Robinson+Cole

Data Privacy + Security

June 25, 2015

Data Privacy + Security Insider Update

CYBERSECURITY

Connecticut Governor Signs Cybersecurity Study Act

Yesterday (6/24/15), Connecticut Governor Dannel Malloy signed Special Act No. 15-13, effective immediately, which requires the Connecticut Department of Administrative Services, in consultation with the Department of Emergency Services and Public Protection, to conduct a study "to identify cybersecurity issues facing the state and to make recommendations regarding specific actions the state can implement to promote and coordinate communication between government entities, law enforcement, institutions of higher education, the private sector and the public to improve cybersecurity preparedness."

The Act requires the Department of Administrative Services to submit the results of the study and the recommendations to the joint standing committee of the Connecticut General Assembly no later than January 1, 2017.

No doubt a reaction to the massive Office of Personnel Management data breach, it is good to see state governments putting cybersecurity high on the priority list.

We are anxiously awaiting the Governor's signature on Connecticut's amended data breach law (Substitute Senate Bill 949), and we will provide you with the details of that amendment as soon as it is signed.

–Linn Foster Freedman

Cardinals Hacking Update

St. Louis Cardinals owner Bill DeWitt, Jr. threw staff members under the bus following the breaking story last week that the Cardinals have been hacking into the Astros' database for up to three years. According to DeWitt, a small number of Cardinals employees were behind the intrusions into the Astros database, conduct which he called "roguish behavior." He confirmed that those staff members would be held accountable for their actions. The FBI and Department of Justice are investigating the incident, and in addition to any discipline and/or termination that DeWitt may hand down, the actions of the staff members could result in criminal charges. As we have said before, it is always better to keep your day job than to

succumb to the temptation to steal or use others' data.

Reports since the story broke indicate that the first intrusions occurred as early as 2012. This is the first known case of a sports team attempting to obtain another team's data, and is a reminder that data is valuable in any context and no business is immune from theft of its intellectual property and trade secrets and valuable business information, which could have a substantial impact on the bottom line.

–Linn Foster Freedman

ENFORCEMENT + LITIGATION

Supreme Court Declares Warrantless Searches of Hotel Registries Unconstitutional

A 116-year-old Los Angeles city ordinance that allowed police to make unannounced inspections of hotel guest registries at any time without a warrant or subpoena has been ruled as an unconstitutional violation of privacy by the United States Supreme Court.

The ordinance required Los Angeles hotel owners and operators to keep on record for 90 days guests' names, addresses, vehicles, and other information, and to offer the data to law enforcement on demand without a warrant. Hotel owners sued the city of Los Angeles over the law in 2003, claiming it violated their Fourth Amendment privacy rights.

The city argued that the ordinance is minimally intrusive and is a valuable deterrent against hotels that allow criminals to rent hotel rooms without taking down their information.

In a 5-4 decision in the case of *City of Los Angeles v. Patel*, the Supreme Court found that the ordinance was facially unconstitutional because it did not provide for judicial review of the reasonableness of an officer's demand to search the registry before issuing penalties for noncompliance.

The recent decision does not require warrants or subpoenas for every hotel registry inspection. Rather, it orders that these measures be in place for when they are needed, giving hotel owners the opportunity to challenge warrantless searches without facing jail time or fines.

The holding constitutes a small and very narrow victory for the Fourth Amendment rights of Los Angeles hotel owners. The decision pertains solely to the Los Angeles ordinance and does not address the constitutionality of other, similar records sweeps allowed under the Third Party Doctrine. Nor does it address the Fourth Amendment implications of the "pervasive regulation" of certain businesses—like the records legally required to be kept and provided to officers on demand by businesses like firearms dealers, pawn shops, and junkyards.

–Kelly M. Frye

DATA BREACH

Security Bug Found In Samsung® Smartphones

Samsung recently announced that more than 600 million Samsung mobile devices contained a factory installed third party software produced by SwiftKey that predicts the words you will type on your keyboards. The issue with the SwiftKey software is it contains a flaw that permits hackers to access the

device when the Keychain software is applying a software update. While the flaw provides just a narrow window to access the device, if the hacker is successful, they will have access to the device's GPS, camera and microphone, to secretly install malicious apps, to eavesdrop on inbound and outbound messages or voice calls, or access pictures and text messages. Because of the way SwiftKey is installed, the software comes with the device and cannot be deactivated or uninstalled.

This flaw was discovered by NowSecure in November. NowSecure told Samsung, and only now is the news becoming public. Samsung is working on a solution.

–Kathleen A. Porter

Password Management Company LastPass Discloses Security Breach

We know it's hard to keep track of passwords. A good security practice is to use different and complex passwords across different platforms, but it is so hard to keep track of all of them. That's why password management products have entered the marketplace—to help us manage our passwords. But what happens when the password management system gets hacked?

