Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | June 2018

We have a particularly full issue this month. Our cybersecurity team looks at various recent developments, including the release of the highly anticipated Botnet Report. I then look at three unrelated but critical issues – including a summary of my Bloomberg Law panel on the recent GDPR deadline and its ongoing implications, some significant potential HIPAA revisions, and an analysis of the Eleventh Circuit's recent LabMD decision.

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. ■

Are HIPAA Changes Coming?

By Kirk J. Nahra

ALSO IN THIS ISSUE

While the health care industry continues to wonder what the enforcement philosophy and approach of the HHS Office for Civil Rights (OCR) will be under new leadership, there is now a likelihood that some elements of the HIPAA Rules will be undergoing change in the next few years, based on a series of upcoming rulemaking proceedings. At a minimum, we can expect several different rulemaking proposals over the course of 2018.

What Is Happening?

As part of a broader administrative document setting forth a broad regulatory agenda across the federal government, HHS has indicated an official intention to propose changes to several components of the HIPAA rules. This formal regulatory announcement follows various media reports of speeches by HHS leadership about these expected proposals.

continued on page 2

Kirk Nahra on: "Ready or Not, GDPR is Here."

The 2018 Bloomberg Law Leadership Forum, held May 23, included a panel discussion on the EU General Data Protection Regulation (GDPR), whose compliance date was May 25. Privacy & Cybersecurity Practice chair Kirk Nahra, together with other experienced compliance professionals, provided insights concerning the challenges posed by the far-reaching GPDR regime as enforcement begins. Bloomberg's video recording of the panel discussion is available **here**.

The perspectives shared by Mr. Nahra included the following:

Big Fine Potential

One of the things that's always interesting to watch is what gets people to pay attention to major compliance issues. Notably, most of GDPR is law that has been in effect for about the last 20 years under the European Privacy Directive. Lots of people didn't pay attention to it. It is crystal clear that the GDPR potential sanctions numbers are very big. If a privacy regulator in one of the European countries decides that you are going to be the test case, and that they're going to push the sanctions authority as far as they possibly can and do it as fast as they can, that will be a big problem.

Does anyone actually think that's going to happen? I have been astonished at how many people expect to get a call from the data protection regulators next week. I was at a conference a couple of weeks ago where one of the leading regulators

continued on page 5

Are HIPAA Changes Coming?

continued from page 1

The Accounting Rule

The most significant proposal involves the HIPAA accounting rule. The accounting rule has been one of the primary "individual rights" in the Privacy Rule since it first went into effect. As part of the HITECH statute, Congress directed that certain changes be made to the accounting rule, primarily to broaden the scope of the rule in connection with electronic health records. While the statutory language created meaningful concerns in the health care industry, these concerns exploded when HHS – in May of 2011 – issued a proposed rule on the accounting provisions. (It has never been fully explained why the accounting rule provisions have been on a separate time frame from most of the remainder of the HITECH changes.)

This proposal was met with widespread and virtually universal criticism. While there are a variety of reasons to criticize the NPRM proposal on the accounting rule, several key points stand out.

- The HHS proposal wildly misconstrued the state of feasible technology for tracking uses and disclosures of health care information, resulting in a proposal that was both not realistically feasible and exceedingly burdensome.
- HHS identified few specific patient interests that were furthered by the

continued on page 3

NPRM proposal, and the interests that were identified either are already addressed through privacy notices or are more appropriately and directly addressed by privacy investigations.

- HHS failed to assess the risks to health care company employees that would be created by providing information about them to patients, in addition to failing to analyze other unintended consequences of providing details about internal operations of health care facilities.
- HHS based many of its assumptions about technological feasibility on a misunderstanding of its own previous interpretations of the requirements of the HIPAA Security Rule.

As I said at the time:

> My conclusion is that this NPRM is fundamentally misguided and should be withdrawn – it relies on an unreasonable interpretation of the HIPAA Security Rule, fails to reflect the technological reality of today's health care environment, and mistakenly presumes (even if its assumptions were correct) that creation of this access report will impose little burden, all to support (in a surprisingly untargeted way) an ill-defined and relatively unjustifiable patient interest in learning specific details about the internal activities of health care companies. See generally, Nahra, "**The HIPAA Accounting NPRM and the Future of Health Care Privacy**," *BNA Health IT Law & Industry Report* (July 4, 2011).

Now, *seven years* after this proposal was issued, HHS is withdrawing the proposal. In its place, HHS will initiate a new "advanced notice of proposed rulemaking," to gather stakeholder input on how to move forward with the accounting rule. It will be critical for HIPAA-covered entities and business associates to carefully think through this issue so that they can help HHS get to a much more balanced approach on the HITECH requirements for the accounting rule.

In general, I encourage HHS to consider the following points:

- Any new changes to the accounting rule should be limited to "disclosures of PHI" for treatment, payment, and health care operations purposes that are made "through" an "electronic health record";
- "Electronic health records" should be limited to those electronic health records that incorporate "meaningful use" standards; and
- Any compliance period for this new requirement should be delayed until the meaningful use standards incorporate a corresponding requirement connected to this accounting rule change (to ensure that these obligations can be met through appropriate technology) and the implementation date for this new meaningful use standard is in place (with accounting obligations applying only to disclosures from that point in time forward).

Patient Privacy Notices

HHS also has indicated its intention to "change the requirement that health care providers make a good faith effort to obtain from individuals a written acknowledgment of receipt of the provider's notice of privacy practices, and if not obtained, to document its good faith efforts and the reason the acknowledgment was not obtained." While we have not yet seen a lot of discussion about the interests

continued on page 4

served by this proposal, HHS seems to be of the view that this obligation is burdensome for health care providers without much benefit for patients. While there are meaningful criticisms of the language of most privacy notices, it will be interesting to see how HHS removes this requirement while still making clear how individuals should receive these notices.

Individual Shares of Civil Penalties

HHS also has indicated that it will be issuing later this year an "advance notice of proposed rulemaking" requesting public input for how OCR may share funds collected from HIPAA enforcement actions with affected individuals. OMB says the notice "would solicit the public's views on establishing a methodology under which an individual who is harmed by an offense punishable under HIPAA may receive a percentage of any civil money penalty or monetary settlement collected with respect to the offense." This step also is required by the HITECH statute. However, despite this announcement, this step may still be a long time in coming. Not only is this an "advance notice" of proposed rulemaking – meaning that it is simply seeking information from which HHS might develop a future proposed rule – but OCR has announced similar plans 12 previous times, all without any actual activity. There is no obvious reason why this year should be any different.

