Wiley Rein LLP

PRIVACY IN FOCUS©

Developments in Privacy and Information Security Law | May 2017

In this month's issue, we look at the past, present, and future of privacy and security. For the past, we continue to get questions on a regular basis about the core elements of the HIPAA privacy and security rules, including the important question of HIPAA's scope. These issues are taking on added importance as many kinds of entities struggle with their role under HIPAA, including whether it applies at all to their activities. I try to cover the basics of these provisions, as a starting point for more sophisticated assessments. For the present, Megan Brown and Kat Scott write about the implications of the recent Executive Order on Cybersecurity, which we will be following closely all year. For the future, Umair Javed evaluates important scope issues related to the new GDPR privacy rules for the European Union (taking effect in 2018). John Lin also addresses new categories of litigation related to the Internet of Things, which we also will be seeing a lot more of in the coming years.

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

— Kirk Nahra, Privacy & Cybersecurity Practice Chair

ALSO IN THIS ISSUE

The GDPR's Reach: Material and Territorial Scope Under Articles 2 and 3

By Umair Javed

With just over a year to go before the European Union's (EU) General Data Protection Regulation (GDPR or Regulation) comes into force, companies around the world are recognizing the importance of complying with the new laws. According to *Forbes*, analysis from information management company Veritas Technologies suggests that "86 percent of organizations worldwide are concerned that a failure to adhere to GDPR could have a major negative impact on their business" and "nearly 20 percent said they fear that non-compliance could put them out of business."[1] Given that fines under the GDPR can be as high as $21 million or 4 percent of

continued on page 2

Refresher on the HIPAA Privacy and Security Rules

By Kirk J. Nahra

The Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules continue as important compliance and business challenges for a broad range of entities both in the health care system and in the broader ecosystem providing services to the health care system. With the passage of time, it is important to remember the key principles of HIPAA – and to make sure that your company's employees (both new and old) remember how these principles work.

Background

The HIPAA era began in 1996, with the passage of the Health Insurance Portability and Accountability Act of 1996. While "HIPAA" now means many things to many people, at its foundation, the HIPAA law itself focused on "portability," the idea that individuals could "take" their health insurance coverage from one employer to the next, without having pre-existing health conditions acting as an impediment to job transitions.

continued on page 3

The GDPR's Reach: Material and Territorial Scope Under Articles 2 and 3

continued from page 1

annual turnover, whichever is greater, these fears are hardly baseless.

Nonetheless, confusion reigns over the actual scope of the GDPR, and many non-EU companies are unsure whether they must comply with the new Regulation and, if so, how. That the GDPR will impact many more companies than the EU Data Protection Directive (Directive) it replaces is a dictum. Yet, much of the discussion about the territorial reach of the GDPR appears to be generating more heat than light. While non-EU companies should take EU privacy laws more seriously, there is a risk of taking the fear of non-compliance too far and needlessly chilling innovation. Guidance from regulatory authorities and the Article 29 Working Party will be crucial for understanding the real risk to non-EU companies.

GDPR: A Brief Overview

Adoption of the GDPR – after more than four years of intense debate, negotiation, and lobbying – marked an important milestone in EU data protection laws. The GDPR replaces the EU Data Protection Directive – a 22-year-old privacy framework. One of the most significant changes in the GDPR is the very fact that it is a "regulation," as opposed to a "directive." A regulation applies directly to EU Member States and, as a formal matter, allows them little discretion in implementation, whereas a directive sets desired results and policies but depends upon Member State implementation into national law. Because regulations automatically become part of each Member State's legal framework, they typically reduce the potential for regulatory patchwork across EU Member States' domestic laws. Whether the GDPR will truly create a consistent data protection framework in the EU remains to be seen – Member States retain the ability to derogate from certain aspects of the Regulation.

The GDPR introduces significant and ambitious changes to EU privacy laws. Under the GDPR, consent must be "freely

continued on page 16

When Congress passed HIPAA, it also added into the mix a variety of other topics related to the health care industry (such as creating large funding for what has now become an extended fight against health care fraud). One of the policy mandates adopted in HIPAA was to move toward standardized electronic transactions for the health care industry. The core idea was that certain "standard transactions" – such as the submission of a health insurance claim and the payment of that claim – could be "standardized" in mandatory electronic formats, and thereby create efficiency savings and more effective results. With these standardized transactions came a concern about privacy and security associated with health care information being put into electronic form, with the resulting requirements for the creation of the HIPAA Privacy Rule and the HIPAA Security Rule. So, now, for most people and in most situations, HIPAA has become shorthand for health care privacy and security.

Who Needs to Care About HIPAA?

As a result of this statutory history, HIPAA is not a general medical privacy rule. It is an important and far-reaching set of rules that provides protections to individuals in certain contexts – mainly where the relevant information originated with or flows through a HIPAA "covered entity" – a health care provider, a health plan, or a health care clearinghouse.

