Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

January 14, 2016

ENFORCEMENT + LITIGATION

Former Cardinals Scouting Director Pleads Guilty to Hacking the Astros' Database

Last Friday, Chris Correa, the former scouting director of the St. Louis Cardinals, pleaded guilty in federal court in Texas for unlawfully accessing the Houston Astros' database, which included scouting and draft information.

Correa pleaded guilty to five counts of unauthorized access of a protected computer because he admitted that he accessed the database five times between 2013 and 2014. He faces up to five years in prison for each charge and will be sentenced on April 11th. Prosecutors have reportedly already agreed to allow him to serve counts consecutively.

Correa admitted to using the passwords of former Cardinals employees who had moved to the Astros to access the scouting database, dubbed "Ground Control." The database included contract information, scouting reports, and other proprietary information about the players. He allegedly viewed 118 pages of information, including details about trades, draft rankings, and draft strategy. He accepted responsibility and admitted that he "trespassed repeatedly." He called his behavior "stupid."

The Astros allege that the hacking cost it $1.7 million. The hacking was first reported in June of 2014 when it was discovered that some of the material was posted online.

Correa was fired by the Cardinals, and the case is the first-known case of sports espionage. Cub fans have been quick to point out that the Cardinals completed the 2015 season with the best record in MLB.

— Linn Foster Freedman

Shutterfly Biometrics Case Proceeds in Illinois

In what is being described as the first case in the U.S. regarding a state biometric privacy statute, a proposed class was successful in thwarting a motion to dismiss by Shutterfly last week over its alleged practice of collecting and storing face geometry from photos without individuals' authorization. The plaintiff alleges that Shutterfly is using his face pattern to identify him in photographs posted on various websites and that this violates the Illinois Biometric Information Privacy Act.

The Judge found that the plaintiff had "plausibly stated a claim under" the Illinois Biometric Information Privacy Act.

Three states to date have biometric information privacy statutes—Illinois, New Hampshire, and Texas. As we have seen with other privacy issues, no doubt additional states will implement similar statutes in the future.

Facebook is facing a similar proposed class action case in federal court in Chicago over its use of biometric identification technology. We will be watching that case closely, as well as any other developments in this area.

— Linn Foster Freedman

Uber Settles with New York Attorney General over "God View" Tracking of Riders

Attorney General Eric Schneiderman announced last week that his office has settled its investigation of Uber Technologies, Inc. (Uber) over allegations that Uber executives could access an aerial view of riders' locations, dubbed "God View." Readers may recall that Uber was in the news when a reporter found out that executives were allegedly targeting his whereabouts, and there is speculation that this spurred the investigation.

Uber agreed in the settlement to adopt data security protection practices and to encrypt all riders' GPS information. Further, Uber will adopt authentication protections before an employee can access riders' sensitive personal information.

Uber will also pay the AG $20,000 for failure to provide timely notice to drivers and the AG following a September 2014 data breach that exposed Uber employees' personal information.

In his press release, the AG stated, "This settlement protects the personal information of Uber riders from potential abuse by company executives and staff, including the real-time locations of riders in an Uber vehicle."

— Linn Foster Freedman

Data Breach Class Action Dismissed against SuperValu for Lack of Standing

Last week, a Minnesota court ruled that a consolidated class action filed against the SuperValu retail chain failed to assert any harm, finding that while SuperValu did suffer two data breaches, the class's claims of possible future injuries were too speculative, and the class therefore lacked standing to sue. The data breaches occurred in 2014 at over 1,000 retail stores. The only "harm" alleged by any of the class members was a single unauthorized credit card charge. However, the court said in its decision, with the frequency of credit card fraud, this one unauthorized charge is not fairly traceable to the SuperValu breaches. U.S. District Judge Ann D. Montgomery said, "This speculation prevents the court from finding an increased risk of fraud and identity theft is 'certainly impending' or that there is a 'substantial risk' the harm will occur." The class attempted to argue that its case was similar to that of Target; however, the court concluded that cases like Target alleged factual evidence of actual data misuse to suggest that hackers were actually using customer data for fraudulent activities. Judge Montgomery said, "Here, the singular incident from one named plaintiff over the course of more than a year following the data breach is not sufficient to 'nudge' plaintiffs' class claims of data misuse or imminent misuse across the line from conceivable to plausible." The court also ruled that the class members could not inflict harm on themselves by paying for credit monitoring and other similar services—fear of future harm will still not satisfy the elements of standing. However, Judge Montgomery did rule "without prejudice" which could

leave room for the class to file an amended complaint.

