Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

June 2, 2016

BIOMETRICS

Proposed Amendment to Illinois Biometrics Privacy Law Introduced Then Stalled

On May 26, 2016, Illinois Senator Terry Link filed a proposed amendment to the Illinois Biometric Information Privacy Act that would presumably ease the rules relating to the collection and use of biometric data. What irked some is that he reportedly tacked it onto a bill that deals with unclaimed property. The next day, Senator Link announced that the amendment was put on hold but did not disclose any reasons why the amendment stalled.

Privacy advocates have stated that the amendment was not given appropriate public debate, and they are concerned that it would relax existing legal protections for biometric data, including exempting facial recognition software from the law.

As we have reported, both Shutterfly and Facebook faced class action litigation in Illinois for alleged violations of the Biometric Information Privacy Act for using facial recognition technology to identify and tag individuals. Shutterfly settled its case, and Facebook was successful in transferring its case to California, where it is still pending. Snapchat was the most recent technology company that uses facial recognition technology to become a defendant in a class action suit in Illinois in the past few weeks.

Senator Link's proposed amendment merely adds the words "physical or digital" to the word "photograph" to make it clear that photographs are not included in the law. This hardly appears to change the intent of the law. The amendment further includes a definition of "scan," which clarifies that a scan included in the law is "an in-person process whereby a part of the body is traversed by a detector or an electronic beam." These changes would in effect confirm that the scanning of a digital photograph of a person's face is not covered by the law. Some would argue that these changes are merely clarifications to the definitions in the existing law and are consistent with the intent of the law. They are clearly in response to the class action cases against Facebook and Shutterfly, which alleged that facial recognition technology was being used to analyze photographs without individuals' consent.

The activity in Illinois around biometrics will no doubt shape legislation and litigation in the other states that already have, or are contemplating biometrics information privacy protection laws. We will be watching this closely.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Fourth Circuit Joins Other Circuits Holding No Warrant is Required For Cell Tower Data

The Fourth Circuit held that the government is not required to obtain a warrant for cell tower data in *United States v. Graham* (4th Cir., No. 12-4659, en banc 5/31/16). The Court found that cell tower data was voluntarily turned over to a third party by the cell phone user. This information was created and maintained by the cell phone companies in the normal course of their business. The information can be used by the government to establish that a defendant was in the vicinity of a certain area when a crime occurred.

The Fourth Circuit joins the Third, Fifth, Sixth and Eleventh Circuits who have already decided this issue. The government is required to apply to the federal court for an order directing the cell phone company to disclose the records. The Stored Communications Act provides a lesser standard than that required for a warrant. The government need only demonstrate "specific and articulable facts showing that there are reasonable grounds to believe that... the records... are relevant and material to an ongoing criminal investigation."

Two dissenting judges argued that cell phone users do not voluntarily turn information over to the cell phone companies merely because they bought a mobile phone, turned it on, and put it in their pocket. Unlike other voluntarily conveyance cases, the dissenters found that cell phone users do not necessarily know that they are communicating this particular information, and they did not act in some way to submit this information to the cell phone companies.

— Kathleen E. Dion

DRONES

Insurance Company Drones May Be Hitting the Skies

Back in March, our *Data Privacy + Security Insider* blog reported an increase in the use of commercial drones by state Departments of Transportation across the country. Now, insurance companies are also getting in the game. Using drones for underwriting, to determine property values and conditions for policy issuance, inspections, and risk evaluations may be more economical, may provide for better response times for inspections of insureds' properties during a catastrophe, and may increase the safety of insurer employees.

So what does this mean for insurance companies? Well, certain provisions of the Federal Aviation Administration (FAA) Modernization Act may be implicated. Insurers may also consider a Section 333 exemption and certificate. Section 333 of the FAA Modernization Act allows the FAA, case-by-case basis, the ability to grant entities the authorization to use certain unmanned aircrafts (i.e., drones) to perform commercial operations prior to the finalization of the Small UAS Rule. To date, the FAA has granted approximately 5,200 exemptions. All of this applies until a final rule for small drone operations is adopted. Right now, the proposed rule is still sitting in limbo—the comment period closed back in April 2015. Insurance companies may need to consider whether the employees who will operate the drones (presumably insurance adjusters) may need to get an airman certificate from the FAA.

