Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | April 2017

Introduction

This month we cover a variety of important recent developments impacting the Internet of Things (IoT), privacy and security enforcement, and the growing set of insurance-related disputes involving privacy and security coverage. I look at the most significant privacy enforcement developments so far this year, a series of cases brought by the New York Attorney General. Megan Brown examines several IoT developments, including "acoustic hacks" and the impact of "managed services" on IoT security. Ted Brown covers two recent insurance-related cases, dealing with potential coverage for specific losses under commercial crime insurance policies. We also have a broad variety of speaking appearances this month, and several recent presentations of note. Please look at our upcoming events, as well.

As always, please let me know if you have questions or comments on any of these topics. Also, if there are topics you would like to see addressed in future issues of *Privacy in Focus* – or if you have a need for a privacy or data security speaker at your event – please let me know. I can be reached at 202.719.7335 or knahra@wileyrein.com. Thank you for reading. ■

— Kirk Nahra, Privacy & Cybersecurity Practice Chair

ALSO IN THIS ISSUE

New York Attorney General Addresses Key Health Care Privacy Gaps

The most important health care privacy cases so far this year emanated not from Washington, but from Albany. New York Attorney General Eric Schneiderman announced on March 27, 2017, that his office had reached settlements with three different health mobile applications, based on misleading claims and inappropriate privacy practices. These cases begin to fill in various gaps in the regulatory structure for privacy, and also present the possibility that state attorneys general may step up to fill an enforcement void if Washington pulls back on privacy and security enforcement across the Administration (and may become stronger actors regardless of Washington activity).

The Cases

Following a year-long investigation, the attorney general (AG) announced three settlements against the following companies (as described in the AG press release):

- Cardiio, an American company that sells Cardiio, an app downloaded hundreds of thousands of times that claims to measure heart rate. The developer had not tested its accuracy with users who had engaged in vigorous exercise, despite marketing the app for that purpose. The developer also misleadingly implied that the app was endorsed by the Massachusetts Institute of Technology (MIT).
- Runtastic, an Austria-based company that sells Runtastic, an app that purports to measure heart rate and cardiovascular performance under stress. Yet the developer failed to test its accuracy with users who had engaged in vigorous exercise, despite marketing the app for that purpose to the 1 million people who downloaded it.

continued on page 4

‘Business E-Mail Compromise’ Scheme Losses Not Covered by Traditional Insurance

Introduction

According to the Federal Bureau of Investigation’s (FBI) Internet Crime Complaint Center (IC3), there has been a total of more than $3 billion in losses resulting from “business e-mail compromise” (BEC) schemes. *See* *Business E-Mail Compromise: Cyber-Enabled Financial Fraud on the Rise Globally*. Oftentimes in these crimes, a third-party criminal actor provides fraudulent wire instructions to a company’s accounting department and then, upon completion of the transaction, the criminal withdraws the funds. These losses can be very significant, and there are reported cases where sophisticated corporate parties have fallen victim to such schemes and lost millions of dollars at a time.

The existence of a loss gives rise to a related question – is there insurance coverage for these losses under traditional commercial crime insurance policies? To date, the answer appears to be a resounding “no.” In a recent case, the U.S. Court of Appeals for the Ninth Circuit, applying California law, added to the weight of authority finding no such coverage. *Taylor & Lieberman v. Federal Ins. Co.*, 2017 WL 929211 (9th Cir. Mar. 9, 2017).

Taylor & Lieberman

The insured in *Taylor & Lieberman*, an accounting firm, received several emails from a client’s email address with instructions for transferring client funds. Believing the instructions to be genuine, the accounting firm initiated the transfers. The firm subsequently learned that a third party had gained access to the client’s email address and sent the payment instructions as part of a fraudulent BEC scheme. It then sought coverage for the loss under its commercial crime policy, but the insurer denied coverage and coverage litigation ensued. The district court granted summary judgment in favor of the insurer after concluding, as a threshold matter, that the accounting firm could not show a “direct loss” because there were intervening causes between the initial fraudulent emails and the resulting loss.

On appeal, without addressing the “direct loss” issue, the court affirmed the decision on alternative grounds.

First, the court determined that the loss did not result “from Forgery or alteration of a Financial Instrument by a Third Party.” The accounting firm had contended that the words “financial instrument” only limited coverage for an alteration, and that a covered forgery need not be of a financial instrument. The court disagreed, holding that “under a natural reading of the policy, forgery coverage only extends to forgery of a financial instrument.”

