Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | March 2018

We cover a broad range of topics this month, consistent with the frenetic activity around the country and the world relating to privacy and security. I look at one of the top recent news items involving health care, the evolving role of employers in the health care of their employees. Leland Jones, Edward Brown, and Bonnie Thompson address the insurance implications of one of the hot topics in the field today, coverage issues relating to cryptocurrencies. We also cover two recent events in Washington – Shawn Donovan summarizes the Federal Trade Commission's PrivacyCon 2018, and Michael Diakiwski and Megan Brown review NIST's second botnet workshop. Megan Brown, Matthew Gardner, and Michael Diakiwski assess the Department of Justice's new Cyber Task Force and its role in reviewing the cyber implications of the Internet of Things (IoT). John Lin and Megan Brown review recent IoT litigation and the ongoing battles over "standing" in breach-related litigation.

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

Employer Challenges for Health Care Data Are Growing

By Kirk J. Nahra

ALSO IN THIS ISSUE

For reasons largely lost to American history, for many decades employers in the United States have been intimately involved in the provision of health care services – including health insurance – for their employees. While the role of employers in providing health insurance is the source of extensive debate today, a substantial portion of Americans continue to receive their health insurance coverage through their employer.

Obviously, as with everything in the health care system, the role of employers has been evolving in recent years. Many employers still provide on-site health clinics for their workers, which may provide a broader range of services than just

continued on page 2

Suing over Technology Security Still Requires Standing, but for How Long?

By Megan L. Brown and John T. Lin

We continue to see concern over technology and security, with an increasing focus on the Internet of Things (IoT). Courts are becoming a popular forum for these disputes, with class-action litigants, like those in *Edenborough et al v. ADT, LLC et al*, No. 3:16-cv-02233 (N.D. Cal. Apr. 25, 2016), hoping that the courts will step in to set technology policy. Likewise, commentators like Bruce Schneier encourage the government to use regulation or standards of care to let litigants "**impose liabilities on manufacturers**" of IoT devices.

Courts, in the main, insist that plaintiffs bring non-abstract claims based on actual harm. In an **opinion** released late last year in a highly watched case, the Ninth Circuit affirmed a lower court's dismissal of C*ahen v. Toyota Motor Corp*, a class-action case involving automotive cybersecurity. There, class-action plaintiffs claimed, based on news reports, that their vehicles contained electronic control units that could be hacked, and sought money damages despite there being no actual exploit or breach of consumer data.

continued on page 7

Employer Challenges for Health Care Data Are Growing

continued from page 1

routine care in connection with work-related activities. Employers are struggling to make health care and health insurance programs both more effective in promoting employee health and less expensive. The industry saw enormous speculation about the potential impact of a recently announced partnership between Amazon, Berkshire Hathaway, and J.P. Morgan to engage in some new form of employee health care and health insurance (although details are scarce).

The general push towards wellness programs also has complicated this discussion. As employers (and the vendors they retain to promote these programs) expand wellness programs, both in terms of scope and potential impact on employees – employers are faced with increasing challenges in terms of how to realistically, effectively, and appropriately monitor and oversee both these programs and their employees' health in general.

Most recently, Chrissy Farr, CNBC's prominent and tireless health care and technology reporter, reported on an intriguing new development involving Apple, where Apple has announced that it will be establishing primary care clinics for some of its employees (starting near its corporate headquarters). While described in these reports as "independent of Apple," these clinics will create more tensions for the employer's role in providing health care services for employees because of the volume of health care data that will be gathered.

On top of all these challenges are the HIPAA privacy and security rules, which create compliance challenges for any employer

continued on page 3

that provides health insurance benefits to its employees.

So, with that background, what should employers be paying particular attention to in connection with their provision of health care services and related benefits to employees?

HIPAA compliance is even more important in today's environment

Since the HIPAA privacy rule first went into effect in 2003, employer health plans have been "covered entities." While this may have been an odd result, and employer health plans never operated in the same way as a hospital or health insurer, the rules applied to these plans. I first wrote about these obligations in 2004, in an article entitled "Making Sense of HIPAA Privacy for Employers." (An updated version of this article is available **here)**

Now, almost 15 years later, it continues to be surprising to me how few employers seem to understand that they are subject to HIPAA if they provide health care benefits to employees, and how many of those that are aware of these obligations have not re-evaluated their compliance activities in many years. For most employers, these obligations arise because the employee benefit plan that provides health insurance benefits is considered a "health plan" under the HIPAA rules. The company's obligations will vary somewhat based on how the plan is financed and operated. And some of the risks I was concerned about in 2004 have not in fact arisen (such as the likelihood that employees who were terminated would allege HIPAA-related violations which could create problems for employers even where none should exist because of a failure to comply with HIPAA's regulatory requirements).

Other employers – a smaller number for sure – may also have obligations as a health care provider, if health care services are provided directly to employees in certain situations.

But the fact remains that employers in every industry need to evaluate their HIPAA obligations and take steps to both comply with the rules (based on the enforcement and security breach risks) and ensure that sensitive employee health information remains appropriately protected.

HIPAA creates two major challenges for employers. First, from the employee benefits perspective, HIPAA imposes compliance obligations on the benefit plan directly – not on the employer. However, this obligation does not reflect the reality at most employers – which is that the benefit plan is primarily a contract with employees that is defined by the ERISA statute and is not in any other way an independent organization or group of individuals. Employers must make sense of how to comply with a set of obligations imposed on this piece of paper.

In addition, the HIPAA rules do not apply to all health information – they apply to individually identifiable health information in contexts subject to the HIPAA rules, mainly where a health care provider or health plan is involved. So, there is a broad variety of "health information" held by employers – from workers compensation and disability claims to Family and Medical Leave Act materials to basic employment-related data – which is health-related but is not subject to the HIPAA rules.

