Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

January 21, 2016

CYBERSECURITY

DOT and Automakers Agree to Data-Sharing Pact to Encourage Best Cybersecurity Practices

The National Highway Traffic Safety Administration (NHTSA) has entered into a data-sharing agreement with all of the major car manufacturers. The agreement includes the requirement that the manufacturers develop best practices around cybersecurity and encourages them to share information relating to cyber-threats and defenses to cyber intrusions.

The "Proactive Statement of Principles 2016" states that "automakers and NHTSA are reaffirming our resolve to leverage our collective strength and knowledge to work collaboratively, consistent with the law, to further enhance the safety of the traveling public."

The fourth objective of the Principles is "Enhance Automotive Cybersecurity," which is to "explore and employ ways to work collaboratively in order to mitigate those cyber threats that could present unreasonable safety risks." It includes developing suggested best practices learned from within and outside the auto industry concerning cyber threats and remediation, developing ways to engage researchers to assist with cyber threat identification and response, and supporting and enhancing information-sharing by the auto industry's information sharing and analysis center (Auto-ISAC) by voluntarily sharing cybersecurity threat and vulnerability information with members, sharing information about countermeasures used, and expanding the membership in the Auto-ISAC to the supplier community.

Signatories to the agreement include the National Highway Traffic Safety Administration, Honda, BMW, FCA, Ford, GM, Hyundai, Jaguar Land Rover, Kia, Mazda, Mercedes-Benz, Mitsubishi, Nissan, Porsche, Subaru, Tesla, Toyota, Volkswagen, and Volvo.

— Linn Foster Freedman

DHS Official Warns of Increase in Cyber-Attacks of Industrial Control Systems

Marty Edwards, head of the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), recently warned attendees at a conference that ICS-CERT, which assists U.S. businesses in investigating suspected cyber-attacks on industrial control and corporate systems, has seen an increase in attacks to industrial control networks over the past year.

Industrial control networks control operations of industrial processes, such as energy plants, critical

infrastructure, manufacturing processes, and food and beverage processing.

This warning follows a power outage in the Ukraine, which has been blamed on a cyber-attack from Russia, and is the first known cyber-attack causing a power outage. ICS-CERT issued an alert last week indicating that it had identified the malware used in the Ukraine attack as BlackEnergy 3 but did not confirm that it caused the outage.

Edwards noted that the increase in attacks is due to the fact that the control systems are connected to the Internet. Companies with industrial control systems may wish to take note of this warning and assess security controls in place over their networks and systems.

— Linn Foster Freedman

FDA Issues Guidance on Cybersecurity Risk Management for Medical Devices

Last Friday (January 22, 2016), the FDA published draft guidance for medical device makers on the importance of including cybersecurity measures in approved products. Further, the guidance highlights the importance of reporting any post-approval fixes to assist others with cybersecurity measures, particularly for medical devices connected to the Internet.

The guidance, entitled "Postmarket Management of Cybersecurity in Medical Devices," includes how medical device manufacturers should assess security vulnerabilities during development, as well as after market approval of medical devices. The vulnerabilities should be assessed based upon the harm that could occur to patients if there was a security incident. A section on medical device cybersecurity risk management includes assessing exploitability of the cybersecurity vulnerability, assessing the severity of the impact to health, and evaluating the risk to essential clinical performance.

In addition, the guidance discusses what type of information should be included by manufacturers in annual reports to the FDA, including device upgrades as a result of vulnerability assessments, and why the upgrades were made. It also provided explanations of the important elements to be assessed during post-approval product surveillance, including using NIST standards.

Finally, the guidance provides elements that should be included in an "effective postmarket cybersecurity program." All in all, the guidance is consistent with the FDA's previous guidance on cybersecurity for medical devices but provides more details.

Medical device manufacturers may wish to review the draft guidance and give comment. The comment period is open for 90 days.