On June 15, 2015, LastPass, a company offering a product for customers to centrally manage their passwords with a single password, disclosed on its blog that intruders had broken into its system and absconded with users' email addresses, password reminders, server per user salts and authentication hashes. According to LastPass, it "quickly detected, contained, evaluated the scope of the incident, and secured all user accounts."

LastPass posted FAQs on its website on June 16th in response to a flurry of questions. The first FAQ "Was my master password exposed?" was answered with a firm "No." LastPass explained that LastPass never has access to a customer's master password, and therefore, the hackers did not get access to it either. LastPass uses encryption and hashing algorithms for both the username and master password. Further, LastPass confirmed that the encrypted user vaults were not compromised, so no data stored in customers' vaults were at risk. Nonetheless, LastPass is requiring that customers change their master password, and further recommending that it be changed if it has been used for any other website.

The lesson here is that even companies with the most sophisticated security measures are vulnerable to attack and compromise. So if you aren't the most sophisticated company, and you haven't suffered a security compromise, you either don't know that it has already happened or it will. If implementing privacy and security measures are not at the top of your priority list, you might consider placing them there now. Take a look at the next article, written by team member Jim Merrifield, on information governance—hopefully it will help get you started.

–Linn Foster Freedman

INFORMATION GOVERNANCE

Data Breach: How Information Governance Reduces Risk

With all the data breach activity over the past several years, any organization or individual that hasn't been affected in some way almost feels left out. According to the Department of Health and Human Services, the data of 120 million people has been compromised in more than 1,100 separate breaches at organizations handling PHI (protected health information) since 2009. That number is almost a third of the U.S. population! Now is the time for organizations to take action! The data breach problem

is very real and is going to get worse before it gets better.

Most organizations' immediate reaction to such activity is to invest in some new type of data security technology or purchase a higher level of cyber insurance coverage. However, they should also be equally concerned with ensuring proper governance of their information. More often than not, the information compromised during such an activity shouldn't have been stored there in the first place and having an information governance program in place can reduce those risks.

For instance, an information governance program addresses the following items:

1. Identify which stakeholders in the organization have access to sensitive information (PII and PHI)
2. Document the storage locations (repositories, servers, applications ,etc.) where sensitive information is stored
3. Explain how long sensitive information is stored in both public and local environments
4. Outline data storage requirements and guidelines for third-party vendor compliance
5. Dispose of ROT (redundant, outdated, trivial) data to reduce discovery costs

No doubt, it's crystal clear that information governance can reduce an organization's risk in connection with a data breach. Of course, there are many other items that would fall under the information governance umbrella, but these surely provide a starting point. As with any endeavor, getting started is usually the hardest part.

Do you need help getting started with your information governance journey? If you would like to discuss information governance, please contact any of the Data Privacy + Security Team members here at R+C.

–Jim Merrifield

TELEPHONE CONSUMER PROTECTION ACT

FCC Adopts Declaratory Ruling on TCPA Regulations to Loosen Restrictions on Some Types of Robocalls

On June 18, 2015, the Federal Communications Commission (FCC) adopted a set of declaratory rulings related to robocalls and spam text messages under the Telephone Consumer Protection Act (TCPA). Specifically, the rulings provide the following:

- Robocall blocking can now be offered to consumers by telephone service providers.
- Consumers' can now revoke their consent to receive autodialed telephone calls and text messages in any reasonable way at any time. This will make it even more difficult for businesses to track consumer consent.
- Businesses must stop calling reassigned wireless telephone numbers after one single call.
- The definition of "automatic telephone dialing system" includes machines with a future capacity to dial randomly, sequentially and even from a list loaded into a dialer. But human intervention,

is NOT sufficient to overcome automatic telephone dialing system status under TCPA regulations.

- Consumer consent passes from a land line to a wireless telephone number if the consumer ports his or her telephone number from the original land line to a wireless device.

- Telephone calls and text messages can be sent to consumers for "urgent circumstances" such as to alert a consumer of potential fraud (e.g. from a bank or other financial institution), or to remind the consumer of an urgent medication refill (e.g. from a health care provider or pharmaceutical company).

Additionally, the rulings reaffirm that text messages are in fact considered "calls" under the TCPA regulations, the called party must provide consent not the intended recipient, autodialed or prerecorded telephone calls or text messages to mobile devices still require prior express consent, and consumers still have a private right of action in addition to statutory fines and penalties.

While FCC Chairman, Tom Wheeler, said that "legitimate businesses seeking to provide legitimate information will not have difficulties," not everyone agrees with these rulings. FCC Commissioner, Jessica Rosenworcel, said in her dissenting opinion, "Consumers have made clear–abundantly clear–they want fewer robocalls. So I do not understand why for some sectors of the economy [the FCC] gives the green light for more robocalls when consumers want a red one."

