinsurance coverage is sufficient.

identify essential services operators. The NIS Directive lays out security and notification requirements for key service providers and requires member states to:

- adopt a national network and information systems security strategy;
- designate a national authority;
- support a Computer Security Incident Response Team (CSIRT); and
- engage with other member states through a CSIRT network.

In October 2016, the European Court of Justice also ruled that dynamic IP addresses might qualify as personal data under EU law (Case C-582/14, *Breyer v. Bundesrepublik Deutschland*, available at *curia.europa.eu*). However, the court limited its decision to those situations where an online service provider has legal access to data needed to identify an individual, for example, a public authority or an ISP that has access to dynamic IP address assignment records.

LOOKING FORWARD

Issues likely to get particular attention and affect privacy and data security trends in 2017 include:

- **Changes introduced by the Trump administration.** The new administration is already pointing to likely changes in privacy and data security expectations and enforcement. New leadership at both the FTC and the FCC indicate a refocus on actual harm in data security actions and a possible rollback of the FCC's new privacy rules. Cybersecurity risks will continue to receive bipartisan attention, based on recent attacks, although voluntary industry efforts are likely to gain renewed attention. For example, in early 2017, NIST issued draft updates to its Cybersecurity Framework for public discussion that emphasize managing vendors and measuring cybersecurity programs.
- **Cross-border data transfers.** Ongoing concerns regarding government surveillance, GDPR implementation, and growing interest in the APEC CBPR System will likely keep cross-border data transfers an active area, along with challenges to the EU-US Privacy Shield and long-used standard contract clauses.
- **Data security in critical sectors and the IoT.** Federal and state regulators are likely to continue raising the bar on proactive, risk management-based cybersecurity practices, especially in critical sectors such as financial services. Organizations that manufacture, distribute, and use IoT devices will be pressured to improve their data security practices and better manage risks, as seen in an early 2017 FTC action against wireless router and internet-connected camera maker D-Link (see Press Release, FTC, FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras (Jan. 5, 2017)).
- **Health information risks.** Hackers will continue targeting vulnerable, high-value health information and data-dependent healthcare organizations for cyber attacks, especially using ransomware. Organizations should review their information security and business continuity programs, while also considering whether their current cyberinsurance coverage is sufficient.
- **Privacy and transparency in smart toys.** Continuing the recent focus of regulators and advocates on children's privacy and COPPA enforcement, 2017 is likely to see increased attention on internet-connected, interactive (smart) toys, especially regarding transparency in parental notices, consent mechanisms, and other privacy controls.
- **State-level privacy litigation.** *Spokeo*'s impact will continue to be felt on data breach and other privacy-related litigation and might drive more cases into state court, complicating companies' defense strategies.

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