A few key steps that virtually any employer should be taking:

- You should be conducting a review of the role played by your company in the management of your health care benefits program.

continued on page 4

- You should identify the information that comes into your company that is regulated by the HIPAA rules – primarily the information about employee health care claims through your health insurance benefits program.
- You should identify (and strictly limit) the internal personnel who play any role in the use or disclosure of individually identifiable health information from your benefits program.
- You should train these people on the requirements of the HIPAA rules and the complexity of overall management of employee health data.
- You should identify where within your information systems this individually identifiable health information is stored.
- You should conduct a security risk assessment for those information systems that store this information.
- You should evaluate the overall requirements under HIPAA for documentation of your HIPAA obligations, and evaluate carefully whether your policies and procedures meet these requirements.
- You should have a plan for how to separate HIPAA data from other employee data.

Understand your wellness program

The complexity of HIPAA's requirements in an employer-based environment is exacerbated by the recent expansion of employer wellness programs, which raise both the confusion and risks related to the protection of employee health information.

Wellness programs are evolving constantly. There is a meaningful debate about whether these programs are "successful" (including debate on how to measure what successful means). Early programs were often informational – simply providing information about specific illnesses or conditions (e.g., smoking cessation) to whomever was interested in receiving it. Now, these programs are often more participatory – and significantly more information is gathered through them. They often involve a requirement to participate in certain health insurance programs, or provide discounts (or penalties) based on your participation. Other programs focus on substance beyond "participation," to include actual results.

For employers, it is critical to understand how these programs operate, even if you have primarily outsourced their operation. Are they covered by HIPAA? This may depend in large part on who is covered by them – if employees who are not part of your health insurance program can participate in wellness programs, then HIPAA may not be relevant. If HIPAA is not in play, what are the guiding rules? Do you know what your vendor is doing with information about your employees? Do the employees know? Has someone provided them with a privacy notice about the wellness programs? Do they have reasonable choices about the information being collected and how it is being used?

These wellness programs are complicated, and may present opportunities to control costs through improved employee health (presumably a win-win). There certainly are those in the field who believe that wellness programs disproportionately focus on costs without addressing employee health. Independent of this debate, companies that offer wellness programs should ensure that they understand how they operate, are aware of how employee data is being used and disclosed (and by

continued on page 5

whom), and that employee privacy issues are being considered appropriately in the management and oversight of these programs.

Employee monitoring should be included as well

An additional (and increasingly important) element is overall employee monitoring and related data gathering efforts by employers. This is a particularly challenging area because it is very loosely defined. Employers are looking constantly to improve employee performance. This effort is taking on a growing range of possibilities because of new means of overseeing what employees are doing on the job, and new areas where employers can gather data about what employees are doing away from the job.

From a privacy perspective, the biggest risk for employers may be in gathering and analyzing data without a thoughtful privacy analysis upfront. Because of the significant gaps in the law that exist today (for example, in the collection of health data outside of the HIPAA environment), companies may in fact have reasonable flexibility to gather and analyze data about their employees. At the same time, there are substantial risks that can be avoided through thoughtful planning.

Do you know what data you have about employees? Conduct a thoughtful review throughout your company on where data about employees is being collected – and make sure that you update this regularly, as your corporate team will be looking constantly for new sources of information.

Do you know how this information is being used? Are you making judgments about employees based on this information? Do employees know this? Do you have standards for how to make these decisions?

Have you restricted where this information goes and who has access to it?

Have you implemented reasonable and appropriate security procedures for any portions of your information systems that store this information? Remember – even if HIPAA is not relevant, many state laws now require breach notification in the event of security breaches involving health information.

Do you have documented procedures about this information, including when it is covered by HIPAA, when it is not, and how you are keeping those lines separate?

Managing Your Contracts

Many of these information-gathering efforts are operated by outside entities – the sources of much of this information, the operators of various programs, and the analytics firms that guide decision-making. Do you have appropriate protections – for your employees and your company – in these contracts? Do you know what these companies are doing with data about your employees? What happens if there is a security breach on their end about this information? Make sure that your contracts address these issues and that they stay current as laws and practices evolve.

Do you have an international component?

The HIPAA rules and state breach notification laws create enormous tensions and complexity for employers operating in the United States. Do you have an international component that adds to these concerns? New data protection laws across the globe are expanding on these challenges. The new GDPR rules going into effect in Europe later this year (May 2018) will create compliance

continued on page 6

challenges for a broad range of companies, both obvious ones operating in the EU and many others. If you have employees in other countries – particularly in Europe – and you send employee data to the United States, you will need to meet both the compliance challenges of the law where the data starts (in Europe, the GDPR, for example), as well as the array of new data transfer principles that you must meet to legally transfer data from these countries to the United States (such as the Privacy Shield program or the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System). For many of these countries, health data is considered sensitive data, with additional compliance obligations and complications.

Do you understand the scope of health data?

Last, one of the most recent developments in the broadest health care privacy space involves the increasing breadth of the personal data that is considered "health data," or that is being used for health-related purposes. Insurers are using data such as income, marital status, and number of cars to evaluate potential emergency room utilization. Health care providers may be taking action based on patient data involving clothing purchases and gym membership status. As new sources of data emerge, data analytics professionals (who operate in a very loosely regulated environment) search for meaningful connections between pieces of data and intended results. They often want data simply to evaluate where it might be relevant or how it could be used – without any real sense of how useful or accurate it will be. You should understand how your company – and your vendors – are gathering and using data about your employees, to understand whether these actions create meaningful privacy concerns.

Have you communicated to your employees?

Privacy notices remain an important element of how any company communicates its data use activities to its relevant audiences, and how it also protects itself from allegations about its activities. Outside of HIPAA (for employers), many privacy notices are not heavily regulated, or there is substantial flexibility to describe comprehensively and accurately how a company is using data. Any employer should be re-evaluating its employee privacy notices, to ensure that it is incorporating all relevant activities and uses of the data.