So, who does need to comply with the HIPAA rules? The HIPAA privacy and security rules applied only to specifically designated "covered entities," health care providers, health plans, and health care clearinghouses. This includes a full range of health care providers, generally physicians, hospitals, pharmacies, and a wide variety of entities that provide direct health care services to patients. It also reached to various "health plans," including government health care programs, private health insurers, and significantly, the health care benefit plans offered by employers. However, even from the start, HIPAA was not a general medical privacy law. It applied to certain entities in certain situations, for certain information. That meant that a large number of companies that obtain or use health care information are not within the scope of these rules, such as consumer-facing entities, many health care web sites, life and disability insurers, employers in their employment role, etc.

Because of this limitation to covered entities, the U.S. Department of Health and Human Services (HHS) (the agency tasked with writing these privacy and security rules) developed a creative solution to respond to a key fact about the health care system. While the covered entities are core participants in the industry, they rely on tens of thousands of vendors to provide them services, with many of these services involving protected patient information. Therefore, the concept of a "business associate" was born, i.e., an entity that provides services to the health care industry where the performance of those services involves the use or disclosure of patient information.

Because HHS originally had no direct jurisdiction over these "business associates," HHS imposed an obligation on the covered entities to implement specific contracts with these vendors that would create contractual privacy and security obligations for these vendors. The failure to execute a contract would mean that the covered entity violated

continued on page 4

the HIPAA rules. A business associate's failure to meet a contractual privacy standard would be a breach of that contract, but would not subject the business associate to government enforcement, because the business associate was not regulated under the HIPAA rules.

Now, as a result of the 2009 "HITECH" law and HHS regulations issued in 2013, these "business associates" must comply directly with significant portions of the HIPAA rules. Accordingly, while these vendors have had contractual obligations since the beginning of the HIPAA era, they now must meet many of the same standards as the covered entities, and face the same risks of government enforcement. Although this legislation does not turn business associates into covered entities, it does impose direct accountability on these business associates, with potential civil and criminal liability for a failure to meet these requirements. This compliance obligation extends "downstream," to service providers of a business associate, and service providers to that downstream business associate, on indefinitely. These "subcontractors" face the same compliance obligations as a first-tier business associate that contracts directly with a hospital or a health insurer.

What are the Core Principles of the HIPAA Privacy Rule?

Use and Disclosure

The HIPAA Privacy Rule consists of the "Standards for Privacy of Individually Identifiable Information," found at 45 CFR Part 160 and Part 164, Subparts A and E. The core idea for most privacy rules involves the principles around how information can be used and disclosed. The general premise of the HIPAA Privacy Rule is straightforward. Information about individuals (called "Protected Health Information" or "PHI" in HIPAA) cannot be used or disclosed unless permitted by the rules or specifically authorized by the individual. The premise is that use and disclosure should be relatively easy for core health care purposes, and harder for everything else.

Under the HIPAA structure, patient consent is provided by assumption, for particular categories of uses and disclosures. From the regulator's perspective, there are certain kinds of uses and disclosures of patient identifiable information that are essential to the operation of the health care system and for which patient consent is presumed under the regulatory structure. These purposes (known as "TPO" in the HIPAA system) are for (1) treatment; (2) payment for health care services; and (3) health care operations, essentially the administrative operations of running a health care business. For uses and disclosures that fit these categories, patient consent is presumed, and no further steps are needed. These TPO disclosures represent the overwhelming percentage of information use in the health care system, covering the core areas of treating patients, paying for this treatment, and operating health care businesses.

There also are certain categories of disclosures – known as "public priority" purposes – where patient consent is, essentially, irrelevant (from the perspective of those drafting the rules). These are areas such as public health disclosures, enforcement investigations, litigation, and a wide variety of other purposes where there is a public goal to be served in the disclosure, independent of patient consent. Disclosures in these areas can be made –

continued on page 5

consistent with specific limitations in some circumstances – without the need for patient consent.

For all other uses and disclosures, the disclosure can be made only with patient "authorization," a carefully defined and very specific document executed by a patient in a particular situation. Using an authorization, a patient can "authorize" any use or disclosure of the patient's information. So, if a patient wants his medical records disclosed to a future employer, or wants them sent to a financial advisor, or the covered entity wants to promote a patient's story in a newsletter, this can only be done with the patient's authorization.

Beyond these consent principles, there are various other core elements of the overall rules on use and disclosure. The "minimum necessary" principle provides a general overlay for most uses and disclosures (and is a good operating principle in all contexts). "Minimum necessary" means that an entity, even where a use or disclosure is permitted, should only disclose the "minimum necessary" information needed to perform the particular function. This is not a hard and fast rule, and companies do not need to spend an inordinate amount of time and energy scrutinizing each disclosure. But, it is important to develop general principles surrounding how companies determine what is the "minimum necessary" information to be disclosed, and employees should be trained to think about this principle in all settings.

Sale and Marketing

There also are specific rules related to the sale of PHI or the use of PHI for marketing. As with many privacy rules, using individual information for marketing purposes is highly limited. The HIPAA rules place substantial restrictions on how PHI can be used or disclosed for marketing purposes. Because the HIPAA restrictions apply to both use and disclosure, this means that companies are restricted in how they can communicate with their patients about marketing opportunities, in addition to placing restrictions on to whom this information can be disclosed. The HITECH rules limited this marketing even more, by precluding marketing (without a patient authorization) where there is remuneration (or payment) in connection with the marketing in most situations. As with all other areas, if a covered entity wants to do more than what is permitted by the HIPAA rules, then the entity must obtain the individual's authorization. For example, a health insurer that wants to market its life insurance products, or those of a business partner, must obtain the individual's authorization.

