Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

**October 15, 2015**

## DATA BREACH

### American Thrift Stores Announces Data Breach

American Thrift Stores announced this week that like other retailers, it has been hit with a security breach "that occurred through software used by a third-party service provider" that allowed "criminals from Eastern Europe" to obtain unauthorized access to payment card numbers. According to American Thrift Store's statement, the Secret Service has advised that only card number and expiration dates were stolen. The breach occurred between September 1, 2015 and September 27, 2015.

American Thrift Stores states that it has removed the malware, but will not be providing customers with any identity theft protection services.

Security experts warn that this type of stolen data can be used to produce new counterfeit cards.

*— Linn Foster Freedman*

---

### OPM Data Breach Update

The Judicial Panel on Multidistrict Litigation has decided that the three lawsuits filed against the OPM by the National Treasure Employees Union, the American Federation of Government Employees and Mary Woo, a former employee of the U.S. Attorney for its data breach affecting 21.5 million individuals will proceed in U.S. District Court for the District of Columbia.

It was noted by the Judicial Panel on Multidistrict Litigation that almost a dozen other suits are pending but not transferred with this order, but may be transferred in the future.

*— Linn Foster Freedman*

---

## DATA PRIVACY

### California Electronic Communications Privacy Act Signed by Governor

Last Thursday, Governor Jerry Brown signed the California Electronic Communications Privacy Act (CalECPA) into law, which requires law enforcement to obtain a warrant before accessing or searching individuals' digital information, including emails, text messages, online materials, cellphones and other tracking devices.

The bill was supported by a wide coalition, including the ACLU of California, the California Newspaper Publishers Association, the Electronic Frontier Foundation, the American Library Association, Apple, Inc., the California Chamber of Commerce Association, Microsoft Corp., Google, Inc. and the California Public Defenders Association.

Not surprisingly, California is the trend setter and is the first state to enact a law aimed to combat

warrantless searches of digital information. We anticipate that other states will follow.

*— Linn Foster Freedman*

---

**Smart-TV Now Regulated Under New California Law**

Californians are now protected from smart-TV eavesdropping under new law, Assembly Bill 1116, which requires that smart-TV manufacturers ensure that voice-recognition features will not be enabled without consumer consent, and bars them from recording conversations for advertising purposes. For those smart-TV manufacturers that fail to implement privacy safeguards in accordance with this new law, the state attorney general or district attorney can prosecute those companies, and seek injunctive relief and a civil penalty up to $2,500 per violation; there is no private right of action under this new law.

Smart-TV manufacturers must also notify consumers that their voices may be recorded and transmitted to the manufacturers or third-parties. Assemblyman Mike Gatto, who also serves as the Chairman of the California Assembly's Privacy and Consumer Protection Committee, said, "We're not trying to stymie technological advances or fetter profit margins. The television industry has survived for over half a century without knowing what I said to my wife during an episode of 'The Bachelor.'" The law goes into effect January 1, 2016.

*— Kathryn M. Rattigan*

---

**New Landmark Consumer Disclosure Rules Trigger Privacy Concerns**

The Consumer Financial Protection Bureau's new "Know Before You Owe" mortgage disclosure rule is designed to prevent surprises at the closing table, but with increased transparency come concerns over borrower and seller privacy. The TILA RESPA Integrated Disclosure Rule (TRID) took effect October 3, 2015 and replaces four previous disclosure forms with just two, the Loan Estimate and the Closing Disclosure. The latter form contains a summary of the mortgage transaction, including personal details about the borrower and seller.

To address worries that the exposure of Non-public Personal Information (NPPI) contained in the Closing Disclosure could violate borrower and seller privacy, TRID allows the settlement agent to prepare two different forms for the parties, omitting the seller's personal information from the borrower's form and vice versa. While the CFPB has gone as far as providing model seller-only and borrower-only forms, preparing separate Closing Disclosures is not mandatory, highlighting fears that NPPI could be inadvertently disclosed.

In a separate issue also stemming from privacy concerns, some lenders remain hesitant to share the Closing Disclosure with real estate professionals without first obtaining consent from the borrower, believing that privacy laws might restrict the sharing of NPPI between the two parties.

A bill which would provide the mortgage industry with a four-month grace period regarding TRID compliance is currently making its way through Congress. Regardless of the outcome of the bill, Closing Disclosures are now a permanent part of the mortgage process and borrowers, sellers, and lenders all need to take steps to avoid the potential exposure of NPPI during the mortgage lending process.