Conclusions

Personal health care information is inherently sensitive. And, while the scope of what is considered health information is growing, individuals remain concerned about job impacts, personal embarrassment, insurance risks, and a broad variety of other potential risks of adverse consequences resulting from their health care information. Identity thieves also find health care information to be incredibly valuable. At the same time, as employers become more involved in the overall management of employee wellness and health care expenditures, there is a stronger interest in effective management and utilization of this employee data for a growing range of employer interests. And, as employers participate (along with many others) in the big data revolution, there are new opportunities to gather information that will promote more effective and efficient workplaces. Employers need to very carefully consider their approach to employee health care information and how they will act

continued on page 7

Employer Challenges for Health Care Data Are Growing

continued from page 6

effectively and intelligently in this controversial and risky area. This is not a message to avoid this data or avoid its potential benefits. Instead, the challenge is to ensure that you are engaging in this growing range of opportunities with careful thought and an appropriate consideration of the evolving and confusing legal and regulatory environment. ■

For more information on these and other health care data issues, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

Suing over Technology Security Still Requires Standing, but for How Long?

continued from page 2

The Ninth Circuit affirmed the dismissal for lack of standing, because the plaintiffs failed to allege an injury-in-fact. Their vehicles had not actually been hacked, and they could not show that any vehicle had been hacked outside of a controlled environment. The court stated that mere risk of being hacked was "speculative" and not enough to show injury.

Nor could the plaintiffs show injury based on overpaying for their cars, a novel theory that plaintiffs were testing. The court stated that such an allegation was "conclusory and unsupported by any facts," because the plaintiffs could not show any economic loss.

Finally, the plaintiffs could not show they suffered injury based on invasion of privacy. They could not show why the data collected from their cars is sensitive or individually identifiable to a particular driver. They therefore could not "demonstrat[e] how the aggregate collection and storage of non-individually identifiable driving history and vehicle performance data cause an actual injury."

This case shows that a high bar continues to face plaintiffs bringing lawsuits related to security issues in new technology: They will need to show that they were actually injured. Abstract claims are insufficient. But the case also highlights the growing use of litigation to try to influence emerging technology. We expect more such litigation in the future, even though, as discussed in an **earlier post**, tech policy is best developed not by judges and juries – but by the market, supported by Executive and Legislative branch action to facilitate innovation. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

John T. Lin
202.719.3570
jlin@wileyrein.com

FTC PrivacyCon 2018 Examines Opportunities and Challenges in Privacy and Data Security

By Shawn M. Donovan

On February 28, 2018, the Federal Trade Commission (FTC or Commission) hosted **PrivacyCon 2018**. The conference featured the presentation and discussion of original research completed during the prior two years. It explored a variety of privacy and cybersecurity issues in the Internet ecosystem. The FTC's stated objective was to examine the privacy and security implications of emerging technologies. Companies should expect the FTC to remain vigilant about new products and services, and the conference previewed a number of potential action areas.

The Conference

Acting FTC Chairman Maureen K. Ohlhausen opened the conference by highlighting **recent FTC privacy actions** and **related initiatives**. The remainder of the conference was divided into four sessions, each focusing on a distinct area of privacy and data protection. The panelists brought a variety of expertise in topics that ranged from the exfiltration of personal data by session-replay scripts to consumer expectations regarding **Internet-connected toys**.

Session 1: Collection, Exfiltration, and Leakage of Private Information

- Steven Englehardt, Ph.D. candidate at Princeton University, discussed email tracking. He claimed that many of the top web trackers are now in emails, and the line between email and web tracking has been blurred.
- Michael Weissbacher, doctoral student at Northeastern University, focused on browser extensions. According to Weissbacher, these extensions often leak complete consumer browsing history to third parties.
- Milijana Surbatovich, Ph.D. candidate at Carnegie Mellon University (CMU), discussed the use of "if this, then that" applets in the Internet of Things (IoT). She noted research finding that half of all tested applets violated secrecy or data integrity standards.
- Gunes Acar, Postdoctoral Research Associate at Princeton University, focused on session-relay scripts, which record individual browsing sessions (e.g., user scrolls and clicks). Companies often use these scripts to improve websites, but the recorded sessions can expose passwords, credit and health data, and purchase details.
- Alan Mislove, Associate Professor and Associate Dean at Northeastern University, argued that social networks are modern data brokers and can be misused to link multiple pieces of personally identifiable information (PII) to single users, infer phone numbers, and de-anonymize visitors.

Takeaways: The panelists agreed that unintentionally collecting certain data creates liability risks. They also suggested that the FTC should take steps to encourage transparency on data collection and sharing. To mitigate these risks, companies should continue to find innovative ways to minimize data collection and follow FTC transparency guidelines.

continued on page 9

continued from page 8

Session 2: Consumer Preferences, Expectations, and Behaviors

- Jingjing Ren, Ph.D. candidate at Northeastern University, discussed data leaks in mobile apps. She emphasized that mobile adoption of https has been slow and that third-party tracking is pervasive and broad.
- Kristopher Micinski, Visiting Professor at Haverford College, discussed permissions on mobile operating systems. He has led two studies examining how apps use permissions and device functionality. The studies found that apps use the most sensitive functions (e.g., cameras and microphones) only when interacting with consumers, while other functions are used more often and without consumer interaction.
- Emily McReynolds, Senior Privacy Manager at Microsoft and former researcher at the University of Washington Tech Policy Lab, highlighted consumer expectations for connected toys. In her research, some parents claimed to not have time to review all required disclosures, while others were concerned about their children's information. When told that they were recorded, the children said it sounded "scary."
- Pardis Emami-Naeini, Ph.D. student at Carnegie Mellon University, discussed expectations and preferences in an IoT world, as well as a mobile application that provides information on nearby IoT devices. She described a survey showing that consumers want to be notified when their data is shared or biometric data is collected. The type of data and perceived benefits mattered most to consumers.
- Yang Wang, Assistant Professor at Syracuse University, explored privacy violations in crowd work (i.e., when a company obtains contributions from an undefined pool of people). He argued that information collection, processing, dissemination, invasion, and deceptive practices are ripe areas of consumer concern.