The HITECH changes also included specific limitations on the sale of PHI. For some, this provision seemed unnecessary, since many "sale" situations would involve disclosures of PHI that were already prohibited by the HIPAA rules. Nonetheless, for those limited situations where a sale would be permitted in the context of the rules, the HITECH changes generally now require an authorization from the individual before information can be sold.

De-Identification

The HIPAA rules apply to individually identifiable information. The principle – set forth in significant detail in the HIPAA rules – is that if otherwise protected information has been "de-identified" according to the rules, this information is no longer "individually identifiable" and therefore there are no longer sufficient privacy interests at stake to justify regulation. The HIPAA rules set out a highly detailed formula for de-identification. If information is "de-identified" under these standards, then the information is no longer

continued on page 6

regulated by HIPAA, and can be used or disclosed for any purpose.

At the same time, it is important to understand that PHI remains PHI until it has been de-identified under these standards. Therefore, companies need to focus on these de-identification standards when making specific uses and disclosures. At the same time, something less than full de-identification is permitted in situations where a use or disclosure already is permitted by the HIPAA rules. If PHI can be used or disclosed in a specific situation, then removing a limited number of identifiers is an appropriate step (under a "minimum necessary" principle or otherwise), as no full de-identification is required. De-identification is required only for situations where PHI cannot be used or disclosed in a particular situation.

Individual Rights

The HIPAA rules also provide patients with specific individual rights, beyond the general rights conveyed through the use and disclosure limitations. Specifically, individuals have the following rights:

- The right to receive a notice of privacy practices (the one right that happens automatically, since notices must be provided by most covered entities);
- The right to "access" (receive a copy of) a "designated record set" about the individual;
- The right to amend information in certain situations;
- The right to an "accounting of disclosures" in certain situations; and
- The right to additional restrictions on use and disclosure of a confidential communication.

The individual rights have an impact on all covered entities and some business associates. Covered entities, for example, provide privacy notices to individuals. Business associates, who often are invisible to these individuals, do not. Covered entities must develop means of responding to individual requests for a designated record set (even though few individuals will seek one), while only a small percentage of business associates maintain any element of a designated record set.

Business Associate Contracts

While business associates now are covered directly by the HIPAA rules, HIPAA still requires contractual provisions defining how business associates can use and disclose PHI when performing services, along with various other requirements. Covered entities must execute these contracts with their service providers, and business associates must execute similar contracts with their downstream subcontractors. Negotiating these contracts in a reasonable and cost-effective way is a substantial challenge for both covered entities and business associates. While many of the provisions of these agreements are "standard," there are other provisions that typically result in significant negotiations between the parties.

General Policies and Procedures

Under the HIPAA Privacy Rule, there also is a requirement for covered entities to develop specific administrative procedures to ensure compliance with the overall rules. Under the precise language of the privacy rule, business associates do not appear to have a requirement to implement all of these procedures. However, for most business associates, it will be appropriate to develop these procedures as a means of both

continued on page 7

ensuring and documenting compliance with the rules.

The key topics for these procedures include:

- Designation of a privacy official;
- Training of employees;
- Development of "appropriate safeguards" for PHI (a "min-security rule" for all PHI);
- A complaint process;
- A sanction approach for employees who violate these rules;
- Appropriate mitigation procedures;
- Overall policies and procedures; and
- Record retention processes.

The HIPAA Security Rule

The second key component of HIPAA is the Security Rule, known formally as the HIPAA "Security Standards," set forth in 45 C.F.R. Parts 160 and 164, Subpart C.

The HIPAA Security Rule sets forth detailed requirements for the protection of electronic PHI. All covered entities and business associates must meet the requirements of the HIPAA Security Rule. Because it is process- and documentation-intensive, the Security Rule presents serious challenges for any health care company. While covered entities have had to comply with the Security Rule since 2005, business associates must now comply with these provisions as a result of the HITECH changes. For most business associates, this Security Rule compliance represents the single biggest challenge under HIPAA.

In setting out the Security Rule requirements, HHS focused on four key goals/mandates for the protection of electronic PHI. To be in compliance with this rule, a covered entity or business associate must:

- Ensure confidentiality, integrity, and availability of electronic protected health information created, received, maintained, or transmitted;
- Protect against "reasonably anticipated threats or hazards" to the "security or integrity" of this information;
- Protect against "reasonably anticipated uses or disclosures" of this information that are not permitted under the Privacy Rule; and
- Ensure compliance by its workforce.

In order to make this mandate feasible, HHS developed a "flexible" approach to compliance, by making the requirements "scalable" based on the specifics of the organization. The provisions also are intended to be "technology neutral" – meaning that the rule does not dictate any specific technological solution. Instead, the rule focuses on process – how to evaluate a company's security risks and decide what steps should be taken.