This issue is a challenging one, and there is likely to be a lot of controversy about any proposal. Defining "harm" in the context of a regulatory enforcement proceeding is extremely difficult, and will put additional pressure on OCR's already tight resources. There also will be a concern from industry that this provision will lead to higher demands for monetary payments – to "compensate" these individuals while also permitting OCR to obtain significant amounts for its own purposes. In addition, as courts across the country continue to struggle with definitions of "harm" in class action litigation, there likely will be reasonable concerns that any OCR definition of harm will spill over to a litigation context.

Good Faith Sharing

The most abstract provision – and one not driven in any way by the HITECH statute – involves OCR's stated effort to "modify the HIPAA Privacy Rule to clarify that health care providers are presumed to be acting in the individual's best interests when they share information with an incapacitated patient's family members unless there is evidence that a provider has acted in bad faith." Presumably, this provision is driven by ongoing concerns about opioid abuse situations – which, on a broader level, is driving virtually all of the health care privacy debate at this time, particularly in Congress.

While the goal of this provision may make sense, it is not at all clear why it is needed. OCR clearly can (and usually has) taken this view in its enforcement efforts generally. It clearly has the ability to insulate providers from enforcement if they disclose in this context, and can change its approach if there is an indication of bad faith. So, until we see a proposed rule, it is hard to understand what this provision will do beyond setting into the rule current enforcement discretion, and it will be interesting to watch whether this provision "flips the burden" for OCR in enforcement settings, where they will be required to show bad faith before taking enforcement action.

Conclusions

The health care industry likely will see a flurry of these proposals over the course of the next year. Most of these proposals seem to be at the "advance notice" stage, indicating that any

continued on page 5

Are HIPAA Changes Coming?
continued from page 4

meaningful implementation of new rules is still a long way off. However, particularly for the accounting rule, it will be important for the industry to think carefully about how best to engage in this dialogue, since these provisions may require significant resources for the industry to implement. ■

For more information, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

Kirk Nahra on: "Ready or Not, GDPR is Here."
continued from page 2

was asked whether there was going to be a grace period for GDPR compliance, and her response was, "Well it goes into effect on Friday, I doubt we'll do anything until Monday." But, at the same time, there are not 50,000 privacy regulators who have nothing else to do but go out and do enforcement on Monday.

It's been intriguing, even over that last couple of days, to see how many companies are sending out hundreds of contracts and saying they need to be signed by Monday. Such behavior is driving a lot of the activity as well. So, the combination of these events, with sanctions a big piece of it, has led a lot of people actually to pay attention to compliance. Do I expect everyone's going to be ready to go on Friday? No. Is that a major problem for everybody? No. I have been telling my clients: "There is lots of low-hanging fruit; your job is not to be low-hanging fruit."

I want you to be trying to be compliant. If a regulator calls you on Monday and you say, "What's GDPR?," that's a problem. But, they're certainly not going to call some random company somewhere just because. You want to avoid having a big obvious problem. You want to be moving towards progress. You want to be paying attention to what regulators seem to be doing, and what they care about. If we did a poll in this room on who are the top five companies that are going to be the first to be investigated by the GDPR regulators, we would name at least three or four of them correctly. So that's a lot of it. And every regulator that I've ever dealt with has wanted to know you are trying. It is possible these GDPR regulators are going to say, "I can fine you 4%, I'm going to be ridiculously aggressive as to every company that's ever talked to a person in Europe." I just don't expect that to happen.

I have had several different clients in the last couple of weeks whose consultants have told them that because their website was accessible to somebody in Europe, they are covered by GDPR. That is not true. Let me be clear about that. You are not subject to GDPR just because somebody from Europe could find your company on the web. Big point. Lots of people actually are not covered by GDPR requirements.

In the U.S., we have sector-specific privacy regulation. I've long dealt with the HIPAA Act and HIPAA rules for the health care industry. HIPAA enforcement regulators went out of their way at the beginning to make clear to the health care industry that they weren't going to be very aggressive about sanctions. The

continued on page 6

continued from page 5

regulators were concerned that if they were too aggressive in how they enforced the laws, people would stop sharing information, and that would actually be bad for patients. So, they went out of their way to say, "Look, we're going to try to fix your problems; we're going to try to help you; we're going to guide you; we're going to educate you." They were very clear that they were not going to do aggressive enforcement. That went on for several years, and it really let the health care industry work their way through it. One could debate whether that enforcement approach continued too long, but it was a smart thing to do at the beginning.

It is interesting that GDPR enforcers recently have been speaking in the newspapers. What we've had historically is the newspapers first, and the enforcement, if it's going to happen at all, being way down the road. That's true in the U.S. with virtually everything. It has been true in the EU to the extent that there has been enforcement, and so companies have been driven by things that are not enforcement. That is why the data breach issues are so important. Breaches cause a lot of underlying conditions to become visible and become public issues. If you are disclosing a customer list to somebody that you shouldn't be disclosing it to, people often don't know that. If they get another piece of junk mail, they may not care about that much. But data breaches are where these things started to become meaningful and then there was publicity on top of it. Again, all that publicity has been well in advance of the regulators doing anything. Particularly in the United States, if you look at the health care data breaches posted by HHS, only about 5% of them ever led to enforcement action. So we can talk a lot about the potential sanctions and we can talk about the formal enforcement process, but much of the impact of these problems typically has already happened by the time the regulators get involved.