Takeaways: Consumer expectations are complex and evolving. The FTC noted that it often gets complaints that people do not read privacy policies, and the panelists agreed that the Commission needs to properly scope disclosure requirements to avoid notice fatigue. Companies should consider information sensitivity in tandem with consumer benefits and avoid excessive notifications.

Session 3: Economics, Markets, and Experiments

- Ying Lei Toh, Ph.D. candidate at the Toulouse School of Economics, explored incentives for firms to protect consumer data. Her research focuses on whether data breaches cause reputational damage and found that the answer depends on whether a consumer is both willing and able to punish the firm (e.g., do they know of the breach?). She also noted that mandatory breach notification could hurt investment levels.
- Sasha Romanosky, Policy Researcher at the RAND Corporation, discussed cyber insurance policies and how a lack of data limits insurers' ability to price cyber risks.

continued on page 10

continued from page 9

- Jaspreet Bhatia, Ph.D. candidate at Carnegie Mellon University, examined empirical measurements of perceived privacy risks, finding that consumers are more likely to share data with government about who they are (e.g., device information, IP address) than what they do online.
- Caleb Fuller, Assistant Professor at Grove City College, considered whether there is a market failure in digital privacy. His research suggests that users are aware of collection practices generally but unaware of specific practices. He claimed that consumers want more privacy, but only 15% are willing to pay for it.
- Christian Catalini, Professor at the Massachusetts Institute of Technology, discussed the digital privacy paradox, in which consumers claim to value privacy but are willing to provide extensive personal data for free services.

Takeaways: Consumers are generally aware of collection policies and believe that information sharing is beneficial. Companies should continue to offer services that consumers value in exchange for the data they collect and share.

Session 4: Tools and Ratings for Privacy Management

- Periwinkle Doerfler, Ph.D. candidate at New York University, discussed the use of mobile spyware in abusive relationships. She demonstrated a mobile app that does not display an icon and records video and audio while the phone appears off.
- Saksham Chitkara, Graduate Research Associate at Carnegie Mellon University, examined context-aware privacy management on smartphones. He claimed that the current app permission structure is a "black box" and that third-party libraries often collect data for which they have no use. He has developed a mobile app, ProtectMyPrivacy, that minimizes data flowing to third-party libraries.
- Ian Douglas, from the Office of the Privacy Commissioner of Canada, discussed IoT privacy in health and medical devices. His research found that the amount of data collected varies; sharing is not as frequent as expected; well-established medical companies have better safeguards; and scrubbing data is not always easy or possible.
- Katie McInnis, Policy Counsel for the Consumers Union, presented privacy and security research on connected televisions.
- Norman Sadeh, Professor at Carnegie Mellon University, discussed "assisting users in a world full of cameras." He found that there are over 6,000 cameras in Times Square alone, with uses that include facial recognition, security, and marketing. He also found that the use of facial recognition is on the rise. He noted that most users claim to want notice and choice for facial recognition, and would disable the feature if given the option.

Takeaways: Data collection and integrity processes vary. Companies should ensure that their processes are properly suited to their use cases.

continued on page 11

continued from page 10

Conclusion

As the FTC continues to emphasize consumer privacy and data security, companies should be mindful of the issues explored at the conference. Companies should be careful to minimize the data they collect and share; follow FTC transparency guidelines; weigh the sensitivity of consumer information with perceived consumer benefits; offer relevant services that consumers value in exchange for collected data; and ensure that collection and security processes are properly scoped.

The U.S. Court of Appeals for the Ninth Circuit recently upheld FTC authority to regulate non-telephone activities of mobile operators and other common carriers, and companies should prepare for increased FTC action in the privacy and security space more generally. ■

For more information, please contact:

Shawn M. Donovan
202.719.7293
sdonovan@wileyrein.com

NIST Hosts Second Botnet Workshop

By Michael L. Diakiwski and Megan L. Brown

The National Institute of Standards and Technology's (NIST) National Cybersecurity Center of Excellence (NCCoE) hosted its second workshop on enhancing resilience of the Internet and communications ecosystem. The February 28 – March 1 workshop focused on substantive comments from stakeholders on the draft ***Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats***. This is the last workshop before the final report is due to the President on May 11, 2018.

The workshop intended to refine the report's recommendations to the President. Workshop topics included: proposals for Internet of Things (IoT) security; possible assessment, certification, and evaluation schemes; incentivizing security in the IoT marketplace; broadening international engagement; and appropriate roles for various stakeholders involved.

Wiley Rein previously **highlighted important aspects** of the report, its potential impact on the private sector, and the opportunity to file public comments.

Background on this Effort

The Departments of Commerce and Homeland Security developed the report in response to **Executive Order 13800**, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which directed the Secretaries of Commerce and Homeland Security to "lead an open and transparent process to identify and promote action by appropriate stakeholders" with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)."

continued on page 12

NIST Hosts Second Botnet Workshop

continued from page 11

In July, we **covered the first workshop**, which helped inform topics included in the draft report.