— Kathryn M. Rattigan

Volkswagen Refuses to Share Emails with U.S. Investigators Citing Privacy Concerns

German auto manufacturer Volkswagen (VW) is reportedly using German privacy laws to resist turning over its top executives' internal corporate emails and other communication materials to United States attorneys general and United States Justice Department officials investigating the company's excess emissions scandal.

VW's position is not surprising. It is well known that Germany's data privacy laws are among the world's most protective, particularly when it comes to any government's collection and use of an individual's personal information, which would include information in corporate emails. Germany had a particularly strong reaction to Edward Snowden's revelations that U.S. Internet and telecommunications companies were allowing the U.S. National Security Agency "back door" access to phones, data, and online communications of consumers and government officials, including allegedly, the German Chancellor. The reaction included requiring cloud providers doing business with German governmental agencies to basically agree to keep any cloud data from these agencies in Germany to avoid the potential that government data stored in the cloud could be accessed or shared outside of Germany in a country with less robust data privacy protections.

However, these VW executives' communications are likely very significant to the U.S. investigation. The communications being requested are from many of the same executives who for months failed to take U.S. regulators' inquiries about VW emissions levels seriously. These internal communications might reveal whether the executives were intentionally misleading regulators or if they were truly in the dark about the problems. Additionally, these are the same VW executives who have publicly promised transparency on the emission investigation, and so their failure to permit VW to share their email and communications with U.S. investigators seems suspicious, as German privacy laws would likely permit email and communications to be disclosed if the individuals involved consented.

The data privacy concerns raised by VW are focused on the U.S. investigators who are taking a much stronger position against VW than Germany. We know German regulators investigating the same activities were given access to VW's headquarters. We also know VW cooperated with German regulators. The result of this was German regulators approving a modest, simple correction to resolve the emissions problem for most of the 11 million cars sold in the European Union.

Courts in the U.S. have previously favored law enforcement needs over data privacy laws. For example, a major Swiss bank was forced to disclose the personal information of its American customers. Therefore, many believe the U.S. investigators will eventually succeed in getting these internal communications from VW, notwithstanding data privacy concerns.

— Kathleen M. Porter

Michaels Stores Class Action Data Breach Case Dismissed

Michaels Stores, Inc., was dismissed from a putative data breach class action case involving the breach of 2.6 million payment cards, as the plaintiffs were unable to show that they were injured as a result of the incident.

The case follows a long list of cases that hold that plaintiffs in data breach cases do not have standing to sue under Article III unless they can show “certainly impending” harm or that “a substantial risk that harm will occur” from the incident. In this case, the judge noted that the plaintiffs could not show that they had any out-of-pocket losses.

The case was pending in the U.S. District Court for the Eastern District of New York and was dismissed without prejudice. This case adds to and bolsters a consistent approach to these cases by the judiciary that will hopefully continue throughout 2016.

— Linn Foster Freedman

FCC Clarifies TCPA Liability for Texting

The Federal Communications Commission (FCC), in a denial of a petition from a company that provides bulk marketing texts for other companies, clarified that it will maintain separate standards for fax and text messaging senders when looking to investigate and enforce violations of the Telephone Consumer Protection Act (TCPA). In essence, the FCC stated that the TCPA standards are sufficient to protect texters that may be accused of robocalling.

A text marketing broker asked the FCC to declare that it was not the “sender” of the text if it was merely acting as a neutral conduit. The FCC responded by stating that it depends on the circumstances, and the FCC will look at each case on a case-by-case basis, and that it will look “at the totality of circumstances” to determine whether the sender of a text is liable under the TCPA.

Short message? The TCPA continues to be a high-risk area that companies may wish to follow closely, particularly in the marketing arena.

— Linn Foster Freedman

EU PRIVACY

European Union’s New General Data Protection Regulation

Big changes are underway in the world of data protection within the European Union. At the end of December, the European Commission approved the final version of the General Data Protection Regulation (GDPR).

The GDPR will have a significant and wide-ranging impact on businesses, imposing new compliance obligations and threatening significant sanctions for non-compliance. According to experts, the new rules will impact every entity that holds or uses European personal data both inside and outside of Europe.

This is the first overhaul of the regulations since 1995 that, as one might guess, were quite outdated, given the technological advances over the last two decades. The regulations will affect all 28 European Union member states and will replace inconsistent laws that the European Union member states had previously implemented to comply with the 1995 directive.