–Kathryn M. Sylvia

HIPAA

Two House Bills Seek to Address Sharing of Mental Health Information Under HIPAA

The Health Subcommittee of the U.S. House Energy and Commerce Committee held a hearing last week to consider two bills addressing current limits on the sharing of mental health information under HIPAA. The first bill, the Helping Families in Mental Health Crisis Act of 2015 (H.R. 2646), was introduced by Representative Tim Murphy. H.R. 2646 seeks to expand the circumstances under which protected information about a patient with a serious mental illness can be shared with family members and caregivers. Under the bill, a physician would be permitted to share diagnoses, treatment plans, medications and other protected health information with a family member or a caregiver of a patient with a serious mental illness if certain conditions are met, including that the disclosure be necessary for the continuing treatment of the individual and necessary to protect the health, safety or welfare of the individual or the general public. The bill also seeks to expand the ability to share mental health-related information of students under FERPA and proposes several other mental health care-related reforms. A previous version of the bill was introduced by Representative Murphy after the mass shooting in Newtown, Connecticut.

The second bill, the Including Families in Mental Health Recovery Act of 2015 (H.R. 2690), was introduced by Representative Doris Matsui. H.R. 2690 seeks to formalize guidance issued in 2014 by the Department of Health and Human Services Office of Civil Rights (OCR) on sharing protected health information of patients being treated for a mental health condition. That guidance, presented in question-and-answer format, addresses frequently asked questions regarding HIPAA restrictions on sharing mental health information with a patient's family members and caregivers, and with law enforcement. Currently, the guidance does not have the force of law but provides insight on how OCR reviews matters involving the disclosure of mental health information. We will follow the journey of these two bills and keep you updated.

–Pamela H. Del Negro

DATA PRIVACY

Privacy and Transparency in the Context of Government Data Requests

The Electronic Frontier Foundation (EFF) recently released its fifth annual report evaluating the practices of several online service providers with regard to government access to user data. The report rates the major online providers on a five star scale measuring their efforts to promote transparency and protect user privacy in the face of government data requests. While the media has largely focused on the identities of the highest and lowest scorers, it is useful to take a step back and review the five questions that form the basis of these ratings:

1. Does the company meet industry-accepted best practices, including requiring the government to obtain a warrant prior to disclosing user data, publishing regular reports on government requests and enacting company guidelines for responding to government data requests?

2. Does the company give users prior notice of government data requests so that users have an opportunity to challenge the request by appropriate legal means?

3. Does the company publicly disclose its data retention policies for IP address logs, deleted content, and similar types of inaccessible data?

4. Does the company publish regular transparency reports detailing requests the company has received from the government to hand over user data, remove user content or suspend user accounts and how the company has responded to such requests?

5. Has the company taken a pro-user stand on a privacy issue in some public forum such as a blog post, coalition letter or other public written format, namely the issue of government-mandated back doors?

While these questions are oriented towards the privacy challenges faced by large online service providers maintaining troves of user information, they provide insight into the evolving privacy expectations of internet users. Any business that has an online presence and either actively or passively collects user data would be well served to test its own privacy practices against these standards. As businesses try to position themselves for growth, they must be prepared to meet the privacy challenges inherent in the accumulation of user data.

–Christopher J. Librandi

SOCIAL MEDIA

New York State Bar Association Issues Updated Opinion on Lawyers' Social Media Use

The New York State Bar Association (NYSBA) issued a new opinion on lawyers' use of social media last week to "assist lawyers in understanding the ethical challenges of social media." The opinion provides new insight on the following:

- The extent to which lawyers' 'hybrid' social media accounts are subject to ethical rules on advertising and solicitation;
- The types of situations where lawyers are permitted to preserve social media messages used to communicate with their clients;
- Whether it is a violation of lawyers' ethical obligations to access a juror's public profiles on social media that notify the individual when their social media account has been accessed; and
- The responsibility of lawyers to notify the judiciary of suspected juror misconduct discovered through social media accounts.

Additionally, the new opinion includes two new guidelines:

Guideline No. 1: A lawyer has a duty to understand the benefits and risks and ethical implications associated with social media, including its use as a mode of communication, an advertising tool, and a means to research and investigate matters.

Guideline No. 7: A lawyer shall not communicate with a judicial officer over social media if the lawyer intends to influence the judicial officer in the performance of his or her official duties.

Guideline No. 2 was revised to clarify that "hybrid" social media accounts "used for business and personal purposes" are also subject to ethical rules related to advertising and solicitation. That means that Rule 7.1(d) applies to these hybrid social media accounts, including a lawyers' 'tweets' and Guideline No. 2 notes that it "may be impractical or not possible" to use a disclaimer on a tweet (since the tweet is limited to 140 characters) but these types of "structural limitation[s] [do] not provide justification for not complying" with ethical rules. With the use of social media embedded in our society, more and more concerns may arise when it comes to legal ethics and the interaction with clients, jurors, witnesses and other attorneys.

–Kathryn M. Sylvia

To get more thoughtful and timely discussions of legal news and perspectives on various 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.