*— Norman H. Roos and Scott M. Baird*

---

**Experts Cite Employee Wellness Programs as Area of Data Privacy Concern**

In an effort to curb rising health care costs, many employers have introduced wellness programs, which use assessments and motivators to improve employee health. Such programs collect information from various sources including surveys, gym records, lab tests, and even wearable devices. The problem, privacy experts say, is that there are few restrictions on how that information is ultimately used.

The companies administering wellness programs are often not bound by HIPAA and are free to develop and implement their own privacy policies, which can reserve the right to send personal information to third party vendors. Although wellness companies deny selling health information, there is potential for this information to be used in a variety of unexpected ways. For instance, the information could potentially be used by banks and insurance companies in determining who to lend money to, or whether to issue a life insurance policy. Companies could also use the information to market products to a particular person based on their health and lifestyle.

Further complicating the issue is the fact that employees have little control over their health information collected by wellness programs. Wellness programs typically require employees to sign complicated authorization forms that acknowledge that their information is no longer protected by privacy law and may be shared. Employees can choose to opt out of these programs; however, such a choice could result in a sharp increase in their health insurance costs.

These wellness programs are growing at a staggering rate, with estimates that it will be a $12 billion industry by 2020. Despite this growth, federal regulatory agencies have yet to decide whether oversight of the industry is needed.

*— Amanda E. Gordon and Andrew A. DePeau*

---

**ENFORCEMENT + LITIGATION**

**FCC Issues Supplementary Information Clarifying TCPA Robocall Rules**

We previously reported that the Federal Communications Commission (FCC) released an Omnibus Order on July 10, 2015 regarding the rules and regulations implementing the Telephone Consumer Protection Act (TCPA), specifically relating to robocalls.

Last week, in response to 21 inquiries following the release of the Omnibus Order, the FCC issued supplementary information in the Federal Register to clarify the limits and scope of the TCPA's robocall telemarketing ban, including "clarifying when certain conduct violates the TCPA and providing guidance intended to assist callers in avoiding violations and consequent litigation."

Specifically, the FCC reiterated that:

- Callers must obtain prior written consent even if they are not "currently" or "presently" dialing random or sequential phone numbers;
- Callers must get consent for robocalls if an acquaintance's phone contact is downloaded from a third-party app;
- Callers are liable for robocalls to reassigned wireless numbers, but get a one-call exception if the caller didn't know about the reassignment;
- Internet-to-phone text messages require consumer consent;
- Text messages are considered "calls" subject to the TCPA;
- Consumers may stop unwanted calls by revoking consent at any time and through any reasonable means, and carriers and VOIP providers may implement call-blocking technology to help consumers stop unwanted robocalls.

Additional clarification includes:

- App providers that play a minimal role in sending text messages are not per se liable for unwanted robocalls;
- Providers of collect-call services are not liable for making unwanted robocalls if the provider is giving consumers valuable call set-up information; and
- "On demand" text messages sent in response to a consumer request are not subject to TCPA liability

The TCPA continues to be a complicated compliance area and one that has the attention of class action

litigants, so it is beneficial to keep abreast of developments in this area if your business performs sales and marketing through telephone calls and texts.

*— Linn Foster Freedman*

---

**Amazon's Motion for Summary Judgment Denied in FCRA Class Action Suit**

U.S. District Judge Gary Feinerman denied Amazon, Inc.'s (Amazon) motion for summary judgment on October 7, 2015, in Illinois federal court, in a class action case over alleged violations of the Fair Credit Reporting Act (FCRA), stating that while Amazon said it offered plaintiff compensation to drop his accusations, "there is no offer of judgment as that term is understood." Under Amazon's offer, plaintiff would receive statutory damages related to the alleged FCRA violations, but would not address the relief plaintiff sought for actual damages he incurred from loss of employment.

The plaintiff, Gregory Williams, alleges that Amazon offered him a temporary position at one of its warehouses, but the offer was rescinded after a background check listed a felony – belonging to ANOTHER Gregory Williams. Williams claims that had he known about this negative background check result before Amazon decided to rescind the offer, he would have disputed it. Amazon contends that Williams was permitted to reapply for a position and that Amazon itself was not responsible for the adverse action, but SMX LLC (Amazon's third party staffing agency) is the one that completed the application process and the background check, as well as the one that ultimately took the adverse action. Amazon also contends that its offer of $1,000 would provide "full relief" to Williams and therefore any class action claims are moot. We'll let you know how it turns out.