Nearly 50 stakeholders have **filed comments** since its release. We **highlighted** that several major comments note the draft report does not fully address important issues concerning barriers to greater collaboration between private industry and government. For example, a number of commenters emphasized the need for the government to consider ways to limit liability for companies that quickly disclose cyber vulnerabilities or share threat indicators:

- **CTIA** argues that "[t]he Report does not address barriers to implementing many of the Actions it calls for. Information sharing, certification regimes, and labeling involve some risk related to public disclosure of sensitive information, responsibility, and liability ... The Report should explicitly consider barriers."
- **The U.S. Chamber of Commerce** believes that "[i]ndustry and government should look for novel ways to limit liability for private entities that employ defensive measures in good faith."
- **The Aviation Information Sharing and Analysis Center (ISAC)** "recommend[s] consideration to limit liability to companies who make swift public disclosures of vulnerabilities and expeditiously issue patches. This will incentivize two key pillars in reducing cyber risk: the independent researchers will be motivated to continue notifying companies of coding errors and companies will be incentivized to respond quickly."
- **ACT | The App Association** claims that "the existing information sharing environment remains vulnerable," and "[p]rivate sector entities may be reluctant to share this information amongst each other due to concerns about legal liability, antitrust violations, and potential misuse."

While addressing barriers to greater collaboration was mentioned at the workshop, presenters noted that some issues remained, greater detail would be needed, and that the White House would need to direct certain actions or decisions.

Key Takeaways from the Workshop

NIST presenters noted that, based on stakeholder comments, several sections would expand from the draft report, including those on:

- Privacy;
- Civil Society;
- Infrastructure; and
- Education and Awareness.

NIST stated that the agency generally "had a handle" on these issues, so the workshop would focus on other topics, which required further discussion. The following highlights are from workshop panels and breakout sessions.

Leadership

A panel titled "Who Leads?" featured industry representatives and associations who highlighted past, ongoing, and planned efforts to continue to enhance the ecosystem. The roles of industry and government were highlighted and discussed. Panelists noted industry collaboration, shared best practices, notification efforts, and ways to assess and harmonize current activities. One area that could be improved upon is to provide better

continued on page 13

cross-sector visibility into security plans, initiatives, and threats encountered.

Panelists remarked that the U.S. government is positioned to galvanize cybersecurity response without disrupting the technological successes of the past few decades. For example, agencies can work as conveners (as NIST, NTIA, and DHS have done with this botnet effort). Panelists mentioned that third-party trust groups can improve information sharing, although certain barriers still exist.

It was also noted that the U.S. government can and should lead by example – by improving its own cybersecurity posture. The IT modernization effort was pointed to as a good place to start. Beyond this, the U.S. government should work with industry to develop voluntary best practices for IoT, as it has done with the successful NIST *Cybersecurity Framework* (CSF). Such an effort could have impacts on a broad, international scale.

DDoS Cybersecurity Framework Profile and IoT Functional Profile

A NIST representative noted that a distributed denial of service (DDoS) CSF Profile may be included in the report and cited the Coalition for Cybersecurity Law's **comments**, Appendix A "DDoS Threat Mitigation Profile," as an example.

A presenter suggested that ISPs and network operators should take (or improve upon) four core steps to mitigate DDoS attacks, including: (1) improved filtering; (2) anti-spoofing; (3) enhanced coordination with government entities, other ISPs, and end users; and (4) global validation.

Other presenters focused on the need to establish "expectations for baseline security functionality" with consumer IoT devices. A panelist also called for a more consumer-centric model, with greater transparency to be provided by both network operators and device manufacturers, suggesting potential labeling mechanisms and minimum security standards.

Assessment, Certification, and Evaluation

A NIST representative introduced the process for conformity assessments (i.e., standards development). The NIST presenter noted that possible standards in the IoT marketplace could be developed by following a conformity model that includes: (1) coalescing around requirements, or agreeing on a standard of how a device should perform; (2) making that determination based on evidence from standardized testing to ensure that performance; (3) reviewing or attesting to that standard, which may require an independent, trusted third-party; and (4) ongoing testing or surveillance, to adjust standards as the ecosystem evolves.

Another panelist advanced that motivations for industry to move toward standards adoption or development could include: company or product reputation, marketing advantages (for highly certified or "scored" devices), security as benefit to shareholders, and enhancing the security of the ecosystem overall.

Some attendees presented questions on the applicability of a ratings system in an ecosystem comprised of billions of devices, each with varying use cases, risk profiles, and applications across industries. Others questioned whether assurances of security in the form of a "rating" could lead users to falsely assume a device is immune from attack

continued on page 14

or that a rating is a replacement for following best security practices at the end-user stage.

Incentivizing Security

Panelists noted that while labeling for consumer devices could have some merit, benefits could be greater by incentivizing sharing security information of an IoT device or its components at the enterprise level. Large enterprises can drive cybersecurity by leveraging their supply chains, establishing minimum standards, or setting expectations for the type of information needed to participate in the supply chain.

Cyber insurance was highlighted in this conversation as well. It was noted that premiums can be used to incentivize security. A speaker suggested that change could be incentivized by the following: (1) the tax code; (2) insurance; (3) litigation; (4) regulation; and (5) international treaties. Each one of these, or some used in combination, could impact practices related to security.

It was also noted that a tension exists between accountability and transparency – if a sector or industry actor is punished or exposed to litigation, are they more or less likely to participate in information sharing environments? In terms of encouraging greater collaboration, it was suggested that limiting liability at certain levels, offering immunity on certain terms, and reducing exposure to class action lawsuits, could all advance greater information sharing and collaboration on cybersecurity efforts.

International Engagement

Emphasis was placed on the global – and inherently distributed – nature of the botnet threat. These challenges require an international strategy and approach. sThe shared responsibility of securing the network does not stop at national borders. Therefore, panelists noted that cooperation is key to botnet mitigation. Representatives from several international organizations highlighted collaborative efforts, IoT consortiums, global and trusted third-party information sharing programs, and law enforcement activities to help build a more resilient ecosystem.

Next Steps

At the conclusion of the workshop, representatives from NIST highlighted that reviewers from the Departments of Commerce and Homeland Security will still consider comments emailed to the designated address found on the initiative's **main page**, but the window to help shape the report is quickly closing.

The final Report on *Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* is due to the President on May 11, 2018. Then, the decision to adopt or follow recommendations of the report will lie with the White House. ■

For more information, please contact:

Michael L. Diakiwski
202.719.4081
mdiakiwski@wileyrein.com

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Cryptocurrencies: Money, Securities or Other Property?

