Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

California Tackles IoT Security with New Bill

The State of California is once again leading the way with trying to keep up with technology and protecting consumers. Senate Bill 327 requires Internet of Things (IoT) developers to implement "reasonable security features" in IoT products, such as baby monitors, televisions, automobiles, home appliances, fitness monitors, home security systems, and the like.

This is the first IoT security bill in the country, and is designed to make IoT product developers think about, and include, security features in IoT products in response to recent hacking incidents (e.g., a fish aquarium, baby monitors, cars, home security systems). The reasonable security measures include making sure that passwords are not easy to obtain which allows intruders access to IoT devices. *Read more*

ENFORCEMENT + LITIGATION

Two More Companies Sued Under Illinois Biometric Law

Two more companies are under fire for alleged violations of the Illinois Biometric Information Privacy Act (BIPA).

Loews Hotel in Chicago was recently sued in the Circuit Court of Cook County for allegedly violating BIPA by collecting employees' biometric information and sharing it with third parties without the employees' consent.

According to the suit, Loews is reaping the benefits of collecting employees' fingerprints through its timekeeping system and putting the employees' identities at risk, the named plaintiff alleges that the collection of his fingerprints exposes him to identity theft. He further alleges that Loews is sharing employees' biometric data with third-party vendors, including its payroll processor. *Read more*

September 27, 2018

FEATURED AUTHORS:

William M. Daley
Conor O. Duffy
Linn Foster Freedman
Deborah A. George
Kathryn M. Rattigan

FEATURED TOPICS:

Children's Privacy
Cybersecurity
Data Breach
Drones
Enforcement + Litigation
GDPR
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

CHILDREN'S PRIVACY

Protecting the Privacy of Children Online - Updates on COPPA

Protecting the privacy of our children is inherent to parenting. Parents guard against posting pictures of their children on social media or restrict the amount of time and the types of access they have on electronic devices. They may also set parental controls regarding content and try their best to protect their children. But what about the things we don't see, like what data is being collected about our children's online usage and what happens to it? The Children's Online Privacy Protection Act (COPPA), See 15 U.S.C. 6501 and regulations at 16 C.F.R. Part 312 et. seq. provide federal protections for children's personal information as it relates to online services. *Read more*

DATA BREACH

Years-Long Exposure of Sensitive Client Information Results in $200,000 Settlement with New York Attorney General

In late August, the Attorney General of the State of New York announced a $200,000 settlement with a New York-based non-profit organization that provides services to developmentally disabled individuals and their families after concluding that the organization exposed sensitive personal information of its clients on the Internet for almost three years. The settlement is the result of an investigation initiated in early 2018 in response to a tip that sensitive information of the organization's clients was available on its website. *Read more*

Uber Settles Data Breach Case With All 50 State AGs for $148 Million

On September 26, 2018, Uber Technologies Inc. agreed to finish the inquiries of all 50 states into its 2016 data breach by paying $148 million (in different amounts) to all 50 states and the District of Columbia.

The settlement concludes the investigations into the data breach, which occurred in 2016 when hackers absconded with the personal information of 57 million users and drivers, and Uber paid the hackers $100,000 to keep it quiet. The company did not notify the 57 million individuals of the data breach, which the attorney generals (AGs) alleged was a violation of state data breach notification laws and applicable state data security laws. *Read more*

GDPR

Will Insurance Provide Coverage for GDPR Fines?

As many of our readers know, the General Data Protection Regulation (GDPR) imposes significant obligations and responsibilities on entities with regard to data protection and privacy for all individuals within the European Union and the European Economic Area. Violations of GDPR can result in fines of up to €20 million, or up to 4 percent of annual global turnover, for the most severe violations, and fines of up to €10 million, or up to 2 percent of global turnover of the preceding fiscal year—whichever is higher—for less severe violations. Given the substantial magnitude of these potential fines, businesses may want to be proactive in determining what resources will be available to them in the event of a GDPR violation. *Read more*

DRONES

State Farm Uses Drones to Assess Damages from Hurricane Florence

State Farm has been granted a Federal Aviation Administration (FAA) waiver to use drones, under the Small Unmanned Aerial System (UAS) Rule (or Part 107), to assess damages in communities affected by Hurricane Florence. The Part 107 waiver allows both flights over people and flights beyond the drone operator's visual line of sight. These provisions were approved for four states impacted by the hurricane. *Read more*

New Patent Looks to Blockchain for Drone Security

According to recent documents made public by the U.S. Patent and Trademark Office (USPTO), IBM has applied for a patent for a system that would use distributed ledger technology to address privacy and security concerns associated with the increasing usage of drones in both commercial and recreational applications. In the application for this patent, IBM's authors describe how a blockchain ledger could be used to store data associated with drone flights, particularly when a security risk is considered to be relatively high, to help airspace controllers and regulators supervise the increasing number of drones that are now in the skies. The blocks may include a variety of different data points related to the drone's flight patterns, including its location, manufacturer and model number, any erratic behavior, weather conditions, and proximity to restricted zones. *Read more*

PRIVACY TIP #158

IoT Passwords

Considering the purchase of a smart appliance or home security system? This week's privacy tip focuses on securing devices with internet access, by setting a password, so they don't become a privacy weakness. *Read more*

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

Robinson & Cole LLP