The Basic Compliance Challenge

It is important to understand that GDPR is basically a regulatory modernization, responding to all the technological developments that have happened in the last 20 years. More and more companies have data opportunities because of the data that is out there. What GDPR is trying to do is rein in a little bit of that activity. It's going to force companies to be very thoughtful about what they are doing. I don't think GDPR is saying you can't do analytics in the future, you can't take advantage of the Internet of Things, or you can't gather all the data that's available to you. It's not going to make big data disappear. None of those things is going to happen, but companies do have to go into the GDPR era thinking about what they want to do with their data. They need to have a strategy about what they're doing. A lot of companies, over the last 10 or 15 years, as data opportunities have multiplied, have been gathering up stuff just because it was out there, without really having any idea of why they wanted it or what they were going to do with it. One of the real challenges, over the next decade, is to figure out what we can actually do with data that exists: Why do we want it? What is it going to show? GDPR is going to help build a legal structure around that learning. How companies are going to work with that is going to take a lot of thought on what they actually want to do, what they need to be able to do, what do they need in order to be able to accomplish their goals. Then they are going to back into developing their legal structure that is going to govern some of those activities. GDPR is

continued on page 7

continued from page 6

going to push companies to be more strategic about their data analytics activities.

The amount of work depends on what your starting point is. In the United States, regulated industries such as the health care companies and the financial services companies have a history. And a lot of the tech companies, even though they're not regulated in quite the same way, have a real history. If you had built a really strong privacy program for a big company over the years, the evolution to GDPR was incremental. There are some important elements that you would have to address, but again, it's not like starting from scratch. I have clients who have been working on this nonstop for two years. Lots of companies that should be paying attention to GDPR implementation have been paying attention. However, there are certainly some companies that haven't been previously regulated, don't have financial or health care data, but just have regular kinds of marketing data that Internet companies collect. GDPR is an eye opener for them.

One thing that I've seen, even with some companies that have a very good history, is that when they've really done a thorough GDPR compliance approach, they have found new kinds of data and new uses for data that they had not previously recognized were present in their company. All of these companies are hiring data analytics people and they're gathering data from all kinds of places, and that had not necessarily filtered down to the privacy controls, so there were some gaps that people were unaware of, even where they had very sophisticated programs.

Potential U.S. Responses

It's going to be interesting to watch two different potential effects of GDPR, as applied to the U.S. First, from a regulatory perspective, is GDPR going to lead to anything similar here? I have said for years that the sectorial approach is very confusing. Frankly, I have a job because it's so confusing. But if they were to put me in charge, I would pass one law that would cover everybody. However, I see virtually no movement towards that politically in the United States. It's just not where we are going.

The second potential effect, which is likely to be more important, is whether companies start behaving like GDPR is worldwide law. We've seen a lot of discussion with the most prominent companies, Facebook being a perfect example, where they are under a lot of pressure to agree to implement GDPR essentially on a global basis. We may see small, medium, or large companies basically saying it's better for us to build a one-size-fits-all privacy operation for our company, and asking whether they are going to use GDPR as the model. I will be curious as to how much that is going to come into play. I will be curious whether particular companies undertake to operationalize GDPR globally. I am not sure a company would ever say it is following GDPR everywhere, because that makes it enforceable. The Federal Trade Commission could go after the company if it said it was complying with GDPR but was not. Watching whether companies try to make a one-size-fits-all process for their company is going to be a really interesting issue over the next few years.

I see three categories of laws in the area we are discussing. First, there are privacy kinds of laws, which is what we've been focusing our attention on. There also are data security laws, which are related but reflect a really different kind of idea. Then we have the data breach kinds of laws. The privacy laws are the ones

continued on page 8

continued from page 7

where it probably makes the least sense to try a one-size-fits-all integrated approach. Part of the reason is that you have many different roles for data. A vendor has to deal with all different kinds of rules from different customers and different roles that it is playing with each of its different customers. So, it is very hard to try to build a single privacy framework. Obviously the GDPR tries to do that, which is why we are all spending so much time on this these days. It is not simple to say, here is a rule that's going to fit you the same way it's going to fit everyone else. I would have one standard for data security. I think it's harder to come up with such rules on the privacy side, because people use data for so many different purposes. That's also the reason we are seeing the reluctance of the U.S. government to regulate in a way that will impede innovation, because the amount of innovation we're seen with data even the past couple of years is astonishing. I think U.S. regulators are really hesitant to be too invasive.

For security, by contrast, I foresee companies trying to build a one-size-fits-all, because you don't have a European computer system and an American computer system. You don't have a health care computer system and a financial services computer system. You have one computer system for the most part. And so, I think it makes a lot of sense to try to build a consistent framework for data security. Data breaches are somewhat similar in that they are not usually in conflict, but there is some real tension among the different state laws in particular. I would very much like to see a single data breach notice approach.

I think the EU 72-hour approach is going to be very challenging and very disruptive, because of the immediacy of the notice. In United States data breaches, we focus first on the individual and then on the regulator. EU flips it; they say focus on the regulator first, and then focus on the individual later. I don't particularly like that approach and it's going to be really interesting to watch.

I don't like the GDPR breach reporting time frames very much. The idea of saying every breach makes sense to report in 72 hours is ludicrous. If the breach you have is a simple lost laptop, report that. However, the Equifax breach was a perfect example of a situation where they were under pressure to get notice out and they got a couple of things wrong in the race to do that. It almost made things worse for everybody. That's not a good thing. I think we're going to see a ton of that with the 72-hour reports. Moreover, companies who use contractors are writing into their contracts requirements to inform them about a breach in a "minute and a half." As soon as I, as a contractor, agree to a minute and a half with you, it has got to be "30 seconds" for the next person downstream. That just doesn't work. I would have no problem with a consistent framework, I just don't want that consistent framework to be 72 hours, and I don't want it to be something where you've got to have a series of upstream reports in that 72 hours.

In the Medicare program, they have pushed back on this. For a while, the Medicare program was requiring two-hour reporting. So everybody who had a contract with anybody who was involved in the Medicare program had to report in less than two hours. They realized that was sort of ridiculous and they pulled back on it.