Covered entities and business associates, therefore, must develop appropriate security measures based upon:

- The size, complexity, and capabilities of the business;
- The business's technical infrastructure, hardware, and software security capabilities;
- The costs of particular security measures; and
- The probability and criticality of potential risks to electronic protected health information.

In general, with this "flexibility," a covered entity under the rule may use "any security measures that allow the covered entity to

continued on page 8

reasonably and appropriately implement the standards and specifications" of the Security Rule. This flexibility is both useful, by providing a range of appropriate options, and difficult to assess, as it is hard to tell when an entity has "done enough" under the Security Rule.

In addition, the Rule breaks down the regulatory provisions into "standards" – which constitute the general security topic that must be addressed, and "specifications," which are the particular safeguards designed to address the specific standard. All of these issues are designed to protect "electronic" protected health information – PHI from the Privacy Rule that is transmitted or maintained in electronic media. Some of the specifications are "required" and must be implemented. Others are "addressable," meaning that a covered entity must review the issue and evaluate whether the particular step is "reasonable and appropriate" for implementation by the covered entity.

The rule sets out a series of "administrative" safeguards that constitute the key provisions of an effective security program. In particular, the requirements for "risk analysis" and "risk management" set the stage for the remainder of the activities. In fact, most of the Security Rule describes an appropriate "process" that covered entities must go through in evaluating security options, broken down into technical, physical, and administrative safeguards.

Under the rule, "risk analysis" means to "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity." Risk management, which involves the follow-up steps after a risk analysis, involves the obligation to "[i]mplement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the Security Rule]." A failure to conduct effective risk analysis represents the single most frequent element of HIPAA enforcement actions.

Also included in the administrative safeguards are requirements such as a sanction policy, assigned responsibility for security activities, security awareness and training, contingency planning, and "security incident" procedures. (A "security incident" is an "attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.") There is a separate administrative safeguard related to "business associates," which are vendors to covered entities (as defined by the HIPAA Privacy Rule). These security provisions will require specific provisions in business associate contracts.

"Physical" safeguards are less dramatic, but constitute an additional core set of safeguards. These include facility access controls (limiting physical access to information systems), workstation use policies, workstation security, and device and media controls (such as procedures for disposal of computer hardware in light of recent reports of privacy violations involving discarded computers that still retained PHI).

The "technical" safeguards also are relatively specific, involving access controls (such as unique user identification, automatic log-off, and emergency access procedures), audit controls, integrity (protection against improper alteration or destruction of PHI), person/entity authentication, and transmission security.

continued on page 9

In addition to these safeguards, the Security Rule requires covered entities to develop security policies and procedures, and to maintain appropriate documentation of these policies and procedures.

In general, all covered entities and business associates must develop appropriate processes to identify locations of PHI, implement appropriate measures to protect the confidentiality of this information, and then develop policies and procedures that document and define how these protections are implemented across a company.

Breach Notification

The last "core" provision of HIPAA involves the breach notification rule – the "Notification in the Case of Breach of Unsecured Protected Health Information" provisions, as set forth at 45 CFR Part 164, Subpart D. This regulation was required by the HITECH statute, and certainly has generated an enormous amount of publicity and discussion.

Essentially, the breach notification rule requires notification to individuals in the event of certain kinds of security breaches involving their PHI. In specific circumstances, notification also may be required to HHS and even media in specific geographic locations.

The primary notification obligations are placed on covered entities. Business associates must notify the affected covered entity in the event of a triggering breach.

Under the regulations, a "breach" means "the acquisition, access, use, or disclosure of protected health information in a manner not permitted [by the Privacy Rule] which compromises the security or privacy of the protected health information." Certain situations are exempted from this definition, such as "any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under [the Privacy Rule]."

For any other "not permitted" use or disclosure, notification to an individual is presumed to be required unless the specific standard set forth in the regulation is met. Under the rule, notice must be provided for a breach unless the entity can determine, following a risk assessment, that there is a "low probability" of compromise of the information. Specifically, a covered entity or business associate, as part of its risk assessment, must review the following factors (along with any others that are appropriate):

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

Conclusions

For any health care company, whether a covered entity or business associate, the HIPAA Privacy and Security Rules require significant attention and impose realistic risks related to the protection of individually

continued on page 10

identifiable information about patients or health plan benefit members. Keep in mind that these HIPAA requirements matter to your company if you are any of the following:

- A health care provider (doctor, hospital, pharmacy, etc.);
- A health or long-term care insurer;
- An employer to the extent you provide health care benefits to your employees;
- A service provider to any of these entities; or
- A service provider to a service provider (and on downstream).

While many of these provisions reinforce common-sense confidentiality requirements, the HIPAA rules are complicated and detailed in part, and require meaningful attention to strategies and approaches for protecting personal information. Enforcement of these provisions, by the Department of Health and Human Services' Office for Civil Rights (along with state Attorneys General) has been modest, but is growing steadily. Enforcement sanctions range from corrective action plans to multimillion-dollar penalties. Companies also face a wide range of HHS investigations, triggered by complaints, breach reporting or other public events. HHS also is developing a revised audit program that will involve proactive review of the privacy and security practices of certain health care companies.