The GDPR sets out the rights of individuals, giving them more control over their personal data. It requires companies to inform individuals in unambiguous terms that their information will be processed and/or collected and state the specific purpose for such processing and/or collection. If the information will be

used for multiple purposes, the individual must be informed of each and every purpose. Consent can no longer be implied; rather, it must be explicitly given. The company's request for consent must be clear and concise and may not be presented in an unusual context. Further, companies will be required to delete data if an individual revokes his or her consent.

The GDPR also sets out general obligations for companies that are responsible for processing data. These include the obligation to implement appropriate security measures based on the risk involved in the data processing operations the company performs. Companies will also be required to notify individuals within 72 hours of a data breach involving data that was not encrypted. Further, larger companies or companies that handle significant amounts of sensitive data will be required to appoint a data protection officer whose role will be to ensure, on an independent basis, that the provisions of the GDPR are being followed within the company.

Another key component of the GDPR is that it not only gives rise to increased compliance requirements but also provides for significant financial penalties for non-compliance. Specifically, the GDPR provides for administrative fines of up to €20 million or 4 percent of a company's global revenue, whichever is greater.

The GDPR is expected to become law in 2018, meaning that there is no time to waste for companies to assess the new regulations and to put the proper measures in place to ensure compliance.

— Kelly Frye Barnett

CYBERSECURITY

BIMCO Issues Cybersecurity Guidelines for Ships

Last week, BIMCO, along with other shipping organizations, "launched" guidelines "to help the global shipping industry prevent major safety, environmental and commercial issues that could result from a cyber incident onboard a ship."

BIMCO states that the guidelines are "a first for the shipping industry" (which to our knowledge is true and we applaud).

The guidelines are designed to identify cyber risks on ships and to assist the shipping industry with information in order to protect against attacks and deal with cyber incidents. They discuss understanding the cyber threat to ships, how to assess the risk and determine vulnerabilities, controls to put in place to minimize the risks, and how to develop contingency plans. They reference the NIST framework.

The G*uidelines on Cyber Security Onboard Ships* are free and can be downloaded from the BIMCO website.

— Linn Foster Freedman

Leadership Team Appointed for Cyber Threat Intelligence Integration Center

On January 7, 2016, Director of National Intelligence James Clapper announced the appointment of the leadership team that will head the new Cyber Threat Intelligence Integration Center (Center), which was announced by President Obama a year ago.

The Center will be led by Director Tonya Ugoretz from the FBI (who has also worked with the CIA, Department of Homeland Security, and National Intelligence Council), who will be supported by Deputy Director Maurice Bland, who worked at the NSA, and Research Director Thomas Donahue, a veteran of the Senior Intelligence Service at the CIA. Sounds like quite the team.

The Center is designed to be a central clearinghouse for cyber threat information for the intelligence community, including integrating intelligence on foreign cyber threat capabilities and activities and sharing the most up-to-date information with bureaus and departments in the federal government, including law enforcement.

That team has its work cut out for them but is clearly up to the task.

— Linn Foster Freedman

DRONES

Aerial Trespass, Privacy Violations, and the Drone Slayer

John David Boggs's drone was shot down out of the sky last summer when he flew it over another individual's home. Boggs's claims that he was flying his drone over Class G airspace—federally protected airspace. Bogg's claims that he was not trespassing or invading anyone's privacy when William H. Merideth (who coined himself the "drone slayer") shot down the drone.

Merideth doesn't think he did anything wrong, and he makes that clear on his Facebook page, boldly stating, "Not only did I do it, but I meant to do it. And I'd do it again." He even started selling shirts that say "Team Willie" and "#DroneSlayer" depicting a drone with the statement "We the people…have had enough!" Merideth was charged by Kentucky law enforcement for felony endangerment and criminal mischief, but the court dismissed those charges finding that he "had a right to shoot" the drone.

However, in Boggs's complaint filed this week with the Kentucky District Court he says, "The tension between private property rights and right to traverse safely the national airspace was resolved during the formative days of manned aviation. The issue is now arising in the context of unmanned aircraft, also known as drones. Plaintiff seeks a declaratory judgement from this court to resolve that tension and define clearly the rights of aircraft operators and property owners." He asked the court to make the legal determination that his drone flight did not constitute trespassing and to award him damages of $1,500 for his drone.