Second, the court rejected the accounting firm’s argument that the computer fraud coverage applied because the emails constituted an unauthorized “entry into” its computer system or “introduction of instructions” that “propagate[d] themselves” through the insured’s computer system. The court reasoned that unwanted emails, without more, could not be considered an “unauthorized entry” into the recipient’s computer system. In addition, “under a common sense reading of the policy,” the court found that the fraudulent emails were “not the type of instructions that the policy was designed to cover, like the introduction of malicious computer code.” The court found the computer fraud coverage to be inapplicable on those grounds.

Third, the court ruled that the accounting firm was not entitled to coverage for the “fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by an Insured Organization at such Institution, without an Insured Organization’s knowledge or consent.” The court reasoned that, because the accounting firm requested the wire transfers, the transfers were made with both its “knowledge” and “consent.” The court also ruled that the coverage did not apply for the independent reason that the accounting firm was not a “financial institution.”

Conclusion

Taylor & Lieberman illustrates that traditional commercial crime policies may not afford coverage for losses caused through fraudulent instructions. However, there are specialized coverages available to protect against this exposure. In addition to evaluating operating policies and procedures in an attempt to avoid losses in the first instance, companies should evaluate their insurance coverage and consider purchasing specialized coverage to protect against losses caused by BEC schemes and related events. ■

For more information on these and other coverage issues, please contact:

Edward R. Brown
202.719.7580
erbrown@wileyrein.com

Is 'Managed IoT' the Key to IoT Security?

Policymakers considering the Internet of Things (IoT) and security confront a dizzying array of potential devices, services, use cases, and consumers. Commentary jumps from connected fridges to medical devices to industrial sensors, sometimes with scant recognition that end users' expectations are going to differ wildly across settings and evolve over time.

The U.S. Chamber of Commerce's Technology Engagement Center (C_TEC) recently urged the U.S. Department of Commerce to recognize the diversity of IoT, in order to help policymakers avoid oversimplifying IoT or lumping together dissimilar use cases. Those comments are available here.

To be sure, IoT is "things" that are connected, but it is also the connections and the services that support connectivity. Too much focus on devices ignores the complexity of IoT. IoT can be divided up in multiple ways, each of which may be premature as IoT is still evolving. We see consumer IoT and industrial IoT, though those can overlap when commercial devices and services make their way into enterprise settings like retail, hospitality, education, and the workplace. It may be more useful to watch for evolution into what C_TEC described as "managed and non-managed" products and services. We may see dominant platforms emerge, provided by reputable companies, to support consumer use of diverse IoT. We may also see platforms offered to support developers and product manufacturers looking for consistent approaches, interoperability, and more sophisticated life cycle management, including software updates, interaction with networks, and device end of life.

IBM recently offered "Five Indisputable Truths About IoT Security" that underscore the potential importance of managed services to IoT security. These Five Truths address "the importance of partnering with IoT vendors and solution providers who can be trusted" and the need of "administrators of IoT deployments" to have "visibility and control to deal with" threats and attacks. Indeed, managed services may make it easier to manage life cycle issues and "system defenses," which IBM says "will need to be updated repeatedly – for the life of these devices – impacting the supply chain for both software and equipment."

If the ecosystem evolves toward a managed services approach, it seems unlikely that government intervention or a "nudge" on security would be necessary. Large, experienced companies such as Microsoft, Cisco, Intel, and Amazon Web Services know how to offer large-scale services and support – both off the shelf and customized. They may lead in a similar fashion on IoT development and management, potentially obviating many concerns about security in IoT. The emergence of large-scale managed services could make it easier for policymakers to focus on the most troubling use cases or security risks that remain in the future IoT.

Are managed services a panacea? Probably not, and who knows if the demand for such services will materialize? If it does, will it be at the enterprise level, among consumers seeking to simplify their connected lives, or both? It is too soon to tell. This makes it entirely premature to begin prescribing solutions or have the government put its thumb on the scale. The market will drive development, delivery, and support platforms. Policymakers should look to this rapidly developing ecosystem to see how things unfold. Managed IoT may end up being a welcome solution to many of the technical and operational concerns about IoT security. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Kirk Nahra on the Trump Administration and Cybersecurity

Kirk J. Nahra, chair of Wiley Rein's Privacy & Cybersecurity Practice, was interviewed recently by LIFARS concerning the Trump Administration's anticipated policies and actions on cybersecurity. LIFARS LLC is a digital forensics and cybersecurity intelligence firm. Mr. Nahra discussed the expanding concept of cybersecurity, early indications of Administration thinking, the anticipated Executive Order, and recommendations for appropriate government action. The full text of this Q&A may be found here.