*— Kathryn M. Rattigan*

---

**Users of Free Mobile Apps Not Protected by Video Privacy Protection Act**

Significantly, the Eleventh Circuit issued an opinion on October 9th that consumers who download and use free mobile apps do not fall within the definition of a "subscriber" under the Video Privacy Protection Act (VPPA). The VPPA was enacted in 1988 following the disclosure of U.S. Supreme Court nominee Robert Bork's video rental records (remember the questions around Anita Hill?). The significance of this ruling is that there has been a plethora of class action litigation against companies who disclose information about users of mobile apps without their consent.

In this case, The Cartoon Network allegedly disclosed information about its free mobile app users without their consent in violation of the VPPA. The Court disagreed and found that the mere downloading and viewing of freely available material through a free mobile app does not rise to the level of becoming a subscriber, who is afforded the protection of the VPPA.

Good news for companies that offer free mobile apps. Bad news for plaintiffs' class action attorneys.

*— Linn Foster Freedman*

---

**INFORMATION GOVERNANCE**

**Unmasking Information Governance: What Is It and How Do I Move It Forward In My Organization?**

The heightened state of information security in recent years has instigated genuine collaboration in many organizations, amongst its professionals in IT, records, security, risk, compliance, and other stakeholders in business management. After the various perspectives are heard, the need is clear – an Information Governance (IG) strategy.

What is IG? Wikipedia roughly defines IG as a set of multi-disciplinary structures, policies, procedures, processes, and controls implemented to manage information at an enterprise level, supporting an organization's immediate and future regulatory, legal, risk, and operational requirements. This definition

resonates with me and broadly covers the range of information-related concerns facing virtually all businesses today.

How do I move IG forward in my organization?

- **Establish a steering committee**. An effective IG program requires perspective, steering, and ultimately enforcement by a wide range of stakeholders such as the CEO, CIO, chief legal counsel, risk officer, compliance officer, and a variety of line-of-business executives.
- **Communicate goals and objectives**. While many of the objectives will relate to security, privacy, risk, and compliance, clearly stated goals that speak to operational efficiency, knowledge management benefits, reducing IT infrastructure costs, and more effective utilization of staff resources will more easily win the support of executive management and the organization as a whole.
- **Formalize a policy**. Keep the policy document as short and easy to digest as possible. The document will cover key policies, such as information security, privacy, legal compliance, records and information management. There is a real opportunity to include policies regarding document organization and naming standards, knowledge management, accuracy and completeness, and other information quality benefits. Roles will also be formalized in the policy document and appropriate authorities granted to support enforcement.
- **Rollout and ongoing education**. Key to the success of an IG program is enterprise-wide adoption. The rollout needs to touch just about everyone in the organization and ongoing training is a must to achieve stated goals and objectives.

Establishing an effective Information Governance program is no small task and this writing barely touches the iceberg. On the other hand, getting to a set of shared goals and objectives and realizing the benefits, from a risk mitigation and operational effectiveness perspective, is the first big step toward a successful implementation.

*— Fernando Monteleone*

---

**HIPAA**

**OCR Portal Designed for Medical Mobile App Developers**

The Office for Civil Rights (OCR) of the Department of Health and Human Services has launched a web-based portal so medical mobile app developers can ask their “burning” questions about HIPAA compliance.

The site, released last week, is designed to start a dialogue with mobile app developers about HIPAA requirements and how it can be more understandable in the digital age.

According to the OCR, “[A]ny posting or commenting is not going to be looked at for any enforcement action” so there is no risk of asking away before app developers launch their product. Of course, keep in mind that HIPAA compliance is a tricky matter and non-compliance can result in hefty fines and penalties.

*— Linn Foster Freedman*

---

**HEALTH INFORMATION**

**OIG issues Alert to “Remind” Providers That Information Blocking May Affect Safe Harbor Protection**

On October 6, 2015, the Office of Inspector General (OIG) of the Department of Health and Human Services issued OIG Policy Reminder: Information Blocking and the Federal Anti-Kickback Statute, which “reminds” providers that if electronic health records (EHR) are being used for information blocking, the donation of the EHR may not fall within the EHR safe harbor.

In order to fit within the EHR safe harbor, “[t]he donor (or any person on the donor’s behalf) does not take

any action to limit or restrict the use, compatibility, or interoperability of the items or services with other electronic prescribing or [EHR] systems (including, but not limited to, health information technology applications, products, or services)." The OIG noted that it has stated that such "donations would be suspect under the law as they would appear to be motivated, at least in part, by a purpose of securing… business." The OIG example is that if a provider/donor enters into an agreement with a technology vendor for the vendor to "charge high interface fees to non-recipient providers or suppliers or to competitors" may not fall within the safe harbor. According to the OIG, this "would pose legitimate concerns that parties were improperly locking-in data and referrals and that the arrangement in question would not qualify for safe harbor protection."