Some state, county, and municipal legislatures have passed (or have proposed) ordinances regulating the use of unmanned aircraft systems. Syracuse University's Institute for National Security and Terrorism has a website that reportedly tracks the status of such legislation throughout the nation. Insurers considering the use of drones may need to keep in mind that local rules regarding the use of drones may vary from the federal regulations, and consider whether the federal law preempts state and local regulations. An interesting question also arises with respect to insurers operating under the National Flood Insurance Program and whether they would be subject to state and local regulations.

Drone operations may become a more feasible alternative for insurance companies , and for all businesses for that matter, during major catastrophes; the FAA says that the new rules will be in place soon (supposedly this summer), and the restrictions on commercial drone use may be alleviated a bit.

This post is also being shared on our *Property Insurance Coverage Insights* blog. If you're interested in getting updates on developments affecting insurance coverage, we invite you to subscribe to the blog.

— Kathryn M. Rattigan and Deborah A. Vennos

CYBERSECURITY

Kansas Heart Hospital Pays Ransom but Attackers Renege on Their Word

In a rare and twisted result, Kansas Heart Hospital was hit with a ransomware attack on May 18, and made the decision to pay a "small amount" to the attackers in order to get its data back. Kansas Heart stated that no patient information was compromised and that the ransomware attack did not affect treatment to its patients.

However, instead of decrypting the data, the attackers did not return "full access to the files." Instead, according to the Hospital, the attackers requested another ransom. Dishonest ransomware attackers? Greedy attackers? The Hospital refused to pay the second ransom.

This has been unheard of in the industry, since the whole business plan around ransomware is to attack victims, encrypt their data until paid a ransom that is small enough for them not to think twice about paying it but large enough to make a profit, and then decrypt the data so the victims can go about their day-to-day business. The business plan relies on the attackers being true to their word that they will decrypt the data once paid. Otherwise, victims won't pay.

Keep in mind that the FBI recommends that companies NOT pay the attackers in a ransomware incident. However, many businesses, when confronted with ransomware, perform a risk analysis and determine that it makes more sense to pay the attackers the small sum to get their data back than to resort to getting their backup data online or move to contingency operations or disaster recovery mode.

The murky world of ransomware just got murkier. We have always joked about how ransomware attackers are pretty honest (yes, it is an oxymoron) and will decrypt the files once paid. But now? This oxymoron no longer applies. The greedy ransomware attacker is here.

According to Microsoft, the United States is the country with the worst ransomware problem and all businesses are targeted. These ransomware attacks are not going away, and now you may not get your data back even if you pay the ransom. Developing and testing a backup, contingent operations, and a disaster recovery plan are still imperative in a risk management program to prepare for continued ransomware attacks.

— Linn Foster Freedman

SWIFT CEO Announces Customer Security Programme

Following a series of thefts from international banks utilizing the Society for World Interbank Financial Telecommunication (SWIFT) communication system, the chief executive officer of SWIFT announced a

sweeping five-part plan to “reinforce the security of our shared global financial system.” The plan "includes:

- Improve information sharing among the global financial community;
- Harden security requirements for customer-managed software to better protect their local environments, enhance our guidelines and develop security audit frameworks for customers;
- Support banks’ increased use of payment pattern controls to identify suspicious behavior; and
- Introduce certification requirements for third party providers.”

In his speech on May 24, at the 14th Annual European Financial Services Conference, Mr. Leibbrandt stated that cyber risk has been the main thing keeping him awake at night. He stated that the financial industry must work harder at collective defensive efforts and that the fraud at the Bank of Bangladesh and two other banks will prove to be a watershed event for the banking industry. Mr. Leibbrandt further stated that “**banks that are compromised like this can be put out of business.** It’s not like retailers losing credit card details or telcos losing customer details. Telcos and retailers will take reputational hits, and may face some financial liabilities, but things will move on. When banks lose control of access to their payment channels, it’s different. In the recent cases, thieves were able to move just some of those banks’ overseas assets. As a result, for the banks concerned, the events haven’t been existential. The point is that they could have been.” (emphasis added)

Banks are under ever-increasing regulatory and industry requirements relating to information security. How the new SWIFT plan will work with the Cybersecurity Framework for Critical Infrastructure; the new FFIEC Assessment Tool and revised Handbook; the announced, but as yet unissued, cybersecurity regulations from the New York Department of Financial Services; and similar programs from the UK Financial Authority and the Monetary Authority of Singapore, among others, remains to be seen. Harmonization of the requirements on bank cybersecurity does not appear likely in the near future.