By Leland H. Jones IV, Edward R. Brown, and Bonnie J. Thompson

A 24-year-old trader is facing up to 20 years in prison for wire fraud after being charged in connection with a scheme to use approximately $3.2 million worth of his company's cryptocurrency for personal trading activities.[1] As with many employee embezzlement schemes, the employee allegedly felt "invincible" after a short market upswing and believed he could profit in trading with the company's resources. Ultimately, the employee is alleged to have confessed to being a "degenerative gambler," and his activities led his company to suffer net losses valued at $603,000.

Given the recent volatility in cryptocurrency valuations (and human nature), other companies may find themselves discovering similar losses. For those companies, there is a key question they may face – is the loss of cryptocurrency covered by insurance?

Identifying the answer to this question must begin with the specific policy language. Often the first place an insured would look for coverage is under its commercial crime policy. These forms afford specified coverage for losses caused by "employee theft" or "computer fraud." Subject to the other policy terms, employee theft coverage is triggered for covered loss resulting directly from an unlawful taking by an employee. Likewise, and also subject to other terms, computer fraud coverage is triggered for covered loss resulting directly from the use of a computer to make fraudulent transfers. Cryptocurrency-related losses may fall within the purview of employee theft or computer fraud. But there remains a key limitation under commercial crime policies – coverage is often limited to loss of "money," "securities," or "other property," all of which are specifically defined. The key question insureds and insurers will face is whether cryptocurrency fits within any of these definitions. If cryptocurrency does not, there will be no coverage.

At the outset, we note that some policies now address this specific issue. For example, in 2015, the Insurance Services Office (ISO) made changes to its commercial crime program to address cryptocurrency. On these new forms, the ISO form contains a broad exclusion for "Loss involving virtual currency of any kind, by whatever name known, whether actual or fictitious, including, but not limited to, digital currency, crypto currency, or any other type of electronic currency." For insureds that deal in virtual currency, however, the new ISO form also contains an optional endorsement titled "Include Virtual Currency as Money." That endorsement provides specified coverage for cryptocurrency-related losses, and it addresses the thorny issue of cryptocurrency valuation.[2]

Not all crime forms now in use specifically address cryptocurrency, however. In these instances, the policy language must be carefully analyzed to determine whether cryptocurrency would be covered. As discussed below, there are serious questions as to whether cryptocurrency constitutes "money," "securities" or "other property" under commercial crime policy forms that are currently available. If it does not satisfy any of those definitions, coverage will be unavailable.

continued on page 16

[1] See United States v. Kim, No. 18-CR-107 (N.D. Ill.).

[2] The endorsement contains a schedule for the name of the cryptocurrency, the exchange for valuation, and the applicable sublimit. Loss is determined based on the market value on the date the loss was discovered.

"Money"

"Money" is defined in many crime forms to mean: "a. currency, coins and bank notes in current use and having a face value; and b. travelers checks, register checks and money orders held for sale to the public." Even assuming cryptocurrency could be a "currency" and is deemed "in use" (which is often not the case), it does not have a face value. It also is not a travelers check, register check or money order. Thus, under this definition, cryptocurrency losses may not satisfy a standard commercial crime policy's definition of "money."

"Securities"

The term "securities" is commonly defined in commercial crime forms to mean "negotiable and nonnegotiable instruments or contracts representing either 'money' or property and includes: a. tokens, tickets, revenue and other stamps (whether represented by actual stamps or unused value in a meter) in current use; and b. evidences of debt issued in connection with credit or charge cards, which cards are not issued by you; but does not include 'money.'"[3]

In unpacking this definition, it is useful to review the definition of "securities" under federal securities law. Specifically, Section 2(a)(1) of the Securities Act of 1933 contains a broad definition of "security" to include "any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement … *investment contract* … or, in general, any interest or instrument commonly known as a 'security', or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing" (emphasis added).

Whether cryptocurrency is a "security" under this statutory definition is a hotly debated issue. On the one hand, the U.S. Securities and Exchange Commission has taken the position that a cryptocurrency token is an "investment contract" and thus a "security" under federal securities laws.[4] For this reason, the SEC seeks to regulate initial coin offerings and other transactions in cryptocurrency. On the other hand, some commentators – including prominent Wall Street law firms – have analyzed the issue and determined that a cryptocurrency token may not be an "investment contract" and thus not a "security" in appropriate circumstances.[5] The analysis largely focuses on the nature of the token

continued on page 17

[3] An "instrument" is "a written legal document that defines rights, duties, entitlements, or liabilities, such as a statute, contract, will, promissory note, or share certificate." See Black's Law Dictionary (10th ed. 2014). A "negotiable instrument" means "an unconditional promise or order to pay a fixed amount of money, with or without interest or other charges described in the promise or order" but only when it meets certain conditions – such as being payable to the bearer or to order at the time it is issued or first comes into the possession of a holder. See U.C.C. § 3-104. A nonnegotiable instrument is a financial instrument that may not be transferred from the holder to another, such as a document of title. Cryptocurrency does not fit neatly into either of these categories, and instead the authorities seem to focus on whether a cryptocurrency token is an investment contract. For that reason, we will focus on that prong of the definition here.

[4] See, e.g., **here**.

[5] See, e.g., **here**.

continued from page 16

itself, which may vary across cryptocurrencies – making the issue even more complex.

Finally, a "token" under the crime policy definition is only a "security" if it represents either "money" or "property." (The "securities" definition does not include "money," but a contract or instrument still must represent "money" or "property" to fall within the "securities" definition). There are serious questions whether cryptocurrency could represent "money" (defined above) or "property" given its unique characteristics in how it functions, as well as its existence solely in intangible form in cyberspace.