The courts have never addressed this issue of drone flights over private property and whether this flight would constitute trespassing. However, we will watch the outcome of this case, which will mark the first decision of its kind. This is likely just the beginning of lawsuits related to drones flying over private property and homes. Who owns that airspace? Well, maybe this case will tell.

— Kathryn M. Rattigan

DATA PRIVACY

FTC Issues Big Data Report and Warning

Data analytics are getting more sophisticated and are being used in every industry. The more data in the world, the more it can be analyzed—it's dubbed "big data." In that context, the Federal Trade Commission (FTC) recently issued a report (Big Data: A Tool for Inclusion or Exclusion) on big data and outlined the benefits and risks associated with using big data to discriminate against individuals. In particular, the FTC wants companies to address whether or not there is an inherent bias in its big data analytics.

The FTC cautioned businesses not to use big data to unfairly treat or exclude lower-income individuals or other underserved people, such as using the data to refuse to extend credit or through unfair employment practices. The report noted that information such as zip codes, social media, or shopping history, if inaccurate or biased, can have an adverse effect on certain communities or ethnicities that are more vulnerable than others. Further, this information can be used to determine whether credit will be extended, which may unfairly or inaccurately portray certain credit risks.

The warning is that these practices can violate consumer protection laws, and the FTC has made it abundantly clear that it is going to step up its consumer protection enforcement in the coming year.

— Linn Foster Freedman

Privacy Day!

In the United States, Canada, and 27 European countries, January 28 of each year is known as Data Privacy Day. Started in Europe as "Data Protection Day" to recognize the January 28, 1981, signing of Europe's first legally binding international treaty dealing with privacy and data protection, known as Convention 108, Data Privacy Day was first celebrated in Canada and the U.S. in 2008.

In the U.S., Data Privacy Day is organized and promoted by the nonprofit The National Cyber Security Alliance (NCSA). NCSA seeks to raise awareness in the workplace, in schools, and at home about data privacy and the protection of personal information online and offline.

NCSA has a handy guide to educate you about the personal information you are sharing and storing on e-commerce sites, social media, web browsers, and search engines and on your smart phones and other mobile devices. The guide explains how to look at your current privacy settings online and on your devices, and if you wish, how to make changes to those settings to better protect your personal information.

As part of our ongoing representation of clients on privacy related matters, we conduct training programs and seminars on collecting, using, safeguarding, and sharing information. Please contact us if your business is interested in learning more about these training programs and seminars.

See our blog this month and https://www.staysafeonline.org/data-privacy-day/ for more details on getting involved in National Privacy Day, and as always, be #PrivacyAware.

— Kathleen M. Porter

INTERNET OF THINGS

Hello Barbie May Not Be as Smart as We Thought

We wrote previously about the "Hell No Barbie Campaign" and the recent lawsuit against Mattel for its Hello

Barbie doll privacy violations, but through all this hype, we have yet to learn exactly what Hello Barbie is truly capable of.

In a new report, Hello Barbie isn't so bright. First, in order for Hello Barbie to "hear" what you are saying, you must press a button on her belt. That activities the voice recognition software. Second, while original reports claimed that Hello Barbie could have intelligent conversations, she is "far dumber and more limited than [she] is represented to be," said Future of Privacy Forum representative, Jules Polonetsky. While Hello Barbie is pre-packaged with over 8,000 lines of dialogue, she is not programmed to answer questions beyond a specific topic and will redirect the conversation back to her prescribed responses. So maybe Hello Barbie's ability to record all of our conversations and have deep, personal conversations with our children is a bit more limited than we originally were told.

However, there are still some concerns with the recording of children's conversations and storing them in a cloud database accessible to hackers. And parents who have signed up for a ToyTalk Hello Barbie account will get regular email messages encouraging them to listen to their children's conversations and share them with family and friends easily through social media buttons. When did the ability for children to just play disappear?

The broader question at hand with a toy like this is the future of these types of devices. As these devices "get smarter," we need to be ready with appropriate policies, practices, and regulations to protect children and adults from the overt collection of personal data and potential privacy violations.

— Kathryn M. Rattigan

HEALTH INFORMATION PRIVACY

HHS Issues New Guidance on Individual Access to PHI under HIPAA

On January 7, 2015, HHS issued new guidance (Guidance) regarding an individual's right to access his or her health information under HIPAA's Privacy Rule. The Guidance emphasizes that HIPAA, while protecting the privacy and confidentiality of individuals' health information, also recognizes the importance of providing individuals with access to their health information.