With all of these issues, the health care industry faces a meaningful ongoing challenge from the HIPAA rules. While covered entities have been required to follow these provisions for many years, many companies either do not consistently do a good job or do not adequately engage in ongoing reviews of business activities to ensure compliance. For business associates, these requirements are much newer. Many business associates are still struggling with these requirements, particularly under the Security Rule, with a wide range of companies also unaware of the full range of obligations that have been imposed on them.

These provisions remain important to the health care industry and its individual consumers. Personal data has never been more important in the health care system, and there is a wide variety of societal benefits that stem from the use and disclosure of health care information. At the same time, these rules provide meaningful protections for the privacy and security of PHI, and the health care industry needs to make sure that it continues to take critical steps to protect the sensitive information of its core customers, the individual patients, and members. ■

For more information on HIPAA requirements, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

Litigating the Internet of Things

By John T. Lin

Let's say you manufacture a connected oven, and the six o'clock news runs a story in which researchers claim they can remotely access and turn on the broiler. Anyone exploiting such a vulnerability would be committing a felony, but luckily, no exploit happened. But before you know it, you are slapped with a class action lawsuit claiming economic injury because some consumers would not have bought the oven if they knew it was "defective" – i.e., that it was susceptible to potential third-party "hacking."

As far-fetched as such lawsuits might sound, they may become more common. Everyday devices – cars, home lighting controls, alarm clocks, and fitness trackers – are now connected to the Internet. These "Internet of Things" (IoT) devices, like smartphones and laptops, are under scrutiny by ethical and no-so-ethical hackers, and may be vulnerable to evolving threats. And where there's an issue affecting large numbers of consumer products, litigation looms. This litigation, however, comes at the cost of important progress.

Two cases highlight the litigation potential facing IoT manufacturers and sellers when it comes to security. In *Cahen v. Toyota Motor Corp.,* class-action plaintiffs claim that vehicles contained electronic control units that could be hacked, and seek money damages despite there being no actual exploit or breach. A district court in California dismissed the suit for lack of standing, but its decision is on appeal at the Ninth Circuit. The case has been argued and is awaiting a decision.

Similarly, in *Flynn v. FCA US LLC*, plaintiffs are suing Chrysler over alleged vulnerabilities in their cars' Uconnect system that they claim could allow hackers to take control of the vehicle. A number of their claims were dismissed for lack of standing, but others remain pending.

Cases like these may be just the start. Unless courts and policymakers draw sharp lines, as connected devices are deployed, the likelihood of such lawsuits only increases. Litigation may require courts to set new standards and de facto regulations that will shape the future of IoT. But is this a job for courts?

The entry of federal courts (or arbitrators for those companies that can effectively deploy arbitration clauses) into this fast-moving and technical space might not be a welcome development. Although courts have an important role to play generally, they are not the best place to develop technology policy. Lawsuits are limited to the parties and evidence specific to that case and offer little to no opportunity for the public to participate. Plus, the judiciary does not have the expertise to develop standards to make devices more secure. Yet the outcomes of these lawsuits have serious implications – establishing new standards and responsibilities for the private sector. Rulings – or jury verdicts – might resolve the case, but could have industry-wide implications that slow innovation in a burgeoning industry.

Contrast this approach with what the government is doing. Government agencies, such as the National Telecommunications and Information Administration (NTIA), the Federal Trade Commission (FTC), and National Institute of Standards and Technology (NIST), are evaluating the market and developing best practices for IoT technology. Congress is setting up caucuses and working groups to study these issues and avoid a rush to regulation.

continued on page 12

Agencies have convened working groups of experts and held open forums where stakeholders discuss challenges and desired outcomes. These public efforts have resulted in dialogues between manufacturers, cybersecurity experts, and consumer groups, and can lead to recommendations and best practices that have broad support and create space for manufacturers to continually address security.

Ironically, litigation over product security may ultimately make devices less secure. As Wiley Rein partner Megan Brown discussed at a recent U.S. Chamber of Commerce (Chamber) panel, the risk of litigation may chill needed communication and collaboration. The fear of civil discovery might discourage a software designer from discussing a vulnerability with a product manufacturer, or make companies hesitant to engage security researchers. This destroys the collaboration and sharing that will make the ecosystem smarter and safer.

IoT offers an exciting new world. But like any new field, there are new risks that need to be addressed. Device security is one such risk. As Tom Donohue of the Chamber notes, "the right legal and regulatory framework plays an important role in making new technologies safe and secure."

Thankfully, industry and government understand this need and are developing that framework, based on partnerships and collaboration. But if we're not careful, litigation could slow this important progress. We should be wary of letting courts hack into this regulatory space. ■

For additional information, please contact:

John T. Lin
202.719.3570
jlin@wileyrein.com

President Trump's Cyber EO Contains Few Surprises, But Portends a Busy Year for Federal Agencies and the Private Sector

By Megan L. Brown and Kathleen E. Scott

On May 11, 2017, President Trump signed the long-awaited Cybersecurity Executive Order (Cyber EO). Entitled *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, the Cyber EO has three substantive sections: (1) Cybersecurity of Federal Networks, (2) Cybersecurity of Critical Infrastructure, and (3) Cybersecurity for the Nation. These sections create requirements for a number of reports and assessments by various agencies. These reports will be classified as appropriate. Overall, the Cyber EO contemplates at least 15 reports in the next year, and one report that is required to be updated annually. The Cyber EO picks up on several issues, from botnets to workforce development, that industry and government have been looking at for some time. In the main, it is silent about process and the scope of opportunities for public comment and input.