— Linn Foster Freedman

DATA BREACH

Update on Hyatt Data Breach: Over 250 Locations Compromised

In December, Hyatt Corporation announced that it had identified malware on computers that operate its payment processing systems. Late last week, Hyatt disclosed that upon investigating the malware it discovered "signs of unauthorized access" to customers' payment card data from 250 Hyatt locations in approximately 50 countries, representing approximately 40 percent of Hyatt's hotels. A list of the affected locations and at-risk dates, which range from August 13, 2015, to December 8, 2015, is available here.

The malware, which was aimed at gathering customers' names, card numbers, expiration dates, and verification codes, primarily compromised cards used at Hyatt restaurants, with some other at-risk cards being used at front desks, spas,golf shops and other locations. Hilton Hotels and Starwood Hotels have also experienced payment card breaches. Hyatt is offering affected customers a free, one-year subscription to CSID's protector identity/fraud protection service.

— Pamela H. Del Negro

Tax Season may Bring More Breaches; New Victim, TaxAct

This tax season, the Internal Revenue Service (IRS) has been working closely with big tax preparation vendors and chains to improve the security of online filing this year and safeguard against widespread identity theft. The IRS is now requiring stricter password standards, a new timed lockout feature and limited unsuccessful log-in attempts, along with three security questions. The IRS is also requiring that vendors and chains use "out-of-band verification" for email addresses which include sending an email or a text to the customer with a PIN that they have to enter to process their taxes.

These additional precautions come after a disastrous tax year in 2014 not only for the IRS but for private tax vendors and chains. This week, around 9,000 accounts were frozen by TaxAct, an Illinois tax information software vendor, when it discovered that their accounts were accessed by hackers. TaxAct said, "The attacker did not gain access to income tax returns for the vast majority of suspended accounts." However, TaxAct did sent 450 breach notification letters to its customers informing them of the breach that occurred between November 10, 2015, and December 4, 2015, allowing unauthorized access to their names and Social Security numbers. TaxAct is also offering credit-monitoring services. While this is certainly not a breach affecting a large number of people, it serves as a warning to taxpayers (and vendors alike) that we need to use top-shelf security safeguards to protect our Social Security numbers.

— Kathryn M. Rattigan

ENFORCEMENT + LITIGATION

Supreme Court Opinion in *Campbell-Ewald Co. V. Gomez*: Kicking the Can Down the Road

On January 21, the U.S. Supreme Court decided *Campbell-Ewald Co. v. Gomez*, No. 14-857. The question presented was whether an unaccepted offer of full relief on the named plaintiff's individual claim will render a putative class action moot. The answer is "no," according to a 5-3 opinion by Justice Ginsburg (with a separate concurrence by Justice Thomas). But the Court left open the question of whether, if the defendant had actually deposited the money being offered into court or into a bank account payable to the plaintiff, the case would be moot. That is almost certainly what defendants will now do in some putative class actions. The Court eventually will have to decide that question.

Gomez involved a claim for violation of the federal Telephone Consumer Protection Act. The plaintiff received a single unwanted text message on his cell phone. It probably seems absurd to most nonlawyers that this kind of thing is what leads to Supreme Court cases, but Congress provided for even a single unwanted text message to trigger a potential statutory violation. The plaintiff was theoretically entitled to $1,503 plus costs as the maximum recovery under the statute. The defendant offered (both under Rule 68 and as a freestanding offer) to pay the full amount and consent to an injunction, but the plaintiff did not accept the offer.

Justice Ginsburg's majority opinion adopted Justice Kagan's dissent in *Genesis Healthcare v. Symczyk*,

concluding that "[a]n unaccepted settlement offer—like any unaccepted contract offer—is a legal nullity, with no operative effect." (Slip op. at 7.) That result is unsurprising as a matter of contract law and the plain language of Rule 68, which treats an unaccepted offer as withdrawn. Six of the federal courts of appeals reached the same result after *Genesis Healthcare*.

The majority distinguished other cases in which the defendant had actually paid or deposited the money at issue or entered into a unilateral covenant not to sue to resolve equitable claims. Importantly, Justice Ginsburg's opinion made clear that the result might be different if the defendant in this case had deposited the money being offered:

We need not, and do not, now decide whether the result would be different if a defendant deposits the full amount of the plaintiff's individual claim in an account payable to the plaintiff, and the court then enters judgment for the plaintiff in that amount. That question is appropriately reserved for a case in which it is not hypothetical. (Slip op., at 11-12.)