"Other Property"

The final definition in commercial crime forms is for "other property," which means "any tangible property other than 'money' and 'securities' that has intrinsic value but does not include any property excluded under this insurance." Cryptocurrency is not "tangible property" because it cannot be touched; instead, it exists solely in virtual form.[6] As such, it does not satisfy this definition.[7]

Conclusion

Companies facing cryptocurrency losses may seek coverage under their commercial crime policies. While certain newer forms specifically address the issue, there may be debate over whether cryptocurrency is "money," "securities" or "other property" under traditional crime forms. The argument may focus on whether cryptocurrency is a "security," and that in turn may hinge on the specific currency at issue and surrounding facts. While the issue is untested in courts to date, the prevalence of cryptocurrency and potential for significant losses may lead to coverage litigation over whether those losses are covered as well as the development of new policy forms that may explicitly cover loss of cryptocurrency. ■

This article was originally published in Law360 and can be found **here**.

For more information, please contact:

Leland H. Jones IV
202.719.7178
lhjones@wileyrein.com

Edward R. Brown
202.719.7580
erbrown@wileyrein.com

Bonnie J. Thompson
202.719.3763
bthompson@wileyrein.com

[6] Cryptocurrency is considered "property" for United States federal tax purposes. State taxing authorities have treated it as intangible property. See, e.g., New York State Department of Taxation and Finance, Tax Department Policy on Transactions Using Convertible Virtual Currency (Dec. 5, 2014), available **here**.

[7] See, e.g., Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 96 (4th Cir. 2003) ("The insurance policy in this case covers liability for 'physical damage to tangible property,' not damage to data and software, i.e., the abstract ideas, logic, instructions, and information.").

DOJ's New Cyber Task Force Can Address IoT

By Megan L. Brown, Matthew J. Gardner, and Michael L. Diakiwski

On February 20, 2018, the Attorney General **announced the creation** of a Cyber-Digital Task Force within the U.S. Department of Justice (DOJ or Department). The Task Force will assess "the many ways that the Department is combatting the global cyber threat, and will also identify how federal law enforcement can more effectively accomplish its mission in this vital and evolving area." It will draw from numerous components across the Department and be managed by a chair appointed by the Deputy Attorney General, Rod Rosenstein.

Government task forces and blue-ribbon commissions are commonplace. History is littered with reports and white papers that do not inspire change. But, given the complexity and importance of cybersecurity, there is an opportunity for the DOJ to have an impact. It can identify legal obstacles to information sharing and deterrence, examine liability concerns, request more authorities and resources, and help the private sector address this unrelenting challenge. It should also focus on consolidating guidance and activity – its own and with other agencies – to reduce duplication, burdens, and confusion.

DOJ can move the needle on security by helping the private sector

The Task Force has a broad charge to assess and propose strategies that could affect nearly every corner of the digital ecosystem. In his Department Memorandum, the Attorney General noted, "[w]hile computers, smart devices, and other chip-enabled machines – as well as the networks that connect them – have enriched our lives and have driven our economy, the malign use of these technologies harms our government, victimizes consumers and businesses, and endangers public safety and national security."

Among many hot-button issues on the Task Force's agenda, it has been asked to review "the mass exploitation of computers, along with the weaponizing of everyday consumer devices (as well as of the very architecture of the Internet itself) to launch attacks on American citizens and businesses." This priority is particularly notable for technology and telecommunication companies, including manufacturers of Internet of Things (IoT) devices, software developers, and network providers.

DOJ will not be writing on a blank slate. It can use several existing recommendations to improve collaboration with the private sector and cyber policy. As the U.S. Department of Homeland Security said in its 2016 ***Strategic Principles for Securing the Internet of Things (IoT)***, "[p]olicymakers, legislators, and stakeholders need to consider ways to better incentivize efforts to enhance the security of IoT" by looking at "how tort liability, cyber insurance, legislation, regulation, voluntary certification management, standard-setting initiatives, voluntary industry-level initiatives, and other mechanisms could improve security" while encouraging economic activity and "groundbreaking innovation." Here are a few things DOJ can do now:

First, DOJ can examine and promote NSTAC recommendations. The President's National Security and Telecommunications Committee (NSTAC)'s recent ***Report to the President on Internet and Communications Resilience*** addressed several issues that the DOJ can advance. It recommended that the

continued on page 19

continued from page 18

"U.S. Government should increase incentives, particularly within DOJ, to make preventing cybercrime and disrupting botnets a higher priority …. The DOJ may need additional resources in order to increase these efforts which also are dependent upon collaboration with both the private sector and potential international partners."

The NSTAC called for a discussion about a possible policy framework to support future action against botnets. The government and private sector already do takedowns and use varied tools, but expanded "use of such tools raises policy issues. There are complex questions around 'active defense' and offensive cyber operations …. These issues require a joint discussion and planning among the U.S. Government, foreign partners, and industry."

The NSTAC identified the need for a policy framework if we are going to expect more of ISPs and network providers on filtering, port blocking, and rate limiting. "The NSTAC recognizes that there may be an opportunity to enhance these efforts, but it would require a partnership with the government to develop a policy framework supporting ISPs taking more aggressive actions to block and filter content."

Second, DOJ can inform and use the draft Botnet report to the President. In a draft ***Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats***, the Departments of Commerce and Homeland Security put forth a strategy. It proposed actions to address threats. But several commenters called for improvements, including to address barriers and liability concerns. For example:

- CTIA argued that "Information sharing, certification regimes, and labeling involve some risk related to public disclosure of sensitive information, responsibility, and liability … The Report should explicitly consider barriers."
- The U.S. Chamber of Commerce believes that "[i]ndustry and government should look for novel ways to limit liability for private entities that employ defensive measures in good faith."
- The Aviation Information Sharing and Analysis Center (ISAC) "recommend[s] consideration to limit liability to companies who make swift public disclosures of vulnerabilities and expeditiously issue patches. This will incentivize two key pillars in reducing cyber risk: The independent researchers will be motivated to continue notifying companies of coding errors. and companies will be incentivized to respond quickly."
- ACT | The App Association claims that "the existing information sharing environment remains vulnerable" and "[p] rivate sector entities may be reluctant to share this information amongst each other due to concerns about legal liability, antitrust violations, and potential misuse."

