WINSTON & STRAWN LLP

BLOG

The Top 10 Privacy Changes in 2018 and What's on the Horizon for 2019

JANUARY 30, 2019

Winston's Global Privacy & Data Security Task Force has been monitoring key developments in privacy and provides this summary of key developments. 2018 was a busy year with General Data Protection Regulation enforcement actions, the new California Privacy & Cybersecurity Acts, data breach notification developments, and State and Federal enforcement actions among others.

1. **GDPR Enforcement**
   The EU General Data Protection Regulation (GDPR) became enforceable in May 2018. Privacy advocacy groups immediately filed complaints kicking off investigations of several Silicon Valley companies. Meanwhile, a Canadian data analytics firm was the first company to receive an enforcement action for receiving personal data of UK citizens to target those people with political advertising without their knowledge or consent. Enforcement actions have since accumulated as France's Data Protection Authority published a warning to two French companies for failing to obtain valid consent for the use of location data for profiling and targeted advertising. Germany's Data Protection Authority fined a chat application provider €20,000 after hackers stole unencrypted data concerning approximately 330,000 consumers.

2. **Enactment of California Consumer Privacy Act**
   California passed a groundbreaking law, California Consumer Privacy Act (CCPA) which goes into effect January 2020. California is the first state to pass a GDPR-inspired state privacy law. Although the CCPA protects California residents, businesses around the world must comply with the law, if they receive personal data from California residents and meet the threshold requirements. The law gives consumers more control over their personal information (PI), including (1) the right to know what information large corporations are collecting about them; (2) the right to tell a business not to share or sell their PI; and (3) the right to protections against businesses that compromise their PI. The law also provides a private right of action to bring data breach litigation.

3. **California's Cybersecurity Law Requiring Reasonable Security Measures**
   California also passed the Nation's first Internet of Things (IoT) Cybersecurity Law. When it takes effect in January 2020, SB 327 will require manufacturers of Internet-connected devices that are sold or offered for sale in California to equip the devices with "reasonable security features" designed to protect against unauthorized access, destruction, use, modification, or disclosure. Although the law is intentionally vague as to what constitutes a "reasonable security feature," it provides some broad parameters and examples of specific approaches that may satisfy the requirement.

4. **Significant Developments in Data Breach Notification Legislation**
   In 2018, data breach notification laws passed in South Dakota and Alabama. All 50 states and the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have data breach notification law. Additionally, Colorado and Louisiana passed significant amendments to their existing data breach notification laws in 2018, while Vermont passed the first privacy law directed specifically to data brokers, which includes, among other things, annual reporting and disclosure requirements.

5. **Regulation of Emerging Technology: Developments in ALPR/IoT**
   As privacy laws struggle to catch up to new technologies, several states passed new laws this year to regulate previously ungoverned technologies. One example is the increasing number of laws governing the collection and use of automatic license plate readers (ALPR). ALPR systems are a new type of artificial intelligence technology (AI) either fixed or attached to mobile vehicles and are constantly capturing and storing individuals' license plates. Only a small number of states currently regulate the commercial use of ALPR systems, but several laws are currently pending.

6. **The Supreme Court Expands Digital Privacy Rights in *Carpenter v. United States***
   The United State Supreme Court expanded data privacy protections in *Carpenter v. United States*, finding that the government needs a warrant to access cell site location information (CSIL). This data is automatically generated whenever a cell phone connects to a cell tower and is stored by wireless carriers for years. Cellphone location records are therefore subject to Fourth Amendment protections.

7. **The SEC Brings its First Enforcement Action Under the Identity Theft Red Flags Rule**
   In late September 2018, the Securities and Exchange Commission (SEC) brought and settled the first enforcement action brought under the Identity Theft Red Flags Rule (Red Flags Rule) since its adoption in 2013. As a result of a data breach, the SEC charged broker-dealer and investment adviser with violating the Red Flags Rule's requirement that financial institutions implement a written identity theft prevention program designed to detect the "red flags" of identity theft in their day-to-day operations. Without admitting or denying the SEC's findings, the financial firm agreed to be censured and pay a $1 million penalty.

8. **FCC Clashes with Courts over TCPA Interpretation and Enforcement**
   The Telephone Consumer Protection Act (TCPA) prohibits the use of certain automated dialing equipment to call wireless telephone numbers without consent. Last December, however, in *ACA International v. FCC*, the U.S. Circuit Court of Appeals for the District of Columbia vacated the FCC's broad definition of "capacity." The Third Circuit adopted the D.C. Circuit's reasoning and rejected of the FCC interpretation. However, in *Marks v. Crunch Sand Diego, LLC*, the Ninth Circuit moved in the opposite direction, expanding the definition of "capacity" beyond even the FCC's interpretation. In response to this circuit split, the FCC has sought comment on the definition of ATDS.

9. **Anthem's $16 million HIPAA Settlement**
   On October 18, 2018, Anthem, Inc., agreed to pay $16 million to the U.S. Department of Health and Human Services Office for Civil Rights (OCR) to settle its potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Anthem also agreed to undertake a robust corrective action plan to comply with the HIPAA rules. Separately, on August 15, 2018, the court also granted final approval of a settlement of $115 million to resolve the multidistrict class action litigation relating to the cyber-attack precipitating Anthem's potential HIPAA violations.

10. **Biometric Legislation & Litigation**
    The Biometric Information Privacy Act (BIPA) is one of three state laws (including Texas and Washington) that specifically regulates the collection, storage, and dissemination of biometric data. However, BIPA is unique in that it allows for a private right of action as well as statutory penalties. Under these laws, before collecting an individuals' personal information, an organization must obtain the individual's consent (which must be written under BIPA), inform the individual of its privacy and data retention practices, and be reasonable in protecting the collected data. In 2018, the battle lines in BIPA litigation were drawn on determining what amount of harm is necessary to establish a claim.

What we are watching in 2019

Passage of the new California Privacy law changes the landscape of data privacy in the United States, and the new

law is likely just the beginning. We anticipate additional state and federal privacy legislation and regulation in the coming year, and additional efforts to regulate emerging technologies and biometrics. On the federal side, Congress introduced two sweeping privacy bills at the end of last year. In 2019, we will be watching to see how regulators enforce GDPR and the current state and federal laws.

Learn more about these developments in our 2018 Privacy Year in Review.

5 Min Read

Authors

Shawn R. Obi

Eric Shinabarger

Alessandra Swanson

Related Topics

Data Breach | Europe Privacy | Health Care Privacy | Consumer Privacy | Biometrics

Related Capabilities

Privacy & Data Security | Privacy: Regulated Personal Information (RPI) | Health Care

Related Regions

North America | Europe

Related Professionals

Shawn R. Obi

Eric Shinabarger

Alessandra Swanson

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.