Top Data Governance Issues from 2017 and What to Watch in 2018

Having advised companies on privacy and data security issues for the past 20 years, it is always interesting to consider the previous year’s most significant industry events. In truth, we continue to press for resolution of the same issues year-after-year sometimes as to new technologies or applications. While the answer may be evasive, we moved further along the path of clarity in 2017 and will make further progress in 2018.

Data Breach Litigation: Beyond Spokeo

More than a year after the landmark Spokeo, Inc. v. Robins case, U.S. circuit courts remain divided on data breach and privacy litigation, leaving litigants likely to reach disparate results on Spokeo-based motions to dismiss. As has been the experience since 2005, courts will continue to wrestle with whether data breach cases deserve to go forward, coming to different results on similar issues, often motivated by a results-oriented analysis.

Even where plaintiffs had Article III standing, courts in the Third, Eighth, Ninth, Eleventh, and D.C. circuits still found grounds to dismiss claims based on the economic loss rule and the implausibility or insufficiency of damages allegations. Similarly, courts in the Second, Fourth, and Fifth circuits, where data breach litigation has been less frequent, have been more stringent on plaintiffs and have outright dismissed claims based on allegations of “future harm” as insufficient.

Yet, plaintiffs continue to explore new theories of liability for data breaches. Earlier this year, plaintiffs successfully defeated motions to dismiss in two separate cases in the Third and Sixth circuits, arguing that because the Fair Credit Reporting Act (FCRA) requires consumer reporting agencies to assure that “consumer reports” are delivered only to the intended recipients, implicit in such a requirement is a security obligation. That theory has not been followed by other district courts.

Relatedly, in March 2017, Smith v. Triad of Alabama, a case involving a data breach of records of less than 1,000 patients, became the first consumer data breach litigation to receive class certification.

For business-to-business breach litigation, 2017 has presented a mix of cases. Notably, in SELCO Comm. Credit Union v. Noodle & Co., the district court dismissed the complaint by a plaintiff credit union as barred by the economic loss rule, even though there was no privity of contract between the credit union and the defendant. In Community Bank of Trenton v. Schnuck Markets, the district court dismissed the action against the supermarket chain, finding that while other courts had found a duty of care between plaintiff banks and defendants, those decisions were made under different states’ laws. In USAA Fed. Savings Bank v. PLS Fin. Serv., the district court refused to find any general duty of care to secure PII for the defendant check processor, acknowledging it was deviating from precedence involving large retail breaches.

Data Misuse: Where Technicalities Matter

Compared to data breach cases, there is arguably even greater disparity among data misuse cases. This year, several cases were dismissed based on close readings and application of defendants’ respective terms and conditions.
conditions and privacy policies as well as the specific details of consumers’ use of and interaction with the applications and websites at issue, and the nature of the information collected. These considerations also raised concerns about individualized issues relating to consumers’ actual use and users’ consent that resulted in the denial of multiple motions for class certification.

Courts continue to struggle with applying privacy laws in the context of eCommerce written before or in the early days of the internet. In Pavone v. Meyerkord & Meyerkord, LLC, a plaintiff brought a putative class action alleging the defendants violated the Driver’s Privacy Protection Act (DPPA) by providing accident reports to law firms on behalf of law enforcement agencies. LexisNexis Risk Solutions Inc. and iyeTek, LLC defeated class certification, with the Court holding “that whether crash reports contain personal information from a motor vehicle record is an individualized inquiry that would predominate over questions common to the class.” The Seventh Circuit denied the plaintiff’s petition for leave to appeal the decision. In another DPPA case, Whitaker v. Appriss, the court granted summary judgment, holding that “name, address, and driver’s license number written down or scanned from a driver’s license handed over by the license-holder isn’t ‘personal information, from a motor vehicle record,’ protected by the DPPA.”

With respect to privacy laws governing the disclosure of consumer information, the Eleventh Circuit finally resolved the appeal of Perry v. Cable News Network, Inc. (CNN), which involved allegations that CNN violated the Video Privacy Protection Act (VPPA) by disclosing information to third parties about individuals’ use of CNN’s mobile application. The circuit court affirmed dismissal of the action, finding that the plaintiff was not a “subscriber” (statutory “consumer”) under the VPPA because there was no “ongoing commitment or relationship with CNN” other than the download of its mobile application.

