Having trouble viewing this message? Please click here.

DATA BREACH

Trump Hotel Settles with NY Attorney General Over Credit Card Breaches

Trump International Hotels Management has agreed to pay the State of New York $50,000 for two data breaches that exposed over 70,000 customer credit card numbers and other personal information, according to New York Attorney General Eric Schneiderman. *Read more*

Hundreds to Thousands of Fort Carson Military Personnel Records Discovered on Dirt Road

At least hundreds, and potentially thousands, of files containing personal information originating from Fort Carson were discovered by News 5, in Fountain, Colorado, along a dirt road. News 5 sifted through the abandoned records and discovered detailed information about Department of Defense investigations into soldiers' conduct, disciplinary actions taken under the Uniform Code of Military Justice, and the results of investigations into alleged hate crimes, drug dealing, and at least one rape of a civilian woman. *Read more*

White House Investigating Data Breach of First Lady's Passport

It has been reported that the White House is investigating a hacking of the Gmail account of a contract worker who was working on the First Lady's advance team responsible for logistics. The hacking included emails from February 2015 through July 2016 and included a scan of First Lady Michelle Obama's passport. *Read more*

CYBERSECURITY

September 29, 2016

FEATURED AUTHORS:

Linn Foster Freedman
Kathryn M. Rattigan
Andrea Donovan Napp

FEATURED TOPICS:

Data Breach
Cybersecurity
Enforcement + Litigation
e-Discovery
Data Privacy
Digital Assets
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

Federal Government Releases Policy on Autonomous Vehicles

On September 21, 2016, the federal government, through the National Highway Transportation and Safety Administration (NHTSA), released "Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety," which is the first attempt to provide guidance to the auto industry about the issues inherent in the implementation of autonomous vehicles on public roadways. *Read more*

Additional Olympians' Medical Records Hacked by Fancy Bear

We previously reported that several U.S. Olympians' medical records were posted online by the Russian hacking group Fancy Bear [view related post]. The World Anti-Doping Agency (WADA) has confirmed that the medical records of 25 more Olympic athletes have been accessed and released online. *Read more*

ENFORCEMENT + LITIGATION

Recent FTC Consent Decree with InMobi for Unlawful Geolocational Tracking Provides Insight for App Developers

Recently, in *United States v. InMobi Pte Ltd.*, the Federal Trade Commission (FTC) set a new standard for geolocational tracking. The FTC told app developers and app marketers one simple rule: honor consumers location privacy preferences and do not track them without permission. *Read more*

---

e-DISCOVERY

Considering e-Discovery in Cloud Contracts

Earlier this year, I predicted that 2016 would be a year of increased focus on e-discovery from cloud-based sources and postulated that many organizations would demand better e-discovery solutions and increased cooperation from cloud providers. Industry experts agreed. So, what can proactive companies do to ensure that their cloud providers are on board for e-discovery purposes? *Read more*

DATA PRIVACY

Uber Announces Use of Facial Recognition Technology for Passenger

Safety

In an attempt to reduce fraud and boost passenger safety, Uber is implementing facial recognition technology beginning on September 30. Before starting a driving session, Uber drivers will now be asked to take a photo of themselves "periodically" so that Uber can match that photo against the photo Uber has on file. The driver's account will be temporarily blocked if the photos do not match. *Read more*

DIGITAL ASSETS

California Passes Revised Uniform Fiduciary Access to Digital Assets Act

On September 24, 2016, the governor of California approved the California Revised Uniform Fiduciary Access to Digital Assets Act, which "would authorize a decedent's personal representative or trustee to access and manage digital assets and electronic communications." It also allows a person to "use an online tool to give directions to the custodian of his or her digital assets regarding the disclosure of those assets." *Read more*

PRIVACY TIP #54

Keep Student Data Safe

In the past few years, we have seen the explosion of "big data," "data analytics," "data aggregation," "predictive modeling," and "data breaches."

None of these terms existed when I graduated from law school. We have seen companies implement amazing technology that has the ability to follow our every step for fitness, locate us through location based services, aggregate everything we buy and use our credit cards, and even know where we buy our gas for our car—and follow us with our EZ-Pass.

Adults have the ability to make (hopefully) educated decisions on who they allow access to their information. But kids don't have the luxury of making those decisions for themselves, and their information has been digital for a longer period of time and has been and will be aggregated, used, and sold for a much longer period of time into the future than any other generation.

Many people have commented to me that they are concerned about their child's privacy in reference to the child's school. Not only are they concerned about a data breach, but they are particularly concerned because many schools require students to access an online portal, which may not be secure, or download information onto a USB drive (and you know what I think of USB drives and, in

particular, unfamiliar USB drives that can be infected with malware and ransomware). Often parents and students don't have the ability to push back against school policies that may be putting students' data at risk.

Although 34 states have enacted legislation designed to protect students' privacy, the risks are growing and the data is getting bigger, and now the next generation's data is online more and longer than ever before.

I was pleased when the Southern Regional Education Board issued a report entitled "Data Privacy and Security," which addresses a number of concerns relating to student data and makes recommendations to states and education agencies to safely collect, govern, and share student data.

Recommendations in the report include evaluating data governance, being transparent about how data is collected, used, and disclosed; and using safeguards to guard against a data breach. The recommendations include being transparent in their data governance policies, monitoring data security programs and implementing policies for alerting the public when data breaches occur, training employees on state laws and FERPA, and having a strong information technology department in place to protect the data.

These are pretty standard recommendations, but ones that public and private schools don't often follow. Educators and administrators would do well to read the recommendations and implement them, and parents might wish to provide a copy of the recommendations to their child's school and start a dialogue on how the school is focused on protecting student data.