Mr. Nahra can be reached at 202.719.7335 or knahra@wileyrein.com.

Emerging Technology and Liability: Torts of the Future?

Discussions about connected devices, security, privacy, and liability continue to pick up speed. The U.S. Chamber of Commerce recently held a thought-leadership event in Menlo Park, CA, discussing IoT, emerging technology, and torts of the future. The agenda and panel videos can be found here.

Wiley Rein partner Megan L. Brown was a panelist. She and others from industry addressed emerging issues surrounding IoT-related liability and litigation. In particular, Ms. Brown identified the danger that litigation and fear of liability could stymie collaboration between the many players in the IoT ecosystem. Tort litigation is backward-looking, slow, and takes place before judges and juries that are not experts. Novel privacy-and security-related claims are being pushed in the courts; plaintiffs have struggled to establish standing, but are constantly trying new claims. Recently, "purchase price" claims have been raised. Plaintiffs allege that consumers paid more than they should have for connected products that later were shown to have a vulnerability. These claims are made even though there has been no exploitation or breach.

The day-long discussion featured panels from the auto and unmanned aerial vehicle industries, as well as keynotes from Lyft, Chamber leadership, and the attorney general for the state of Utah, who called for regulatory "humility" in the face of new technologies. One takeaway from the event is that now is the time for industry to help policymakers avoid missteps, and urge them to "think big" about how to promote IoT security in a collaborative, not punitive, way.

Ms. Brown and associate Umair Javed represent the Chamber Technology Engagement Center (C_TEC) on emerging issues in the IoT space. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Umair Javed
202.719.7475
ujaved@wileyrein.com

New York Attorney General Addresses Key Health Care Privacy Gaps *continued from page 1*

- Matis, an Israel-based company that sells My Baby's Beat, an app downloaded hundreds of thousands of times, which Matis previously claimed could turn any smartphone into a fetal heart monitor, despite the fact that it has never been approved by the U.S. Food and Drug Administration (FDA). Although Matis exhorted consumers to use My Baby's Beat rather than a fetal heart monitor or Doppler, it never conducted, for example, a comparison to a fetal heart monitor, Doppler, or any other device that had been scientifically proven to amplify the sound of a fetal heartbeat.

Concerns and Authorities

While each settlement was based on its own facts, the AG's office focused on three separate areas of concern. First, the AG was concerned about the accuracy of various health claims made by the apps. The developers generally agreed to provide additional information about testing of the apps and to change their ads to make them non-misleading. Second, because these apps are not regulated by the FDA, the settlement required the apps to post clear and prominent disclaimers informing consumers that the apps are not medical devices and are not approved by the FDA. Third, on the privacy front, the settlements required specific changes to privacy policies and practices. The app developers are now required to obtain affirmative consent to their privacy policies for these apps and disclose that they collect and share information that may be personally identifying (including users' GPS location, unique device identifier, and "de-identified" data that third parties may be able to use to re-identify specific users).

For the settlements, the AG relied on specific broad principles of New York law. In particular:

- The New York State Executive Law prohibits "illegal or fraudulent acts" in the conduct of any business, trade or commerce, and allows the OAG to institute a special proceeding for restitution, damages, and/or injunctive relief against any party which has committed such acts. N.Y. Exec. Law § 63(12).
- The New York General Business Law prohibits "deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service" in New York State, as

continued on page 6

Loss Caused by Fraudulent Exploitation of Coding Error Does Not Implicate Computer Fraud Coverage

A Georgia federal district court has held that a fraudulent scheme using telephones to exploit a computer coding vulnerability in the insured's system that ultimately led to a loss was not covered under a computer fraud provision in a commercial crime policy. *Incomm Holdings, Inc. v. Great Am. Ins. Co.,* 2017 WL 1021749 (N.D. Ga. Mar. 16, 2017).

The insured managed a prepaid card program. As part of the program, cardholders would load funds onto prepaid cards issued by banks. To load funds, the cardholders called a designated telephone number and inputted certain information. As a result of a coding error in the insured's computer system, cardholders were able to call into the system from multiple phones at the same time and make multiple loads, which enabled them to access more funds than they had purchased. Before the insured fixed the coding error, cardholders made approximately $10.3 million in unauthorized redemptions. As required by contract, the insured paid that amount to the issuing bank.

The insured sought coverage under a computer fraud provision in its commercial crime policy, which afforded coverage for "loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises: a. to a person (other than a messenger) outside those premises; or b. to a place outside those premises." The insurer denied coverage, and coverage litigation ensued.