Blunt message from the OIG: follow the EHR safe harbor closely, and beware if you are using EHR donated technology to block information from competitors.

*— Linn Foster Freedman*

---

**HHS Releases Meaningful Use Final Rules**

After receiving over 2,500 comments from the public to the proposed rules, the Department of Health and Human Services (HHS) has released the long – awaited final rules for implementing Stage 3 of the Meaningful Use Program, applicable between 2015-2017. The rules are designed to improve health care through the use of health information technology.

The final rules will be used to transition physicians from the Meaningful Use program into a new merit based payment system. However, the rules do not delay implementation of Stage 3, which many stakeholders had requested.

The final rules include the following:

- Providers and state Medicaid agencies have until January 1, 2018 to comply
- Stage 3 will be optional in 2017
- Stage 3 has 8 objectives, 60% of which will require interoperability
- Cybersecurity requirements are strengthened
- The reporting period will be 90 days for all providers in 2015, for new providers in 2016 and 2017, and for any provider transitioning to Stage 3 in 2017

HHS also issued the 2015 edition for certification criteria in conjunction with the final rules.

Comments to the final rules will be open for 60 days.

*— Linn Foster Freedman*

---

**DIGITAL ASSETS**

**Uniform Law Commission Revises the Uniform Fiduciary Access to Digital Assets Act**

The Uniform Law Commission (ULC) adopted the Uniform Fiduciary Access to Digital Assets Act (UFADAA) in July 2014 to better align state laws with the virtual reality of modern economic and social life. Under the UFADAA, fiduciaries had the same access to digital assets as they did for tangible assets, but only for the limited purpose of carrying out their fiduciary duties. The ULC hoped the model legislation would be considered, and possibly enacted, in all 50 states. Despite early optimism, the bills were met with stiff resistance from industry coalitions who feared the UFADAA provided fiduciaries with too much access to a decedent's digital assets. By the middle of 2015, aside from a modified version in Delaware enacted in 2014, not one state had signed the model legislation into law.

In an effort to resolve the privacy issues that held back the proposal in 2015, the ULC released a revised UFADAA on September 28, 2015. The revised UFADAA greatly reduces the default authority of a fiduciary to access the digital assets of a decedent, instead providing greater legal effect to the decedent's instructions for the disposition of digital assets. The proposal introduces the concept of an

"online tool," defined as "an electronic service provided by the custodian that allows a user, in an agreement distinct from the terms-of-service agreement between the custodian and user, to provide directions for disclosure or non-disclosure of digital assets to a third person." The online tool will provide fiduciaries with clear, legally enforceable instructions on how digital assets are accessed. In the absence of consent via the online tool, a fiduciary would only have access to the content of a decedent's electronic communications if the decedent consented to such access in a will, trust, or other document. States are likely to begin considering the revised UFADAA in the beginning of 2016.

*— Scott N. Siedor*

---

**DRONES**

**No Flying Drones Over Celebrity's Homes, New California Law Passed**

If flying a drone over someone else's backyard to take some photos is one of your hobbies, think again. California just passed a new law into effect which makes the act of using a drone to take pictures of someone on their property a part of the existing physical invasion of privacy law. Assembly Bill 856 was first introduced by Assembly Member Ian Calderon, who said that he thought the existing law needed to be updated to close the loophole and to clarify that it is indeed trespassing for paparazzi to fly drones over private property. Calderon said, "We learned that the paparazzi have used drones for years to invade the privacy and capture pictures of public persons in their most private of activities –despite existing law," and this new law will prohibit these drones from entering "private sanctuaries," "peering into a stranger's window" and capturing "goings on and otherwise spy[ing] on the private lives of public persons."

*— Kathryn M. Rattigan*

---

**CYBERSECURITY**

**NIST Comment Period Closing for Energy and Health IT Sector Guides**

NIST has issued a reminder that the comment period for the draft Energy Sector guide "Identity and Access Management for Electric Utilities," and the draft Health IT guide, "Securing Electronic Health Records on Mobile Devices," will close on October 23, 2015.

Those wishing to comment can do so online or via email to energy_nccoe@nist.gov or HIT_NCCoE@nist.gov.

*— Linn Foster Freedman*

---

**Feds Continue to Prosecute Hackers**

Sergey Vovnenko, a Ukrainian hacker, was charged in New Jersey federal court this week for wire fraud conspiracy, unauthorized computer access and aggravated identity theft for allegedly hacking into networks of financial institutions and stealing log-in credentials and credit and debit card information. The indictment alleges that Vovnenko "commandeered thousands of computers to create a virtual army of hacked computers that he and his conspirators used to break into other networks and steal valuable information."