All of these things are going to have to play out in GDPR. This morning there was an extensive dialogue on one of the list serves I was reading. People were asking what's going to

continued on page 9

continued from page 8

happen if I'm not in full compliance on May 25? Short answer, nothing's going to happen as long as you don't have a major breach on May 26. Even if you do have a major breach, you're going to have to do deal with the major breach whether it's for GDPR reasons or otherwise. We are five or ten years away from having a fully evolved system. In the HIPAA system, back in 2003, companies had very little idea what they were doing. And the number of problems that came up right away was very significant. By now, however, people have worked their way through it for the most part. So we generally are comfortable with HIPAA. If you took a poll of the people in the health care industry on whether they would rather have HIPAA or what's behind door No. 2, they would take HIPAA every time. The challenge we are seeing in the health care industry is the large amount of health care data that HIPAA doesn't cover. That's the real challenge we're seeing in that industry. Now GDPR avoids that by saying it is going to cover everything no matter who has the data. In the U.S., because the definition of health care doesn't really fit the reality of today, we've got a significant gap that we haven't filled. ■

Kirk Nahra may be reached at:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

Information Sharing, Incident Response, and Mitigating Threats to the Supply Chain: Wiley Rein Hosts DHS Panel on Cybersecurity

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

On June 6, 2018, Wiley Rein LLP hosted clients and other interested parties to learn more about the U.S. Department of Homeland Security's (DHS or Department) cybersecurity initiatives and priorities. This is part of the firm's ongoing Outlook on Cyber **series**, which brings government and the private sector together to talk cyber.

Senior lawyers from DHS's National Protection and Programs Directorate, and the head of International Strategic Affairs in the Office of Cybersecurity and Communications, touched on agency cybersecurity authorities, information sharing structures, engagement with the private sector on incident response and system analysis, supply chain considerations including the Internet of Things (IoT), and collaboration with international partners. Wiley Rein lawyers Megan Brown and Matt Gardner moderated the discussion.

The Department is a key federal entity when it comes to cybersecurity and engaging the private sector. DHS, with the U.S. Department of Commerce, recently published several major reports in response to Executive Order (E.O.) 13800, "**Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure**." The highly anticipated ***Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated***, Distributed Threats (Botnet Report) released

continued on page 10

continued from page 9

in May aims to combat botnets by focusing on six principle themes and five goals. Each goal includes several action items, with a heavy emphasis on private sector activity and accountability. The Botnet Report includes a section on next steps for stakeholder action, which calls for the development of a road map with government, industry, civil society, and international partner coordination, and a "status update that will evaluate the level of progress made by stakeholders in countering automated, distributed threats."

The E.O. also tasked the agencies with supporting greater transparency in the marketplace related to cybersecurity, specifically with publicly traded critical infrastructure entities. The summary of the report on ***Supporting Transparency in the Marketplace***, (1) identifies existing federal policies and practices; and (2) identifies and reviews third-party evaluations of transparency practices and systems from independent sources. DHS notes that due to the short time frame for the report, there was "limited private industry engagement." The report also makes suggestions for further research and policy considerations.

DHS also produced, along with the U.S. Departments of Defense, Justice, and others, a report impacting critical infrastructure operators (*see* the ***Support to Critical Infrastructure at Greatest Risk ("Section 9 Report") Summary***) and, with the U.S. Department of Energy, a report impacting operators within the energy sector (*see* ***Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities***).

Beyond these latest initiatives, DHS Secretary Kirstjen Nielsen **announced** "a voluntary initiative to identify and mitigate systemic risk in supply chains," in which DHS will work with "users, buyers, tech manufacturers, and others to hunt down unseen security gaps – and to share actionable information that will help close them. This includes identifying companies in the supply chain whose risks might go unnoticed." One recent, and very public, example of DHS managing threats identified in the supply chain was the **issuance of a Binding Operational Directive**, requiring federal agencies to remove and discontinue use of Kaspersky Lab products and solutions. In related litigation, on May 30, a federal judge **ruled in favor** of the United States in this matter.

As we have noted several times, these initiatives have **significant implications** for many stakeholders. The recent reports and recommended follow-on actions amplify calls for greater public-private partnerships, cooperation on vulnerability disclosure and information sharing, and the implementation of thorough and thoughtful supply chain management programs. ■

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

Cyber Reports Directed by the 2017 Executive Order on Cybersecurity Are Rolling In

By Megan L. Brown, Kathleen E. Scott, Michael L. Diakiwski

The President's May 11, 2017 Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," required a number of reports and assessments to be submitted by government agencies. A year later, several key reports have been released in full or in summary form – many, like the Botnet Report, being churned out in May. Below we provide a high-level overview of some of the major reports, which could alter how the U.S. government handles cybersecurity issues and raise expectations for the private sector.

- **International Engagement and Deterrence Reports:** The U.S. Department of State released summaries of two reports that may alter how the U.S. government handles international engagement and state-sponsored adversaries. First, in *Recommendations to the President on Protecting American Cyber Interests through International Engagement*, the State Department outlines a strategy that "advances the goal of strengthening coordinated U.S. government cooperation with foreign partners and allies to address shared threats in cyberspace, thereby improving the cybersecurity of the nation. It describes the United States' priority policies, five primary objectives and corresponding actions, and three principal means of engagement to ensure continued benefits and minimized risks in cyberspace." Second, in *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*, the State Department "suggests a new U.S. vision to help guide efforts to deter adversaries and better protect the American people from cyber threats and recommends follow-on work aimed at advancing these efforts; the following unclassified overview touches on these efforts in brief, which have been ongoing."
- **Transparency in the Marketplace Report:** The U.S. Department of Commerce ("Commerce") and the U.S. Department of Homeland Security (DHS) were tasked with developing supporting transparency related to cybersecurity matters in the marketplace, specifically for publicly traded critical infrastructure entities. The summary of the report on *Supporting Transparency in the Marketplace*, which was released this May, (1) identifies existing federal policies and practices; and (2) identifies and reviews third-party evaluations of transparency practices and systems from independent sources. DHS notes that due to the short time frame for the report, there was "limited private industry engagement." The report also makes suggestions for further research and policy consideration.
- **Botnet Report:** The highly anticipated *Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (Botnet Report), released by Commerce and DHS in May, aims to combat botnets by focusing on six principle themes and five goals. Each goal includes several action items, with a heavy emphasis on private sector activity and

continued on page 12

continued from page 11

accountability. The Botnet Report includes a section on next steps for stakeholder action, which calls for the development of a road map with government, industry, civil society, and international partner coordination, and a "status update that will evaluate the level of progress made by stakeholders in countering automated, distributed threats." The actions called for in the Botnet Report are discussed in a companion story appearing in this issue of *Privacy in Focus*.