— Richard M. Borden

Maritime Cyber Threats are Real and Need to Be Addressed

A study published by Plymouth University’s Maritime Cyber Threats Research Group indicates that maritime vessels are at risk for cyber-attacks, as many have outdated software and are not designed with cybersecurity in mind.

A cyber-attack on a vessel could target the navigation and propulsion systems and the cargo-related functions. The results of a cyber-attack could be devastating to the shipping company, particularly since 90 percent of world trade occurs over the ocean. The consequences of a successful cyber-attack includes business disruption, financial loss, brand damage, damage to goods and the environment, incident response and mitigation costs, and legal fines and lawsuits.

The study outlines different scary scenarios of how possible attacks could occur and examples of how successfully carried-out attacks have occurred.

According to the study, “In an increasingly connected and technologically dependent world, new areas of vulnerability are emerging. However, this dependency increases the vessel’s presence in the cyber domain, increasing its chances of being targeted and offering new vectors for such attacks. Longer term, there needs to be a fundamentally different approach to security of the entire maritime infrastructure meaning there is great need for specific cybersecurity research programmes focused on the maritime sector.”

Finally, the paper states, “As things stand, there are fundamental issues with securing technology used in

the maritime industry and the sector is probably the most vulnerable aspect of critical national infrastructure. Both security firms and hackers have found both general flaws and specific, real-world, flaws within the navigation systems of ships, and it seems plausible that similar outdated systems for propulsion and cargo handling may also be compromised and abused by cyber-attackers."

The maritime industry is a significant part of critical infrastructure in world trade, and updating security systems, designing ships with security in mind, and training crew members should be considered, as in every other critical infrastructure industry.

— Linn Foster Freedman

PRIVACY TIP #37

Beware of Fake USB Drives and Phone Chargers

USB drives and phone chargers are expensive. Hackers know that. One way hackers are gaining access to computers to steal data is by planting USB drives and phone chargers in public areas, hoping someone will pick it up and take it to work or home. I find that people are unaware of this tactic, so the tip today is to beware of random USB drives and phone chargers and walk away if you find one.

How does it work? Portable drives are "modular and programmable" so attackers can swap parts or alter coding in the USB drive or phone charger and switch it with code that is able to change the functionality of the device into a password sniffer or keystroke logger that can infect a computer and steal information.

Last year, a white hat hacker was able to develop a device that looked like a generic USB mobile charger but was able to log, decrypt, and track all keystrokes from a Microsoft wireless keyboard and transmit the information over cellular networks, which has been dubbed "KeySweeper." Microsoft has stated that Bluetooth-enabled keyboards are protected against KeySweeper.

Black hats have developed their own malicious sweeping devices and individuals and businesses are becoming victims. It has become such a problem that the FBI recently issued a private industry warning to be aware of and look out for highly stealthy keyloggers that sniff passwords and other input data from wireless keyboards. According to the FBI, "if placed strategically in an office or other location where individuals might use wireless devices" the hackers could steal intellectual property, trade secrets, passwords, and personally identifiable information.

The FBI further stated that "[t]he primary method of defense is for corporations to restrict the use of wireless keyboards. Since the KeySweeper requires over-the-air-transmission, a wired keyboard will be safe from this type of attack."

According to Microsoft, to combat against this threat, use a Bluetooth-enabled keyboard or one that has been manufactured after 2011 that uses Advanced Encryption Standard (AES) encryption technology.

And when you see a stray USB drive or charger hanging around, don't be tempted. Walk away from it.

— Linn Foster Freedman

UPCOMING EVENTS

Authors' Events

In addition to their legal practice and involvement with the blog, our Data Privacy + Security Team members regularly serve as presenters at topic-related seminars, and participate on panels that discuss developments in the area. Following, are several upcoming speaking engagements:

- June 7 – The Quorum Initiative Cyber Intrusions event in New York City (Linn F. Freedman)
- June 8 – The Quorum Initiative Cyber Intrusions event in Washington D.C. (Linn F. Freedman)
- June 21 & 22 – Cloud Financial Services USA Conference in New York City (Richard M. Borden)
- June 22 – National Scholarship Providers Association in Rocky Hill, CT (Linn F. Freedman)
- June 23 – MCLE: Data Security 2.0: The Cloud, Mobile Devices & Encryption Webcast Panel (Kathleen M. Porter)
- July 11 & 12 – Seventeenth Annual Institute on Privacy and Data Security Law (Kathleen M. Porter)

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.