The district court granted summary judgment in favor of the insurer, holding that the loss did not fall within the scope of the crime policy's coverage.

First, the court ruled that the loss was not caused by the "use[] of a computer." The court noted that each cardholder used a phone – which is not a "computer" – to make fraudulent redemptions. The court also rejected the notion that the cardholders "used" the insured's computer system, observing that "[l]awyerly arguments for expanding coverage to include losses involving a computer engaged at any point in the causal chain – between the perpetrators' conduct and the loss – unreasonably strain the ordinary understanding of 'computer fraud' and 'use of a[] computer.'"

As an alternate basis for its ruling, the court determined that the incident did not involve the "loss of … money … resulting directly from" computer fraud. The court reasoned that the "loss" at issue was not the insured's payment to the issuing bank, but instead occurred when the payments were made to merchants from the cardholder funds. As such, the court ruled that the "loss" was not caused "directly" by the fraudulent customer loads, but instead the loss was caused "directly" by the insured's decision to transfer funds to the bank, as required by its contract. ■

For more information, please contact:

Edward R. Brown
202.719.7580
erbrown@wileyrein.com

Kirk Nahra Podcast on the Future of HIPAA Under New OCR Head Roger Severino

Kirk J. Nahra, chair of Wiley Rein's Privacy & Cybersecurity Practice, was recently interviewed by the Information Security Media Group concerning the implications of the Trump Administration's appointment of Roger Severino to head the U.S. Department of Health and Human Services Office for Civil Rights with respect to the future of HIPAA privacy and security enforcement and related regulatory trends. Prior to this appointment, Mr. Severino was Director of the Heritage Foundation's DeVos Center for Religion and Civil Society.

The 15-minute interview is available here.

Mr. Nahra can be reached at 202.719.7335 or knahra@wileyrein.com.

An Acoustic Hack – The Next Botnet Breach?

Researchers at the University of Michigan and the University of South Carolina claim to have discovered that music could be used to disable or, to a certain extent, even control some Internet of Things (IoT) devices. The researchers say they were able, through sound waves, to add steps to a Fitbit tracker and interfere with a cell phone app's ability to steer a remote-controlled toy car.

To do so, the researchers used varying acoustic frequencies to exploit a claimed vulnerability in certain accelerometers – a hardware component that measures the amount of static acceleration due to gravity. These sensors serve a variety of purposes, ranging from those as basic as ensuring that your tablet computer screen is displayed upright to determining precisely when to deploy airbags in the event of a car accident. Manufacturers often build accelerometers within chip-based devices known as microelectromechanical systems (MEMs), which are used in a variety of products including cell phones, wearable devices, and drones and automobiles. The software components of connected devices frequently rely on the information provided by MEMs to determine the appropriate response. By creating an acoustic disturbance, the researchers affected the MEMs output.

This latest announcement emphasizes the role that academics and industry researchers can play in examining, discussing, and enhancing cybersecurity. Third-party research efforts can have various impacts and companies continue to grapple with how to address claims about their services and devices. Threats to IoT security are complex and constantly evolving, making cybersecurity research and information sharing key to enhancing the safety and reliability of connected devices. The University of Michigan and University of South Carolina researchers who discovered this potential vulnerability have also developed hardware and software solutions that can defend against acoustic attacks. The researchers are already working with chip manufacturers to improve the MEMs' design, as well as enhance the security of products already in the hands of consumers.

As connectivity explodes and more "things" interact with each other and the human environment, innovators can expect to continue reading about such "discoveries" – and having to address them. ■

For more information, please contact:

Madi Lottenbach
202.719.4193
mlottenbach@wileyrein.com

New York Attorney General Addresses Key Health Care Privacy Gaps *continued from page 4*

well as "false advertising in the conduct of any business," and authorizes the OAG to enjoin any such practices. N.Y. Gen. Bus. Law §§ 349 and 350.

- Marketing a Health Measurement App without substantiation of its accuracy and that it measures what it purports to measure, and without fully and clearly disclosing privacy practices, constitute deceptive business practices in violation of New York Executive Law § 63(12) and General Business Law §§ 349 and 350.

A Big Deal?

So, why is this a big deal? Three settlements, payment of $30,000, who cares besides these three companies?

State attorneys general have traditional authority to regulate potentially deceptive practices. Each of the apps involved in these settlements was accused of making misleading or inaccurate statements about various health care claims related to the apps. These settlements indicate that at least this state AG is watching these representations, and that apps will be challenged if their claims exceed their facts.