- **Cyber Workforce Report:** DHS and Commerce also issued *Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future*. This report assesses the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, finding that the U.S. "needs immediate and sustained improvements in its cybersecurity workforce situation." Key recommendations include increased focus on developing the American cybersecurity workforce with greater collaboration between the public and private sectors.
- **Section 9 Report:** DHS released a *Support to Critical Infrastructure at Greatest Risk ("Section 9 Report") Summary*, which it prepared in consultation with the Departments of Defense, Justice, and others. The report focuses on supporting critical infrastructure at greatest risk. It sets forth several findings and recommendations for better supporting these Section 9 entities relating to cyber risk management.
- **Federal Risk Report:** Also in May, the Office of Management and Budget published a *Federal Cybersecurity Risk Determination Report and Action Plan*, which reviews cybersecurity risk management capabilities across federal agencies. It finds nearly three-quarters of the 96 participating agencies are "At Risk" or "High Risk" regarding their ability to detect and respond to cyberattacks.
- **Electricity Report:** In another report called for by the Executive Order, the U.S. Department of Energy and DHS (1) identified "known capability gaps" in critical infrastructure sectors' ability to respond to cyber incidents; and (2) proposed "recommendations to address major gaps and accelerate the adoption of cybersecurity measures in the electricity subsector." The report, *Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities*, is dated in 2017 but was posted to agency websites on May 30, 2018.

These latest initiatives have significant implications for many stakeholders. For private industry, this includes network owners and operators, software designers, cloud computing companies, hardware and device manufacturers, and others. These reports amplify calls for more public-private partnerships, sustained engagement, possible certification or standards regimes, supply chain and procurement mandates, the possibility of regulation, and greater international coordination.■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Kathleen E. Scott
202.719.7577
kscott@wileyrein.com

Michael L. Diakiwski
202.719.4081
mdiakiwski@wileyrein.com

Highly Anticipated Botnet Report Finally Released

By Megan L. Brown, Kathleen E. Scott, Michael L. Diakiwski

On May 30, 2018, the U.S. Departments of Commerce and Homeland Security released the final *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (Botnet Report or Report). This builds on a draft report released on January 5, 2018, and responds to the President's May 11, 2017 Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Comments were taken on the draft report from 49 filers, and the National Telecommunications and Information Administration (NTIA) held workshops on the topic.

In general, the Report aims to combat botnets by focusing on six principle themes and five goals. Each goal includes several action items, with a heavy emphasis on private sector activity and accountability. The Report includes a section on next steps for stakeholder action, which calls for the development of a road map with government, industry, civil society, and international partner coordination, and a "status update that will evaluate the level of progress made by stakeholders in countering automated, distributed threats."

The final Report expands on its discussion of liability as a potential barrier to productive action and information sharing, and calls for more work on that issue. And it emphasizes the global nature of the botnet challenge, calling for more international engagement by industry and the government.

This Report will set in motion additional work across government and the private sector if its recommendations and goals are taken seriously. There remains much work to be done on automated, distributed threats, because the problem cannot be solved by domestic regulation or one technological solution.

The Report describes the complex threat landscape, noting ongoing activity by ISPs and others, but indicates more needs to be done.

Highlighting recent distributed denial-of-service (DDoS) and other major attacks, the Report analyzes the global landscape. It identifies six core themes:

- Automated, distributed attacks are a global problem.
- Effective tools exist, but are not widely used.
- Products should be secured during all stages of the lifecycle.
- Awareness and education are needed.
- Market incentives should be more effectively aligned.
- Automated, distributed attacks are an ecosystem-wide challenge.

The Report analyzes the ecosystem: infrastructure, enterprise networks, edge devices, and home and small business networks. Notably, it raises concerns about enterprise networks, finding that "[m]any at-risk enterprises are unaware of the potential impacts of DDoS attacks on their operations" and that many may not understand their Internet service contracts or use available DDoS mitigations. The Report calls for more widespread enterprise use of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, as well as for consumer

continued on page 14

education and for edge devices to be designed more securely.

The Report also looks at governance, policy, and coordination. Although coordination does take place across sectors, countries, and between industry and law enforcement, the Report suggests much more can be done. Looking ahead, the Report presents "Visions" in which purchasers are aware of basic security properties of connected devices, information is better shared and analyzed, and cooperation is more inclusive, occurring across sectors, agencies, and countries.

Specifically, the Report emphasizes the need for industry-led approaches and consensus-based standards. Yet in its "Vision for the Future of Edge Devices" section, the Report states: "Devices must be able to resist attacks throughout their deployment lifecycles – at the time of shipment, during use, and through to end-of-life. For this to occur, security must become a primary design requirement." "Requirement" was changed from "goal" in the draft. It also states that the U.S. government and international partners should conduct their technology and device procurement actions to create market incentives for more secure products, and promote open, voluntary, industry-driven standards. It further emphasizes the need for the U.S. to engage with other countries. Finally, the Report calls for more coordination between industry and law enforcement.

The Report calls for 24 "actions" that promote ongoing discussions in Congress, DHS, NIST, and NTIA.

In its Goals and Actions section, the Report enumerates five goals. For each goal, the Report suggests activities for the government and private sector. NIST receives many assignments. Regulators and the Federal Trade Commission (FTC) receive praise for their work on Internet of Things (IoT) security, as the Report says "[c]areful enforcement actions can benefit consumers and honest participants in the market."

While there is emphasis on the voluntary nature of many actions directed at the private sector, companies can expect additional scrutiny and demands. The Report's emphasis on several topics dovetails with efforts underway, including the IoT Cybersecurity legislation championed by Sens. Mark Warner (D-VA) and Cory Gardner (R-CO) and an expected NTIA effort on software assurance (see Action 1.3).

The Report calls for work on topics ranging from device labeling to increased engagement with "operational technology" companies. It also suggests mandates related to government procurement, and calls for standards that will impact industry broadly across the IoT and connected-device ecosystem, from software and product developers to Internet service providers (ISPs) and network carriers.