Section 1, "Cybersecurity of Federal Networks," Focuses on Federal Network Risk Management, the NIST Cybersecurity Framework, and Procurement

The Cyber EO emphasizes the importance of cybersecurity risk management, defining it as "full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents …, and to mitigate the impact of, respond to, and recover from incidents." This section also highlights information sharing, stating that information sharing "facilitates and supports [cybersecurity risk management] activities."

Section 1 mandates that executive branch agencies implement risk management, and creates a series of reports and reviews:

- "Agency heads will be **held accountable by the President** for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data."
- Each agency head **must use NIST's *Cybersecurity Framework*** (or any successor document) to manage agency cybersecurity risk. Each agency head must **provide a risk management report** to the Secretary of Homeland Security and the Director of OMB by **August 9, 2017.** Reports must document risk mitigation and acceptance choices made by agency heads as of May 11, 2017, and detail action plans for implementing NIST's *Cybersecurity Framework*.
- The Secretary of Homeland Security and the Director of OMB **will make determinations** based on the agencies' risk management reports as to whether each agency's risk mitigation and acceptance choices are adequate. Within 60 days of receipt of the reports, the Director of OMB and Secretary of Homeland Security will **submit the determinations and a plan** to the President. The plan must, among other things: "protect the executive branch enterprise, should the determination identify insufficiencies; address immediate

continued on page 14

unmet budgetary needs …; establish a regular process for reassessing and, if appropriate, reissuing the determination, and addressing future, recurring unmet budgetary needs..." and align with the NIST *Cybersecurity Framework*.

The EO states that the executive branch must "build and maintain a modern, secure, and more resilient executive branch IT architecture." Agency heads are required to **favor shared IT services** – including email, cloud, and cybersecurity services – in the procurement process. Additionally, this section requires a **report to the President regarding modernization of federal IT**. The report is due **August 9, 2017**, and "shall assess the effects of transitioning all agencies, or a subset of agencies, to shared IT services with respect to cybersecurity."[1]

Section 2, "Cybersecurity of Critical Infrastructure," Initiates Market Transparency Efforts, Orders a Special Effort to Address Botnets, and Directs More Reports on Industries and Sectors

This section draws from President Obama's 2013 EO, Critical Infrastructure Security and Resilience, and mandates that the Secretary of Homeland Security, with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the FBI, appropriate sector-specific agencies, and others shall:

- **"[I]dentify authorities and capabilities** that agencies could employ to support the cybersecurity efforts of critical infrastructure entities."
- **Engage with and solicit input from critical infrastructure entities** to determine how identified authorities and capabilities might be employed, and to identify any obstacles.
- Provide a **report to the President** by **November 7, 2017** that includes authorities and capabilities; results from engagement with critical infrastructure entities, and has findings and recommendations for supporting critical infrastructure entities' cybersecurity risk management efforts. The report must be **updated annually**.

Section 2 requires the Secretary of Homeland Security, with the Secretary of Commerce, to submit a report on transparency in the marketplace by August 9, 2017. It is to look at "the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cybersecurity risk management practices by critical infrastructure entities, with a focus on publicly traded critical infrastructure entities."

Additionally, Section 2 launches an effort against **botnets and other automated threats**. Specifically, the Secretaries of Commerce and Homeland Security are to lead an "open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)." They are to consult with other agency heads, including but not limited to the Chairs of the FTC and the FCC. A **preliminary report on the botnet effort** is to be made publicly available by early **January 2018**, and the **final report** is due to the President on **May 11, 2018**.

Section 2 requires additional industry-specific reports and assessments.

- It requires an **assessment of electricity disruption incident response**

continued on page 15

capabilities, to be completed by the Secretaries of Energy and Homeland Security, due on **August 9, 2017.**

- The departments of Defense and Homeland Security, along with the FBI, must present to the President, also on **August 9, 2017,** a **report on cyber risks facing the defense industrial base**, including supply chain.

Section 3, "Cybersecurity for the Nation," Addresses Deterrence, Workforce, and International Issues

The Cyber EO states: "To ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Further, the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace."