New York also is acting in a regulatory gap related to FDA oversight. The FDA has current oversight over certain "medical devices," but the full scope of this authority is an ongoing source of debate. In any event, these apps did not trigger FDA scrutiny. The New York AG is taking steps to ensure that consumers understand that these apps are not medical devices and are not approved by the FDA – a transparency issue of importance to consumers in this area. The Matis settlement, for example, contained a requirement to include language stating "This app is NOT a medical device, has not been reviewed by the FDA, and is NOT intended as a replacement for medical advice of any kind."

continued on page 7

On the privacy front, the AG also is stepping into a regulatory gap. While these apps collected a broad range of health care information, because no "covered entity" is involved (e.g., a health care provider or health plan), the HIPAA rules are not applicable to these apps. HIPAA is an important and broad privacy rule, but it is not a general medical privacy rule – it applies only where personal data flows through or on behalf of a covered entity. Direct-to-consumer apps fit into this gap, meaning that HIPAA does not apply. The New York AG is stepping in to take steps to ensure privacy protections related to these apps, in the absence of a formal regulation. It is possible that we will see this as a first step – much like the Federal Trade Commission (FTC) has done with data security – toward regulation through enforcement.

Specifically, the New York AG required these apps to:

- Obtain affirmative consent to their privacy policies;
- Disclose to consumers the risk that third parties, who receive aggregated or "de-identified" data from the apps in order to provide services to the apps or otherwise, may re-identify data about specific users. (The settlements state that "Although this data does not identify users personally, there is a risk that third parties who receive such data from [the apps] may reidentify specific users.")
- Prior to sharing any de-identified user information with third parties, the apps shall, in writing, request that such third parties not attempt to re-identify the information to any particular individual. (It is interesting to note that one of these settlements required the app to "request" this agreement, while the other two settlements required the apps to "in writing, secure the express written agreement" not to re-identify.)
- Disclose that the health data collected by the apps may not be protected by the HIPAA rules;
- "Establish and implement reasonable security policies and procedures designed to protect user information," which must be "appropriate to the nature and scope of [the apps'] activities and the sensitivity of the covered information," and review and update these policies as necessary, at least bi-annually.

Accordingly, this potentially groundbreaking series of settlements created new rules for factual support for health-related claims, required additional transparency that apps are not regulated by the FDA or HIPAA, and imposed new privacy and security obligations on the creators of these apps.

Obviously, all app developers need to pay close attention to these issues. We will watch for whether the New York AG continues to take action in this area (or in a broad variety of other "non-HIPAA" areas), and whether other state AGs will join this effort. On a broader level, we will be watching closely whether state AGs become a more prominent focus of attention on privacy and data security enforcement. They have broad authority – through general "consumer protection" authority that mirrors the authority of the FTC, authority to enforce data breach notification laws and even the HIPAA rules (through specific mandates created by the HITECH law). They have had this authority for a long time, but we have not seen it exercised much. These cases may signal an important change. Pay close attention to the state AGs and any future actions over the next several years. ■

For more information on these and other health-care-related matters, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

SPEECHES & EVENTS

Privacy Boot Camp

IAPP Global Privacy Summit 2017

Kirk J. Nahra, Speaker

APRIL 18, 2017 | WASHINGTON, DC

IoT from Startups to Titans: Building a Healthy Ecosystem

Women's High-Tech Coalition

Megan L. Brown, Speaker

APRIL 20, 2017 | WASHINGTON, DC

"The Exchange" Data Privacy and Cybersecurity Forum

Today's General Counsel Institute

Matthew J. Gardner, Co-Chair

APRIL 26-27, 2017 | BOSTON, MA

The Changing Landscape of IoT: Medical Device Privacy and Cybersecurity

FDLI Annual Conference: Exploring Advanced Topics in Food and Drug Law

Sonali P. Gunawardhana, Speaker

APRIL 26, 2017 | WASHINGTON, DC

Top 10 Privacy & Information Security Developments for 2017

BCBSA 2017 National Summit

Kirk J. Nahra, Speaker

MAY 9, 2017 | ORLANDO, FL

HIPAA Enforcement Update

BCBSA 2017 National Summit

Kirk J. Nahra, Speaker

MAY 9, 2017 | ORLANDO, FL

The New Era of Big Data for Health Care

American Health Lawyers Association Annual Meeting 2017

Kirk J. Nahra, Speaker

JUNE 26 & 28, 2017 | SAN FRANCISCO, CA

Contributing Authors

Edward R. Brown	202.719.7580	erbrown@wileyrein.com
Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Umair Javed	202.719.7475	ujaved@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com