Chief Justice Roberts wrote a dissent joined by Justices Scalia and Alito. The dissent agreed that an unaccepted settlement offer is a legal nullity as a matter of contract law but viewed the question of whether a "case or controversy" exists under Article III as not controlled by contract law. Chief Justice Roberts reasoned that "[i]f the defendant is willing to give the plaintiff everything he asks for, there is no case or controversy to adjudicate, and the lawsuit is moot." (Roberts, C.J., dissenting, at 9.) Chief Justice Roberts argued that the majority's focus on the fact that the defendant had not yet tendered the money was exalting form over substance. Because the defendant was a multimillion-dollar company, "it would be mere pettifoggery to argue that Campbell might not make good on [its] promise." (*Id.* at 5.) Chief Justice Roberts noted that "[t]he good news is that this case is limited to its facts" because "the majority's analysis may have come out differently if Campbell had deposited the offered funds with the District Court." (*Id.* at 10.)

There were two additional separate opinions. Justice Thomas wrote a concurrence focusing on the historical common law practice with regards to tenders (offers to pay the entire claim), finding that the common law required actual delivery of the money, which was deemed an admission of liability. But Justice Thomas did not reach a conclusion on whether an admission of liability would be required today. Justice Alito wrote a separate dissent, explaining that the "linchpin" for him was the defendant's clear ability to pay the amount offered. Justice Alito would not find mootness where a defendant's ability to pay was not clear. He also suggested that depositing the money with the court or a "trusted intermediary," with delivery of the money to the plaintiff conditioned on dismissal of the case, might be sufficient rather than actual delivery of the money to the plaintiff. That might avoid the prospect of the delivery of money being potentially characterized as a purported admission of liability.

Gomez was not a win for the plaintiffs' bar. Defendants seeking to defeat putative class actions by providing complete relief to named plaintiffs will live to fight another day. Defendants will now ignore Rule 68 and simply tender a check to the plaintiff, or pay money into court or use Justice Alito's tactic of depositing the funds with a "trusted intermediary," contingent on dismissal of the case when the money is transferred. Where the defendant provides complete relief on the plaintiff's individual claim through one of these mechanisms, will that bar the plaintiff from continuing to prosecute a putative class action? There might be a majority of the Supreme Court to support that proposition. But we probably will not know that for a year or two.

— *Wystan M. Ackerman*

Shutterfly and Facebook Fighting Biometrics Suits in Illinois

Friday was a busy day in Illinois with arguments over the Illinois Biometric Information Privacy Act. We previously reported that the first-known biometric case has been given the green light to proceed. The case alleges that Shutterfly violated the Illinois Biometric Information Privacy Act (related post here) by

using facial geometry from photographs that could identify individuals. Last Friday, the plaintiff moved to certify the class of thousands of Illinoisans who used Shutterfly. The allegations in the suit include that Shutterfly stores and uses the facial geometry of individuals in photographs, including nonusers, that can be used to identify the individuals.

Shutterfly notes that the Illinois Biometric Information Privacy Act applies to faces, not photographs. The Judge disagreed, and declared that he interpreted the law to include facial geometry. The plaintiff then moved for class certification.

In another courtroom in Illinois, Facebook argued that the court did not have jurisdiction over a suit against it by an Illinois man alleging that its photo-tagging feature "tag Suggestions" violates the Illinois Biometric Information Privacy Act. The plaintiff, who does not use Facebook, alleges that someone else uploaded a picture of him and tagged him on Facebook, and that Facebook used his facial features in the photo to determine his age, gender, race, and location, violating the Illinois Biometric Information Privacy Act.

Facebook argued that there is no evidence that Facebook deliberately targeted Illinois residents to market the product, which is offered and used worldwide, nor that the person who uploaded this particular picture of the plaintiff lives in Illinois or uploaded the photo in Illinois. Facebook previously pointed out that information derived from photos is specifically excluded by the law.

We will watch these cases closely and keep you up-to-date on developments.