Goal 1: Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace. The Report calls for "market incentives [to] encourage manufacturers to feature security innovations as a balanced complement to functionality and performance." It notes that "Publishing documents is not enough," the "IoT community must work collaboratively to identify and adopt existing best practices, frameworks, and guidelines[.]" This section calls for:

- Establishing accepted baseline security profiles for IoT devices in home and industrial applications, to be promoted by device labeling, bilateral arrangements, and the use of international standards (Action 1.1). The Report calls for collaborative development of "performance-based security

continued on page 15

profiles appropriate capability baselines – which identify suites of voluntary standards, specifications, and security mechanisms that represent the combination of best practices for home and industrial applications of IoT lifecycle security for a particular threat environment[.]"

- The government should then "leverage industry-developed capability baselines, where appropriate, in establishing capability baselines for IoT devices in U.S. government environments to meet federal security requirements, promote adoption of industry-led baselines, and accelerate international standardization." (Action 1.2)
- Reducing security vulnerabilities in commercial-off-the-shelf software. "NTIA should engage diverse stakeholders in examining the strategies and policies necessary to foster a marketplace for greater software component transparency, including identifying and exploring market and other barriers that may inhibit progress in this space." (Action 1.3)
- Expediting the development and deployment of technologies to prevent and mitigate distributed threats, including through "targeted [federal] funding and collaborative technology transition activities." (Action 1.4)
- Government, industry, and civil society collaboration to ensure adoption of best practices in the IoT ecosystem (Action 1.5), with a focus on NTIA. The Report cites NTIA's multistakeholder process on IoT Security Upgradability and Patching, but notes that broader adoption and promotion of best practices, frameworks, and guidelines is essential.

Goal 2: Promote innovation in infrastructure for dynamic adaptation to evolving threats. This section seeks to establish "a more resilient Internet and communications ecosystem, standards and practices that deter, prevent, and/or mitigate botnets and distributed threats should be continually implemented and upgraded in all domains...." The Report notes that "[w]hile network providers cannot be expected to serve as traffic cops and identify all bad packets, both common and newer tools and practices can help filter out some types of bad traffic." Potential solutions cited include "inter-autonomous system, internetwork peering, and transit agreements [which] might improve traffic management accountability." Action items call for:

- ISPs to expand information sharing (Action 2.1) by "work[ing] collaboratively with civil society and government to improve coordinated responses to actionable information and lead the development, refinement, and standardization of information sharing protocols to increase speed and permit automated response. Special attention should be given to engagement and inclusion of smaller ISPs and protocol developments that enhance their participation." The Report identifies the Comm-ISAC as a key venue and expanding information sharing agreements with international peers as an additional enhancement.
- The development of a Cybersecurity Framework Profile for Enterprise DDoS Prevention and Mitigation (Action 2.2). "An industry-led effort, in consultation with NIST, academia, and other subject matter experts, should develop a CSF Profile for Enterprise DDoS Prevention and Mitigation, focusing on the desired state of organizational cybersecurity to mitigate DDoS attacks,"

continued on page 16

citing Comments from the Coalition for Cybersecurity Policy and Law.

- The federal government to create greater market incentives (Action 2.3), by looking at "effective ways to incentivize the use of software development tools and processes that significantly reduce the incidence of security vulnerabilities in all federal software procurements, such as through attestation or certification requirements."
- Industry, government, and civil society organizations to collaborate with stakeholders to enhance and standardize information-sharing protocols (Action 2.4). The Report recognizes that small businesses "do not contribute to or benefit from most current information-sharing arrangements."
- U.S. and global infrastructure providers to work together to expand best practices on network traffic management across the ecosystem (Action 2.5). The Report calls for a "broad coalition of domestic and international experts – industry, academia, civil society, and government – [to] examine the extent to which inter-autonomous system, internetwork peering, and transit agreements might improve traffic management accountability – for instance, as applied to anti-spoofing and filtering."

Goal 3: Promote innovation at the edge of the network to prevent, detect, and mitigate automated, distributed attacks. This section identifies actions stakeholders can take to manage the impact of compromised IoT devices. Actions call on:

- Industry to expand current product development and standardization efforts for effective and secure traffic management in home and enterprise environments (Action 3.1).
- Industry to design user interfaces on home IT and IoT to be used securely and privately (Action 3.2).
- Industry to migrate to network architectures with better defenses and consider how their own networks put others at risk (Action 3.3).
- Government to investigate how wider IPv6 deployment can alter the ecosystem (Action 3.4). The Report expects that "As we transition to IPv6, consumer ISPs may be better positioned to observe device-specific misbehavior when IPv6 addresses are not subjected to NAT. This information can, in turn, map to other edge-focused solutions."

Goal 4: Promote and support coalitions between the security, infrastructure, and operation technology communities domestically and around the world. The Report notes that no stakeholder can address this issue alone and calls for actions that "cross geopolitical, public-private, industrial sector, and technical boundaries." It hits several topics that may give the communications sector pause. Seemingly sensitive to challenges posed by shifting international requirements, it calls for governments to "work with private-sector entities responsible for compliance with data privacy protection regulations, as well as with those entities involved in botnet investigatory work, to ensure that both equities are preserved (compliance and botnet investigations)." It does not state that global privacy and security regimes may impede botnet mitigations or offer solutions.

The Report also paints a rosy picture of the government's approach to victim companies. It states that "law enforcement treats companies that have suffered an intrusion or distributed attack as victims of a crime, and conducts their investigations of such reported crimes with discretion to avoid the unwarranted release of information concerning the incident, whenever

continued on page 17

possible." It does not call for more protections for victimized companies, nor does it address the potential backlash against companies cooperating with the government. The Report calls for several actions that would impact the private sector:

- ISPs and enterprises should increase information sharing with law enforcement (Action 4.1). The Report calls for "[l]aw enforcement [to] proactively identify what kinds of data will help them investigate and prosecute bad actors, and work with infrastructure providers to make it cheaper and easier to share this information with government while protecting Internet user privacy."
- The federal government should promote international adoption of best practices, including through NTIA leadership on global DNS security work (Action 4.2).
- Sector-specific regulatory agencies should engage industry to ensure nondeceptive marketing and "foster appropriate sector-specific considerations" (Action 4.3). This section touts FTC activity and its unfairness authority under Section 5. These efforts, with sector-specific enforcement, "can contribute to, and benefit from, the broader ecosystem security discussion." It is not clear what this means, but the Report may be suggesting a reexamination of some agency efforts.
- Community should identify leverage points and disrupt attacker tools and incentives (Action 4.4). The Report states that "Many threats stem from asymmetries that favor attackers by distributing the exploitation across diffuse actors in the ecosystem [and i]n some cases, relatively light coordination efforts should be able to disrupt broader attack classes."
- Engagement with the operational technology community to accelerate cybersecurity (Action 4.5).