Vovnenko was able to obtain data from computers through a botnet of over 13,000 computers that were infected with malware, including the well-known "Zeus" which stole banking information by recording keystrokes of the users.

The U.S. Secret Service led the investigation and was assisted by Italian law enforcement. Vovnenko's arraignment is scheduled for October 19, 2015.

And last week, a California federal jury convicted Matthew Keys, a former social media editor of a news organization of three felonies, including conspiracy to make unauthorized changes to his employer's website, damage to computer systems and transmitting malicious code. He faces 25 years in prison and fines up to $750,000.

Keys was accused of assisting hacking group Anonymous infiltrate and alter the Los Angeles Times' website. He was prosecuted under the Computer Fraud and Abuse Act.

*— Linn Foster Freedman*

---

**Privacy Tip #5 - Retail Store Reward Cards**

Many retail pharmacies, supermarkets and other retailers offer rewards cards that offer discounts on certain items to be purchased in the store. They give you the cards that contain a bar code in regular size, which looks like a credit or debit card, or a handy miniature one you can put on your key ring so it's always available. In order to sign up for the rewards card, you usually have to give some personal information such as an email address, a residential address or a telephone number. Once you give them your information, you can use the card and shop away and get coupons and small discounts on items you purchase.

When you sign up for a rewards card, there are no limitations on what the store can do with the information you provide them, including the personal information you provided to get the card, and details about each purchase you make. Why is this a privacy concern?

For some, it's not. They are happy for the store to know exactly what they are purchasing and to sell that information to third parties. Others, like me, would rather not provide my personal information to the store or have them track my purchases and sell my purchases and preferences to others. Why? Because when stores like pharmacies, supermarkets and retailers are selling my personal information and exactly what I purchase to large scale marketing firms and data aggregators, they are aggregating the data that they get from other sources such as credit card companies, which are freely allowed to sell and use every purchase you make with your credit card; financing companies; banking and loan information; retail gasoline purchases; publicly available information, including home assessment, car loans and assessments, information from social media sites such as LinkedIn and Facebook, education, age and gender; and are profiling me and you and predicting many things about us.

What does profiling and predictive modeling mean? When data aggregators get all of the data from the sources mentioned above, they are easily able to match it to an individual (including you and me) and they are able to use technology to determine and predict a person's income, age, date of birth, address, how many homes are owned and how much money is owed on each home, how many cars are in the garage and outstanding loans on the cars, how many children they have and who those children are, what schools they go to, what grade appliances are in the kitchen, where they work, what they do for work, where they travel, when they are home and when they aren't, habits and hobbies, whether they smoke and/or drink and what brands they like, whether they engage in risky behavior such as owning a motorcycle or a sports car, like Nascar, football or beauty pageants, whether they filed for bankruptcy, what bars they go to, where they have dinner and how often, whether they are pregnant or not, whether they have a sexually transmitted disease, HIV/Aids or cancer. All under the guise of being able to market appropriate products and services to the individual.

Think about how much information one can get just from your credit card, pharmacy, supermarket and gas fill-ups. Last year, I spoke at a conference with a member of the FTC's consumer protection unit. We talked a lot about predictive modeling, and this was her take away—she had done some research on how predictive modeling had made assumptions about her which included the fact that she owned cats, owned a motorcycle, was in her 50's and was married. She laughed and said that she likes cats, but doesn't own one, never had even been on a motorcycle, was in her 30's and was single. How wrong could they be? The significance to her was that predictive modeling is being used to make assumptions and decisions about consumers, and those assumptions and decisions can be totally wrong. Wrong predictions can have real life consequences. The FTC is concerned that employers, banks, financing

companies, insurers and others are and will make decisions about consumers based on predictive modeling to determine whether or not they are insurable (if one smokes, drinks and owns a motorcycle, or has cancer, is this person insurable and how much will the premium be?); employable (do we really want to hire an employee that is pregnant, has a sexually transmitted disease or cancer that will put our health plan over the top or is going to take a lot of smoking breaks?), or is creditworthy.

So again, whether you use your rewards cards or not is up to you. Just be aware of the information that you are providing, what is being done with your information, how it is being used and may be making erroneous assumptions and predictions about you, and make an educated choice.

*— Linn Foster Freedman*

---

For more thoughtful and timely discussions of legal news and perspectives on issues relating to data privacy and security, subscribe to our *Data Privacy + Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy + Security Team.

---

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

---