Section 3 mandates a number of efforts, including:

- A Deterrence and Protection Report, due August 9, 2017, which should cover the "Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats."
- International Cybersecurity Priorities Reports from various agency heads, in an effort to work with allies to maintain the overarching policy goal stated above. These reports are due June 2017. The Secretary of State is charged with providing a report documenting an engagement strategy for international cybersecurity cooperation 90 days after the initial reports are submitted.
- A domestic and international workforce development effort.
  - First, the Secretaries of Commerce and Homeland Security, with others, must "**jointly assess** the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and [**by September 8, 2017**], provide a report to the President ... with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors."
  - Second, the Director of National Intelligence will review the workforce development efforts of foreign cyber peers; a **report** on this effort is due **July 10, 2017**.
  - Third, the Secretary of Defense will "assess the scope and sufficiency of the United States efforts to ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities, and provide a **report** with findings and recommendations to the President by **October 2017.** ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Kathleen E. Scott
202.719.7577
kscott@wileyrein.com

[1] For "National Security Systems," the Secretary of Defense and the Director of National Intelligence are in charge. They are charged with submitting a report regarding risk management to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism. The report is due in October 2017.

continued from page 2

given, specific, informed, and unambiguous." Data subjects have new rights, including the "right of portability" and the "right of erasure" (also known as the "right to be forgotten"). In addition to broad new rights for data subjects, the GDPR imposes several specific obligations on data controllers and processors, including notice and privacy by design requirements. In some circumstances, data controllers and processors will be required to designate a Data Protection Officer as part of an accountability program. Compared to the Directive, the GDPR also imposes stricter obligations with respect to data breach notifications.

To harmonize application of privacy rules across the EU, the GDPR introduces a "one-stop-shop mechanism" so that businesses with activities in multiple EU countries are primarily subject to the authority of one "lead" data protection authority (DPA). The new Regulation also is backed by a punitive penalty structure that is intended to ensure that data controllers and processors take the protections afforded to data subjects seriously. DPAs have wide-ranging powers to enforce the GDPR, which becomes effective starting May 25, 2018.

Applicability: Does the GDPR Apply to You?

Under the GDPR, jurisdiction is less related to the location where a business is incorporated or headquartered and more to the scope and location of business activity. The GDPR will apply to the processing of personal data by businesses "established" within the EU. More controversially, it also will apply to businesses outside the EU if their data processing activities relate to the offering of goods or services to individuals in the EU or to the monitoring of such individuals' behavior. This latter provision expands the territorial scope of the GDPR well beyond the EU, essentially making it global law.

Material Scope

Article 2 governs the material scope of the GDPR. The GDPR retains much of the jargon from the Directive, although with some important changes. The Regulation applies to the processing of "personal data," which is defined to mean any information relating to an identified or identifiable natural person (a "data subject"). In contrast to the Directive, the GDPR adds special categories of "sensitive data" which include both biometric and genetic data. The GDPR covers all "data processing," which is broadly defined to cover any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. Examples include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, erasure, or destruction. A person or body (alone or jointly) which determines the purposes and means of processing personal data is a "data controller." An entity which processes data on behalf of the data controller is a "data processor."

Territorial Scope

Article 3 of the GDPR governs its territorial scope. Pursuant to Articles 3(1) and 3(2), the GDPR applies to businesses established in the EU, as well as to businesses based outside the EU that offer goods and services to, or that monitor, individuals in the EU. Article 3(3) adds that the GDPR also applies in places where EU Member State law applies by virtue of public international law.

continued on page 17

continued from page 16

Although each of these provisions provides some contour to the broad scope of the GDPR, they also introduce complexities and gray areas.

1. Article 3(1): "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."

The GDPR applies to businesses "established" in the EU, where personal data is processed "in the context of the activities" of such an establishment. Per the Recitals, establishment "implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect." Once this test is met, the GDPR applies whether the actual data processing takes place in the EU or not.

In this respect, the GDPR is consistent with Article 4(1)(a) of the Directive, which reflects the country of origin concept (i.e., where your business is established dictates which law applies). While this may seem straightforward on the surface, interpretation of Article 4 of the Directive has been beset with complexity. In fact, the Court of Justice of the European Union (CJEU) has struggled with the question of what it means to be "established" and what constitutes processing carried out in the context of the activities of an establishment.

In *Weltimmo v. NAIH* (C-230/14), the CJEU adopted a broad and flexible definition of "establishment" that does not hinge on legal form – indeed, the presence of a single representative may be sufficient. In that case, Weltimmo – which was incorporated in Slovakia – was considered to be established in Hungary by virtue of the use of a website in Hungarian, which advertised Hungarian properties, use of a local agent, and use of a Hungarian postal address and bank account.

Similarly, in *Google Spain SL, Google Inc. v. AEPD, Mario Costeja Gonzalez* (C-131/12) (known as the "right to be forgotten" decision), the CJEU found that U.S.-incorporated Google Inc. was established in the EU because its search activities were sufficiently linked to the advertising sales generated by Google Spain, a local subsidiary. Because the data processing at issue in that case was related to the search business which Google Spain's sale of online advertising helped finance, the CJEU found that the processing was carried out "in the context of the activities" of the Spanish establishment.

The implications of these decisions are considerable. In both cases, the CJEU found that entities outside the EU could be subject to the Directive – which did not have express extra-territorial reach – because of the activities of a separate operation in an EU Member State. Of course, it is unclear whether these prior interpretations of "establishment" for purposes of the Directive will continue to apply under the GDPR. Indeed, they may be unnecessary given the express extra-territorial authority now granted under Article 3(2).

To the extent these cases continue to apply, the presence in the EU of a branch or subsidiary, or even a single individual, may bring all the data processing activity within the scope of the GDPR. Global businesses will need to show that there is no commercial connection between a local operation and

continued on page 18

continued from page 17

a non-EU company to avoid application of EU data protection laws to data processing by the non-EU company. And unlike the Directive, the GDPR's establishment rule applies both to controllers and processors.