The Guidance reviews the applicable provisions of the Privacy Rule that establish an individual's general right to access protected health information (PHI) maintained about the individual by or for a covered entity in a designated record set (found at 45 C.F.R. §164.524). The Guidance notes in part that:

- Individuals may be required (at the covered entity's option) to make a written or electronic request for access to PHI;
- Covered entities must take reasonable steps to verify the identity of an individual making a request for access to PHI;
- Access to PHI must be provided in the form and format requested (i.e., paper or electronic), if readily producible in that form and format, or, if not, in a readable hard copy form or other form and format as agreed to by the covered entity and individual;
- Access must be provided within 30 calendar days of an individual's request (which time period may be extended once by 30 days upon notification to the individual);
- Access may only be denied in limited circumstances set forth by the Privacy Rule, certain of which are subject to review;
- An individual may also direct a covered entity to transmit PHI about the individual directly to another person or entity; and
- A covered entity may impose a reasonable, cost-based fee, for providing a copy of PHI or a summary or explanation of such information, provided that such fee may only include the cost of labor for copying the PHI, supplies for creating a paper copy or electronic media, postage, and

the preparation of an explanation or summary (other costs permitted under state law *may not be included*).

The Guidance is accompanied by FAQs regarding the scope of information covered by an individual's right of access, the type of records or other information covered, and the circumstances under which a covered entity may deny an individual's request for access to PHI.

In a press release accompanying the release of the Guidance, Jocelyn Samuels, director of the Office for Civil Rights (OCR), indicated that the Guidance is intended to remove barriers for individuals access their health information. The Guidance appears to be one piece of a broader HHS initiative intended to ensure that individuals understand and are able to exercise their rights under HIPAA. HIPAA-covered entities and individuals will therefore want to continue monitoring HHS and OCR for the release of additional guidance and related tools concerning HIPAA and health information privacy.

— Conor O. Duffy

EMPLOYEE PRIVACY

NLRB Rules Employees Can Record Conversations at Work

Next time your boss is breaking a labor law, remember that the National Labor Relations Board (NLRB) has ruled that Whole Foods cannot prohibit its employees from recording conversations and taking photos or video at work. The caveat—beyond the NLRB—is that there may be state laws that apply where the consent of the two parties is required for a conversation to be legally recorded.

— Kathryn M. Rattigan

PRIVACY TIP #18

Beware of Phishing Expeditions

So I have been in the data privacy and security world for the past 16 years, and I am still amazed at how savvy hacksters are and how vulnerable we are to their antics. And…how much havoc they can wreak personally and to our employers.

This week's Privacy Tip is about phishing. No, not fishing, and I am an avid bass fisherman, and no, not the band Phish, which has quite a following. Why are we talking about phishing? Because phishing has become a huge issue with individuals and companies and is predicted to get worse.

In the past, we used to get emails telling us "You have won the Nigerian lottery!" and in order to win, we need to click on a link. It wasn't very effective, because the email was full of misspellings and terrible grammar. Really, anyone could figure out it was a hoax, and we all immediately deleted it.

Not so true anymore. Last week, I received an email from "my IT department" indicating that they needed to update my security and to send my password so they could implement the security patch. I didn't recognize the name of the individual and took a casual glance at the url, and it was clearly not my "IT department." I sent it to my "IT department" and confirmed it was a phishing attack. Luckily, I knew enough not to click on it and to send it straight to my internal experts.

Just yesterday, I received a text from the “Apple help desk” indicating that I needed an update and to click on a link to get the update. Well, of course, I knew it wasn’t legit, so I immediately deleted it.

Unfortunately, many individuals and employees don’t realize the havoc clicking on these links can wreak on their personal devices and their employers’ systems. Phishing attacks are now sophisticated and frequent. Be vigilant in analyzing any email or text you get that tries to get your user name or password. Don’t give your password to anyone. Your “IT department" isn’t going to ask for such information in order to provide you with security updates. Neither is Apple.

Many companies are sending out internal phishing expeditions to catch their employees (pun intended.) Don’t get hooked and reeled in. You will be an unwanted catch.

Enough of the puns. Seriously, stay alert. When in doubt, enlist your IT professionals to confirm that an email or text is legitimate or not. No question is a bad one, and they will be so happy when you check before you click. It is way better to be safe than sorry.

— 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

---