Goal 5: Increase awareness and education across the ecosystem. This section identifies actions to "close gaps between current skills and responsibilities." Many of these actions veer toward certifications, disclosures, and labeling. This section calls for several Actions:

- The private sector should "establish and administer voluntary information tools for home IoT devices" (Action 5.1) because the Report finds that "[i]n an ideal world, consumers would prefer IoT products that also protect their security and privacy, but security-conscious consumers cannot easily identify which IoT products were designed to be secure." This Action would include "consumer-oriented testing organizations."
- The private sector should "establish voluntary labeling schemes for industrial IoT applications" (Action 5.2). "The private sector should establish an efficient but robust evaluation process to ensure that IoT devices for these sectors offer enhanced resilience at an appropriate level of assurance."
- Government should encourage the academic and training sectors to integrate secure coding practices into computer science and related programs (Action 5.3).
- The academic sector, in collaboration with NIST's National Initiative for Cybersecurity Education, should establish cybersecurity as a requirement across all engineering disciplines (Acton 5.4).
- Government should lead a public awareness campaign to "support recognition and adoption of the home IoT device security

continued on page 18

baseline and branding" (Action 5.5).

The Report calls for many efforts that will impact the private sector.

As is highlighted in the suggested actions for private sector stakeholders, the Report has implications for industry. It calls for public-private partnerships, greater engagement with and from a variety of stakeholders, certifications, standards, procurement mandates, a multistakeholder process "to explore requirements for a viable labeling approach," the possibility of regulation, and international coordination. It tasks industry with enhancing security in several areas, increasing accountability, and network activity. Topics include software and product development, accounting for activity on networks, working more closely with agencies, regulators, and other stakeholders, and assisting with the creation of a new Cybersecurity Framework Profile for Enterprise DDoS Prevention and Mitigation, among others. The Report notes private sector concerns about legal risks and uncertainties, as raised by CTIA in its comments. The final report expands upon this commentary in the draft, noting that a balanced approach must be taken:

> "Some stakeholders noted that any new legal or regulatory regimes may have unintended negative impacts on the IT industry if clear guidance is not included regarding what a vendor can do to limit its exposure. However, advocates caution against blanket liability protections without clear social gains from improved security processes. Some stakeholders, including civil society organizations, called for additional clarity regarding how existing laws in various jurisdictions apply in this area, how these laws can or should affect different stakeholders along the supply and distribution chains, and how to properly address harms. As this area continues to evolve, it is vital that the federal government better understand the interaction between liability and market incentives, as well as how any proposed changes might alter that dynamic. Care must be taken to ensure that our liability laws benefit consumers, protect stakeholders when appropriate, and avoid chilling innovation in today's digital environment. As public-private sector collaboration in this area continues, the federal government should continue to monitor whether protection from liability related to information sharing is sufficient in today's environment to effectively address ongoing and new threats."

Next Steps

While the Report is in its final form, the government plans to continue collaborative work on this effort. Within 120 days, the Departments of Commerce and Homeland Security, in coordination with industry and civil society, and in consultation with international partners, will develop an initial road map for prioritized actions. "Government and the private sector will work together to ensure that the road map is updated and maintained as stakeholders accomplish the identified actions." Further, in one year, a status report will be provided to the President, tracking progress made by the "community as a whole" against the road map on the implementation of the recommendations found in the Report.

The Report and plan for continued action come amidst several ongoing efforts on the Internet of Things and overall Internet resiliency.

continued on page 19

The Report addresses risks from botnets and automated, distributed attacks, which can be launched using IoT devices that are vulnerable, either due to lack of basic security configurations at the time of manufacture, or from failures to update or patch devices. Several efforts are underway to address security in the increasing array of connected devices that will up the IoT.

- NIST has numerous workstreams on IoT, with dozens listed, including efforts to map international standards in NISTIR 8200, the Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT), and to develop a draft document identifying security and privacy considerations for IoT.
- The Department of Homeland Security addressed "Strategic Principles for Securing the Internet of Things (IoT)" and is expected soon to release a cybersecurity strategy that will include connected devices. As Secretary Nielsen told the RSA Cybersecurity Conference in March 2018, "the proliferation of Internet-connected devices – which make our lives easier, and in some cases more fun – have also made it easier to attack us."
- The U.S. Food and Drug Administration has issued guidelines and developed a Medical Device Safety Action Plan to enhance connected device security.
- The Department of Justice has issued IoT guidelines with the Consumer Technology Association, and it may address cybersecurity and botnets in the report to be developed by its Cyber-Digital Task Force.
- The National Highway Traffic Safety Administration (NHTSA) is actively engaged in automotive security related to connected vehicles.
- The U.S. Consumer Product Safety Commission is looking at possible hazards from connected devices. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Kathleen E. Scott
202.719.7577
kscott@wileyrein.com

Michael L. Diakiwski
202.719.4081
mdiakiwski@wileyrein.com

Takeaways from the 11th Circuit FTC vs. LabMD Decision

By Kirk J. Nahra

This article was originally published in IAPP's Privacy Tracker **here**.

The Federal Trade Commission's saga with LabMD began in August of 2013. Someone will write an interesting book about the twists and turns of this enforcement action. Maybe it will be better as a movie — plot twists, multiple sub-plots, changing narratives, interesting characters and a lot of David and Goliath — and the last chapter hasn't yet been written.

Recently, the Eleventh Circuit issued its **long-awaited decision** on LabMD's challenges to the FTC's enforcement action, resulting in a decision to vacate the commission's order.

continued on page 20

Takeaways from the 11th Circuit FTC vs. LabMD Decision

continued from page 19

While there still is more to come, what does this case mean today for the FTC and for companies facing potential FTC enforcement action?

As this case has evolved, four key questions emerged:

- Does the FTC have authority to act on data security compliance?
- If so, does the FTC have authority to take action against a HIPAA-covered entity?
- Is the FTC's authority limited by a need to demonstrate consumer harm (and what level of harm is needed)?
- Was the FTC's decision in this single instance right or wrong?