Whether or not the Report is adjusted to address these concerns, DOJ can tackle this issue to help move the discussion forward.

Finally, DOJ can help streamline and coordinate government efforts. DOJ itself has issued guidance on cyber topics – for example, in July 2017, ***A Framework for a Vulnerability Disclosure Program for Online Systems*** – that adds to a cacophony of other advice and resources about security

continued on page 20

continued from page 19

topics. From DHS to NIST, the FBI and the FTC, and with myriad private resources, it is time for a coordinated and streamlined approach to public education and awareness about cyber responsibility and risk. This is a central challenge of a 21st-century digital economy in which every person and thing will be connected; we have to educate responsible digital citizens.

DOJ can advance discussions about liability, incentives, ethical hacking, and protection of information, among others.

The time is right for this effort

This Task Force is being stood up against a background of concerns about election interference and the exploitation of social media. But in terms of policy, it makes sense to engage now, while we are at a cybersecurity inflection point, as numerous agency activities affecting cyber are in progress and taking shape. The proceedings identified above are just a few examples. Legislation is being proposed. Work is underway at NTIA, NIST, and elsewhere. From new DHS and State Department organizational changes to the release of the President's National Security Strategy, the cybersecurity challenge requires an "all hands" approach across the federal government.

A key figure on the DOJ Task Force will be John Demers, who was confirmed recently as the Assistant Attorney General for National Security. The National Security Division (NSD) already plays an important role in cyber activities, so the Task Force will benefit from its experience. The Criminal Division is also a key player, with its Computer Crime and Intellectual Property Section (CCIPS) able to offer insights about the scope of statutes like the Computer Fraud and Abuse Act, which some stakeholders want to amend, in order to promote ethical hacking.

DOJ has been vocal about the importance of cybersecurity. Over the past year, Deputy Attorney General Rod Rosenstein expressed concerns about the security of Internet of Things (IoT) devices and observed that innovation may outpace the law, raising public safety concerns. The Deputy Attorney General has also noted that public-private partnerships will be important to protect new technologies. Though encryption policy and debates continue, there are myriad ways for the private sector to work with the government on other areas of mutual interest.

Precisely how DOJ's Cyber-Digital Task Force will engage with the private sector, if at all, remains to be seen. Given the many interesting legal issues surrounding cybersecurity, combating threats, and supporting new technologies, this is an opportunity to do some good.

A report from the Task Force is due to the Attorney General by the end of June. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

Michael L. Diakiwski
202.719.4081
mdiakiwski@wileyrein.com

Events & Speeches

State of the Law and Enforcement
Megan L. Brown, Speaker
13th Annual FCBA/ABA Privacy and Data Security Symposium
March 20, 2018 | Washington, DC

Privacy Bootcamp
Kirk J. Nahra, Speaker
IAPP Global Privacy Summit 2018
March 26, 2018 | Washington, DC

HIPAA 2.0—Building Better Privacy and Security Rules
Kirk J. Nahra, Speaker
IAPP Global Privacy Summit 2018
March 27, 2018 | Washington, DC

Today's General Counsel Institute
Matthew J. Gardner, Co-Chair
Cybersecurity Conference
March 27-28, 2018 | San Francisco, CA

I'm a Lawyer: How Can I Advise on Data Security Issues?
Kirk J. Nahra, Co-Chair
IAPP Global Privacy Summit 2018
March 28, 2018 | San Francisco, CA

The Path Towards a New and Complete Consumer Health Regulatory Structure
Kirk J. Nahra, Speaker
Twenty-Seventh National HIPAA Summit
March 28, 2018 | Arlington, VA

Insurance Lifecycle of a Ransomware Attack
Edward R. Brown, Speaker
Litigation Conferences
April 10, 2018 | Webinar

Cybersecurity Summit
Megan L. Brown, Speaker
Greensboro Chamber of Commerce
April 10, 2018 | Greensboro, NC

Corporate Data Governance and GDPR Compliance for U.S. Companies
Kirk J. Nahra, Speaker
Strafford Publications
April 11, 2018 | Webinar

Wiley Rein Reception with HackerOne
RSA Conference
April 18, 2018 | San Francisco, CA

Today's General Counsel Institute
Matthew J. Gardner, Co-Chair
Cybersecurity Conference
April 24-25, 2018 | Boston, MA

Identifying, Understanding and Limiting Your Legal Vulnerabilities
Edward R. Brown, Speaker
Cyber Sector Risk Critical Infrastructure
April 25, 2018 | New York, NY

Events & Speeches

The Urgency of Cyber Threats to U.S. & Global Critical Infrastructures

Megan L. Brown, Speaker

Cyber Sector Risk Critical Infrastructure

April 25, 2018 | New York, NY

Privacy and Security Enforcement Highlights

Kirk J. Nahra, Speaker

Blue Cross Blue Shield Association National Summit

May 2018 | Orlando, FL

Top Ten Privacy and Security Developments for the Health Care Industry

Kirk J. Nahra, Speaker

Blue Cross Blue Shield Association National Summit

May 2018 | Orlando, FL

Contributing Authors

Edward R. Brown	202.719.7580	erbrown@wileyrein.com
Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Michael L. Diakiwski	202.719.4081	mdiakiwski@wileyrein.com
Shawn M. Donovan	202.719.7293	sdonovan@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@wileyrein.com
Leland H. Jones IV	202.719.7178	lhjones@wileyrein.com
John T. Lin	202.719.3570	jlin@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Bonnie J. Thompson	202.719.3763	bthompson@wileyrein.com