In 2017, there were a handful of notable decisions involving audio, geolocation, and facial tracking technologies in which courts seemed to diverge on the level of specificity of the allegations required to maintain such claims. In Satchell v. Sonic Notify, Inc., a plaintiff brought a putative class action against a sports team, a mobile application developer, and an audio beacon developer, alleging multiple claims under the Federal Wiretap Act for purported “listening to” and recording of private communications using the Golden State Warriors mobile application and its integrated audio beacon technology. In November 2017, the mobile application developer obtained dismissal with prejudice of all claims asserted against the mobile application developer for failure to sufficiently allege how the developer unlawfully intercepted and recorded any consumer communications.

**Federal Trade Commission**

The FTC remains the most active cop on the privacy block. This is especially true with the Federal Communications Commission (FCC) recently announcing its withdrawal from privacy enforcement in broadband.

In February 2017, Vizio agreed to pay $2.2 million to the FTC for allegedly collecting the viewing histories of 11 million smart televisions without the end-users’ consent. As part of the consent decree, Vizio was required to delete data previously collected, prominently disclose and obtain affirmative express consent, implement a comprehensive data privacy program, and participate in biennial assessments. In a concurring opinion that nearly read like a dissenting opinion, new Trump-appointee and Acting Chairman Maureen Ohlhausen indicated that “under our statute (the FTC Act), we cannot find a practice unfair based primarily on public policy. Instead, we must determine whether the practice causes substantial injury.”

In July 2017, the FTC entered into a $104 million settlement with Blue Global, a loan lead generator, over allegations that the company induced customers to complete online applications for loans and then sold the personal information to “virtually anyone.” The FTC charged that Blue Global sold very few loan applications to lenders and instead sold the applications to the first buyer willing to pay for them.

**State Attorneys General**

State attorneys general have been particularly aggressive in enforcing proper online privacy practices, with New York now taking the lead. Organizations doing business in New York, New Jersey, and Massachusetts need to take heed of the state regulators’ increased action. With uncertainty looming at the CFPB and FTC, we expect to see greater activity at the state level.

For instance, in April 2017, the Massachusetts Attorney General entered into a settlement with Copley Advertising, which provided real-time advertising intelligence by using geo-fencing. The Attorney General alleged that the geo-fencing practice, which was implemented in the vicinity of reproductive clinics, violated consumer protection laws.

In May 2017, the New York Attorney General and Safetech Products entered into a settlement whereby the connecting doors and padlocks manufacturer agreed to better use encryption and to secure its wireless...
communications. The Attorney General had alleged that the company did not use encryption in its transmissions and that its password protocols were poor.

**Schrems 2.0 and the Future of EU-U.S. Data Flows**

Thousands of applicants have now come to rely on the EU-U.S. Privacy Shield Program as a means of demonstrating “adequate safeguards” to protect the personal information of European data subjects. However, it is unclear whether the program can survive unchanged as it ends its first year.

European authorities are already arguing for the program to be “temporary.” In light of President Trump’s ascension, EU Data Protection Supervisor Giovanni Buttarelli stated, “Something more robust needs to be conceived … . We should work in two tracks.” Additionally, in reviewing the EU-Canada airline passenger data-sharing pact, the Court of Justice for the European Union (CJEU) departed from “adequacy” language and scrutinized Canada’s pact step-by-step, focusing on the EU principles of necessity, proportionality, and retention.

**The Revised Draft ePrivacy Regulation**

While the Global Data Privacy Regulation (GDPR) has received substantial press, drafts of the complementary ePrivacy Regulation (ePrivacy Reg) has received less attention. It would be a grave mistake for an organization with substantial e-commerce activities to ignore these developments.

A proposed draft of the EU’s ePrivacy Reg was released in January 2017 (and subsequently updated in September). Intended to supplement the GDPR and repeal Directive 2002/58/EC generally, the ePrivacy Reg will have significant consequences for device manufacturers and software developers in the Internet of Things (IoT), autonomous cars, and augmented reality by (1) creating general limits on the use and storage of “electronic data”; (2) limiting end-user data collection through “terminal equipment”; and (3) specifying software privacy settings.

Significantly, the provisions mandate that the specified settings on terminal equipment shall apply to “terminal equipment placed on the market” and therefore would apply extra-territorially. On the other hand, Article 10 limits the requirement to the import and retail phase, without specific obligations to keep supporting the device and its software after it has been sold.

**China’s “Network Security Law” – One Year Later**

On November 7, 2016, China enacted its Cybersecurity Law, which became effective on June 1, 2017. Within it, a “Network Information Security” section sets forth requirements for the protection of the personal information of Chinese data subjects.

One year after its passage, predictions that the law was to be used primarily for political purposes have thus far proven true. Since the law took effect, over 40 percent of the enforcement actions were to remove “politically harmful contents,” and less than 3 percent were for protecting the “rights and interests” of the “internet user.”

© 2019 Troutman Sanders LLP