Curiously enough, despite the attention paid to these issues, the court decision really focuses on a fifth issue: Was the relief sought by the FTC appropriate? The court assumed the first issue, avoiding any challenge or support for the Third Circuit's *Wyndham* decision on this point. It said nothing whatsoever about the HIPAA issue and really didn't talk much about consumer harm, a topic that an administrative law judge had focused on earlier in the process. The court also really didn't address whether the FTC was just wrong in its judgment, the narrowest possible basis for a decision.

Instead, the court's opinion turns on the relief sought by the FTC, rather than the "violation" itself. The key language is as follows: "In the case at hand, the cease-and-desist order contains no prohibitions. It does not instruct LabMD to stop committing a specific act or practice. Rather, it commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness. This command is unenforceable."

The decision says that the commission's order — which dictates a compliant information security program going forward — "does not enjoin a specific act or practice. Instead, it mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished. Moreover, it effectually charges the district court with managing the overhaul." Therefore, the Eleventh Circuit vacated the FTC's order.

So, what's next? In Twitter language, it means confusion, nervousness, new challenges to the FTC's authority and the need to develop new and improved compliance orders.

Let's flesh this out. The Eleventh Circuit did not address the FTC's general authority over data security. It simply assumed that this authority exists. A decision that directly undermined the FTC's authority would have had enormous implications (including the possibility for Supreme Court review if there was a direct conflict with the *Wyndham* decision). It also could have led to congressional action to implement data security legislation – although Congress has not been able to do this on its own. The court didn't do this at all, but it is fair to read the decision as being somewhat skeptical in this area. That will lead more potential defendants to act more aggressively about the FTC's enforcement activity.

The biggest challenge in the short term will be the need for the FTC to figure out the path going forward in specific cases, once it has determined that a current violation exists. In some cases, the FTC has simply obtained an agreement of the party to implement the required regulatory or statutory practices. While that results in an enforcement "win" for

continued on page 21

continued from page 20

the FTC, it may be hard for privacy advocates to see the benefits of an order getting a party to follow the law. Here, a broader more general order requiring an improved overall data security program did not meet with the court's approval. The FTC order required LabMD to implement a data security program "reasonably designed" to meet the FTC's approval. How different is that from the idea that a company must maintain "reasonable and appropriate" data security standards (which is both generally the regulatory standard in many situations and also the standard the FTC generally uses to launch its enforcement efforts)? The court seemed to assume that the FTC could determine what is a reasonable and appropriate data security program now, but could not leave that scope open going forward.

It is possible that this decision may lead to more efforts to give the FTC additional authority in this area. Perhaps the FTC will try to define more clearly — presumably through guidance — what it views as these reasonable and appropriate standards (although IAPP and others have collected this information from prior cases). Unlike most enforcement agencies, the FTC does not have the authority in the first instance to fine or penalize companies on data security issues. So, they are forced to focus on the future, while other enforcement agencies could focus on the past.

Much like the Supreme Court's *Spokeo* decision — which has launched a thousand new court challenges in an effort to address a common issue — we can expect that potential defendants will become more aggressive in challenging the FTC and that the FTC in response may direct its challenges in a more focused manner where specific identifiable problems can be enumerated. Putting aside broader political questions of where the FTC is going in this area overall, companies clearly will benefit from a more significant focus on overall policies and procedures and more aggressive efforts to manage overall security risks. Companies that can demonstrate a thoughtful basis for a reasonable and appropriate security program may find even more benefits from this activity. While it is important to prepare for an FTC investigation, it also is important to remember that any government enforcement action typically lags far behind many of the other results of a security breach — including adverse publicity, altered business relationships and class-action lawsuits.

While the LabMD decision by the Eleventh Circuit is interesting, important and, frankly, a bit surprising, we should expect that it will not immediately alter the overall landscape for data security enforcement, but it will lead to more opportunities for well-prepared defendants to respond appropriately to enforcement investigations. The FTC's challenge will be to navigate the tricky lines left by the court's decision — the FTC's current ability to determine that existing security issues were not reasonable and appropriate, but an apparently tougher standard in defining what that behavior must be going forward. ■

For more information, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

Chambers USA Recognizes 32 Wiley Rein Attorneys Across 12 Practice Areas as Among Best in the Country

The 2018 edition of *Chambers USA: America's Leading Lawyers for Business* recognizes 32 Wiley Rein attorneys across 12 areas of law. The practices ranked as leaders nationwide are Election Law & Government Ethics, Franchise, Government Contracts, International Trade, and Privacy & Cybersecurity. The practices ranked as leaders in Washington, DC, are Insurance, Media, and Telecom, Media & Technology.

In addition, Wiley Rein is listed as a "Noted Firm" for Environment, Litigation: White Collar Crime & Government Investigations, and International Trade: Export Controls & Economic Sanctions. The firm also is featured in a Spotlight Table for "Privacy Data Security: Health Care."

The *Chambers USA* rankings for Wiley Rein attorneys can be found **here**.

Events & Speeches

Genetics: New Healthcare Opportunities New Legal Challenges

Kirk J. Nahra, Speaker

The Virginia Bar Association's 128th Summer Meeting

July 21, 2018 | Hot Springs, VA

Data Privacy and GDPR Within the Life Science Industry

Kirk J. Nahra, Speaker

Q1 Productions Life Science Data Privacy Governance & GDPR Alignment Conference

July 26, 2018 | Philadelphia, PA

Privacy Bootcamp

Kirk J. Nahra, Speaker

IAPP Privacy. Security. Risk. 2018

October 17, 2018 | Austin, TX

I'm a Lawyer: How Can I Advise on Data Security Issues?

Kirk J. Nahra, Moderator

IAPP Privacy. Security. Risk. 2018

October 18-19, 2018 | Austin, TX

Mastering the Evolving Law of Data Analytics

Kirk J. Nahra, Speaker

AHIMA Data Institute: Making Information Meaningful

December 6, 2018 | Las Vegas, NV

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Michael L. Diakiwski	202.719.4081	mdiakiwski@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Kathleen E. Scott	202.719.7577	kscott@wileyrein.com