2. **Article 3(2): "This regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:**
   a. **The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or**
   b. **The monitoring of their behavior as far as their behavior takes place within the Union."**

Unlike the Directive, the GDPR expressly extends the reach of EU data protection laws to businesses based outside the EU. Non-EU established businesses are subject to the GDPR where they process personal data of data subjects in the EU in connection with (i) the offering of goods or services or (ii) monitoring the behavior of individuals in the EU.

Under the first prong, the GDPR explains that having a commerce-oriented website that is accessible to EU residents does not by itself constitute offering goods or services in the EU. Rather, a business must show intent to draw EU customers, for example, by using a local language or currency. Article 3(2) appears to adopt a sliding scale approach as opposed to a bright-line rule, and there is little guidance so far on how to interpret this provision.

However, the CJEU has considered when an activity is "directed at" EU Member States in other contexts. A similar requirement can be found in Article 15 of Regulation 44/2001, known as the Brussels Regulation, which deals with contract disputes involving more than one country. In that context, a joint declaration by the EU Council and the Commission states that "the mere fact that an Internet site is accessible is not sufficient of Article 15 to be applicable, although a factor will be that this Internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance."[2] In *Pammer v. Schulter* (C-585/08), the CJEU found that it was necessary to show that the trader has "manifested its intention to establish commercial relations with consumers from one or more other Member States." To facilitate the application of this test, the CJEU offered a number of criteria to be considered, such as a clear statement by the trader on the website that its goods or services are offered in one or more Member States mentioned by name; the paid inclusion in search engines accessed from particular Member States; or "the international nature of the activity at issue; … telephone numbers with the international dialing code; use of a top-level domain name other than that of the Member State … mention of an international clientele composed of customers domiciled in various Member States."

Based on this guidance, the following factors (among others) may be strong indications that a non-EU business is offering goods or services to data subjects in the EU and may therefore be subject to the GDPR:

- Use of the language of a Member State (if the language is different than the language of the home state);
- Use of the currency of a Member State (if the currency is different than the currency of the home state);

continued on page 19

continued from page 18

- Use of a top-level domain name of a Member State;
- Mentions of customers based in a Member State; or
- Targeted advertising to consumers in a Member State.

Under the second prong of Article 3(2), businesses monitoring the behavior of individuals in the EU also are subject to the GDPR's requirements. The Recitals specifically contemplate tracking individuals online for purposes of creating profiles, "particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes."

Notably, Article 3(2) applies to the processing of personal data of any individual "in the EU." The individual's nationality or residence is irrelevant. The GDPR protects the personal data of citizens, residents, tourists, and other persons visiting the EU. So long as an individual is in the EU, any personal information of that person collected by any controller or processor who meets the requirements of Article 3(2) is subject to the GDPR. Where Article 3(2) applies, controllers or processors must appoint an EU-based representative.

3. Article 3(3): "This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

The GDPR also applies wherever EU Member State law applies by virtue of public international law. The Recitals provide a single example: a diplomatic mission or consular position. While that case is limited, the rule in public international law established by the Permanent Court of International Justice in Lotus is that a country has any extra-territorial jurisdiction it claims so long as there is not a public international law rule prohibiting the assumption of jurisdiction. Thus, the EU potentially could expand the GDPR scope in the future using this provision. ■

□ □ □ □ □

There is much that still must be clarified about new aspects of EU data protection laws. Guidance from regulatory authorities and the Article 29 Working Party will be crucial for understanding the real scope of Articles 2 and 3. In the meantime, non-EU companies should consider the scope of their activities and their risk tolerance in crafting a GDPR compliance strategy.

For more information on these and other EU data protection issues, please contact:

Umair Javed
202.719.7475
ujaved@wileyrein.com

---

[1]Adrian Bridgwater, Forbes, "Worldwide Climate of Fear over GDPR Data Compliance Claims Veritas Study" (Apr. 25, 2017) available at https://www.forbes.com/sites/adrianbridgwater/2017/04/25/worldwide-climate-of-fear-over-gdpr-data-compliance-claims-veritas-study/#763d37b1680c.

[2]See Joint Declaration, Statement on Articles 15 and 73, available at http://ec.europa.eu/civiljustice/homepage/homepage_ec_en_declaration.pdf.

Events & Speeches:

European Public Policy Trends

Megan L. Brown, Panelist

1st Annual API-IOGP Cybersecurity Europe Conference for the Oil & Natural Gas Industry

June 22, 2017 | London, England

Privacy Regulation in the New Administration

Bennett L. Ross, Speaker

Law Seminars International

June 27, 2017 | Telebriefing

The New Era of Big Data for Health Care

Kirk J. Nahra, Speaker

American Health Lawyers Association Annual Meeting 2017

June 26 & 28, 2017 | San Francisco, CA

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Umair Javed	202.719.7475	ujaved@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
Kathleen E. Scott	202.719.7577	kscott@wileyrein.com

To update your contact information or to cancel your subscription to this newsletter, visit:

www.wileyrein.com/newsroom-signup.html.