— Linn Foster Freedman

Feds Focus on Damage to Computers as Basis for Computer Fraud and Abuse Act Prosecution

Last week, a federal judge sentenced Yijia Zhang, a computer systems manager, to 31 months in federal prison for transferring thousands of his employer's electronic files to European storage sites. The case highlights the potential power of an overlooked clause of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

The prosecution was under the "Unauthorized Damage to a Protected Computer" clause of the CFAA, which creates criminal liability for "[w]hoever...knowingly causes the transmission of...information...and as a result...*intentionally causes damage without authorization*, to a protected computer." 18 U.S.C. § 1030(a)(5)(A) (emphasis added).

In a press release, the U.S. Attorney's office admitted that it did not have some of the evidence one might expect in a CFAA case. There was "no evidence that the files had been passed to anyone else," no evidence "that any of the information had been used to harm the company," and "no customer information was taken." There was, however, evidence of damage to the company's servers. When Mr. Zhang allegedly deleted files from a server to cover up his transfer, he "caused the server to stop working and its log files to be overwritten."

Charging Mr. Zhang for "Damage to a Protected Computer" is a departure from the more widely used CFAA clauses under which the prosecution must prove the employee "knowingly accessed a computer without authorization" or exceeded "authorized access." 18 U.S.C. § 1030 (a)(1), (a)(2). As we have reported, it has become harder for prosecutors to prevail in such cases when employers give employees access to the data. As those cases get harder to make, you can expect more cases like *U.S v. Zhang*.

— Nuala E. Droney

INTERNET OF THINGS

FTC Warns That Connected Baby Monitors Are More Susceptible to Hackers

At the PrivacyCon event held by the Federal Trade Commission (FTC) last week in Washington, D.C., the FTC warned that several brands of baby monitors lack basic security features like complex passwords and data encryption, making the transmission of data through connected baby monitors more susceptible to hackers. While the FTC did not reveal the brands of baby monitors it tested, Bureau of Consumer Protection attorney Seena Gressin said, “It may be time to update an old lullaby with a new stanza: “Hush little baby, don’t say a word, unless your Wi-Fi baby monitor is well-secured.” The FTC offered tips to consumers (in hopes that baby monitor manufacturers will also heed the warning), such as shopping for monitors with strong security protocols like SSL or TLS encryption, making sure that the security features are actually turned on once you get home with the device, and choosing a strong password for the monitor and the device to which the baby monitor feed is being transmitted.

— Kathryn M. Rattigan

PRIVACY TIP #19

Protecting Seniors from Scams

A surprising number of seniors are embracing digital technology, including computers, tablets, and smartphones. Many use social media and email to stay in touch with friends, children and grandchildren, all of which is good. What is bad is the fact that seniors are being heavily targeted by scammers and fraudsters and are at risk of becoming victims of scams.

These scams include using all sources of communication, including the telephone, and through phishing and texting.

How can we help the seniors in our lives from becoming victims? Educate them just like you educate yourself and your children about safe online behavior, including using appropriate tools, such as firewalls and virus protection, and being suspicious of emails and texts from people they don't know.

Many seniors have been scammed through telephone calls. Suggest to them that they should register their number with the state and federal "Do Not Call" list. It is easy to do. Make sure they never give their personal information and, most importantly, their Social Security number or financial information to anyone over the phone or through an email or text. Tell them not to agree to solicitations for charity or anything else over the telephone or through email or text.

Educate them about phishing and how it works. Encourage them not to fall for phishing emails and texts that ask them to click on a link and not to provide their user name or password to anyone. Encourage them to delete all emails and texts that are from unfamiliar sources.

Grandchildren—help your grandparents with setting up passwords and implementing basic security measures on their phones, tablets, and computers. Help them understand what their privacy settings are and how to implement privacy settings they are comfortable with on their phones and social media accounts. For that matter, help your parents too!

We can all become the victim of a scam. But in general, seniors have less experience with digital media than the younger generations, as they did not grow up with it. Empower the seniors in your life with

knowledge and the tools to embrace digital technology in a safe way, and enjoy the time you spend with them bringing them into your digital world.

— 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

---