Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | July 2015

Introduction

In this month's issue of *Privacy in Focus*, we're covering some of the more significant recent developments in privacy and security, as well as providing readers with a broad perspective on two lasting endeavors. Shawn Chang looks at the Federal Communications Commission's role in the "Do Not Track" debate. Megan Brown discusses the recent controversy involving consumer privacy advocates and the National Telecommunications and Information Administration multistakeholder process intended to develop a voluntary code of conduct for the use of facial recognition technology.

On a broader level, Matt Gardner reviews the Federal Trade Commission's recent educational efforts focused on its overall data security enforcement efforts, with an eye towards providing businesses of all stripes with useful advice on reasonable data security protections. I provide a checklist for all companies to use in addressing the key areas related to privacy and data security, independent of industry.

Please let us know if you have questions or comments on these issues, or have other topics that you would like us to address. I can be reached at 202.719.7335 or knahra@wileyrein.com. Thank you for reading. ■

Kirk Nahra, Privacy Practice Chair

ALSO IN THIS ISSUE

Better Late than Never: FTC Data Security Initiative a Potentially Useful Guide to "Reasonableness"

On June 30, 2015, the Federal Trade Commission (FTC) announced a new data security initiative called "Start With Security."[1] The stated purpose of the initiative is to use the FTC's experience in data security enforcement actions to help businesses adopt appropriate measures to protect customers' data. The initiative has three components: a website that consolidates the FTC's guidance on data security,[2] a series of conferences aimed at helping small and medium businesses, and a "Guide for Business" (the Guide) that outlines 10 lessons derived from the FTC's data security enforcement actions.[3] Notably, the initiative comes amid judicial review of the fairness of FTC enforcement activity in the absence of clear rules or expectations.

The "Guide for Business"

The Guide is a must-read for general counsels and chief security officers. The FTC has brought over 50 enforcement actions against companies for having unreasonable data security practices under Section 5(a) of the Federal Trade Commission Act (FTC Act), which prohibits "unfair or deceptive acts or practices." The FTC's admonitions about security

continued on page 2

always return to the agency touchstone of "reasonableness."[4] The Guide is the FTC's most comprehensive public statement about what it considers to be an unreasonable data security practice.

The Guide, however, is not a detailed checklist of acceptable cybersecurity practices. The FTC is not claiming to weigh in on granular issues like how a firewall should be configured, whether data at rest should always be encrypted, or when to use two-factor authentication. Rather, the FTC returns to its "reasonableness" standard and confirms that "reasonableness" will change according to the particular characteristics of each business.[5]

The FTC's fluid and situation-specific approach to reasonableness is reflected in the Guide's data security lessons. The lessons, like "Start with Security," and "Control Access to Data Sensibly," are very broad and, in and of themselves, do little to inform a company about whether a particular data security practice is reasonable. That said, the Guide is not so abstract as to be meaningless. The Guide includes summaries of each enforcement action that supports a particular lesson, including the specific facts and practices that the FTC stated were unreasonable in that case.

The Wyndham Litigation

The Guide is clearly an attempt to address criticisms that the FTC has not provided sufficient detail about what it considers an unreasonable data security practice. The most pointed of these criticisms came from Wyndham hotels in the FTC's ongoing data security enforcement action against the hotel chain.[6] The FTC complaint alleges that Wyndham failed to implement reasonable data security practices, allowing Russian hackers to steal significant amounts of customer data.

The FTC prevailed against Wyndham's motion to dismiss in the district court, and the case is now before the U.S. Court of Appeals for the Third Circuit, in *FTC v. Wyndham*, No. 14-3514. Among other points, Wyndham argued that the FTC failed to adequately notify companies through "rules, regulations, or other guidelines" as to what constitutes reasonable data security practices. Without clearly defined standards for data security, Wyndham argues that any enforcement action by the FTC under Section 5 would violate principles of fair notice and due process.

At oral argument on March 3, 2015, the Third Circuit appeared to take Wyndham's concerns about notice seriously. During argument, Judge Thomas L. Ambro asked, "Assuming that complaints and consent decrees or decisions on motions to dismiss are clear enough to give notice when companies read them, how do companies know when they should be reading them? If I were counsel, and I was advising somebody, that wouldn't be the first place I would necessarily look…as to whether there was an unfair [data security] practice." The FTC replied that "careful general counsel" should be looking to and following the FTC's enforcement actions.

Judge Ambro then asked, "Have you informed the public that it needs to look at complaints and consent decrees for guidance?" At oral argument, the FTC was not able to provide a definite answer. It can now. The Guide is a clear communication to the public that the FTC will be looking to its past data security enforcement actions in determining whether or not a data security practice is unreasonable.

The FTC may have been eager to push the Guide out now, before a somewhat skeptical Third Circuit decides the *Wyndham* case. However, while the initiative may aid the FTC in educating the private sector, it should not alter the fate of its case against Wyndham. The guidance is not detailed, prescriptive, or binding, and even it if were more robustly detailed, offering it now does nothing to establish that Wyndham was on notice of FTC expectations at the time of its cyberattacks in 2008–2010. Indeed, this initiative could be seen as confirming the lack of earlier notice. Regardless of the impact on the Wyndham litigation, it is clear the agency is trying to put businesses on notice that they should review the FTC's prior enforcement actions in determining whether a data security practice is reasonable.

Using the Guide

The Guide has the advantages of being brief and accessible. It should be a fairly simple task for general counsels and chief security officers to take steps to make certain that their IT department can affirmatively state that they are not engaging in any of the practices listed in the FTC's guidance. And while it is no safe harbor or shield from liability, an assessment using the FTC's Guide will likely be looked on favorably by the FTC should a data breach occur. More importantly, an assessment is a relatively low-cost way to evaluate cybersecurity and potentially prevent a data breach.

continued on page 3

Consumer Watchdog's "Do Not Track" Petition – A Harbinger of the FCC's New Role as Internet Privacy Cop?

Last month the public interest advocacy group Consumer Watchdog submitted a Petition for Rulemaking to the Federal Communications Commission (FCC or the Commission) asking the agency to initiate a proceeding that would require "edge providers," such as Google and Netflix, to honor "Do Not Track" requests from consumers. The Petition marks the first in what will likely be a series of similar requests to be filed with the Commission asking the agency to broadly assert its authorities to become the privacy regulator for the entire broadband ecosystem. Whether the current FCC leadership will heed the call for such an expansive assertion of the Commission's jurisdiction and how the courts will assess such a view of FCC authority remain unclear. What is clear is that, thanks to the FCC's decade-long effort to adopt network neutrality regulation for broadband providers, privacy advocates now believe they have found a new venue in which to challenge the privacy and information security practices of not only broadband Internet access providers, but all companies that utilize the Internet as part of their business models.

FCC's Open Internet Proceeding and Impact on Privacy Regulation

The FCC's decade-long effort to adopt open Internet rules for broadband Internet access service providers began with its assertion of Title I "ancillary jurisdiction" under the Communications Act (the Act) over providers of "information services" (as broadband was then classified), and was followed by its efforts earlier this year to reclassify broadband as a "telecommunications service" subject to nondiscrimination provisions of Title II of the Act. This effort has greatly blurred the FCC's regulatory distinctions and its ensuing consumer protection obligations between not only broadband service providers and providers of plain old telephone service (POTS), but also providers of broadband infrastructure and the providers of content, applications, services, or devices—known as edge providers—that use such infrastructure.

In the privacy context, two major decisions on net neutrality over the past two years could have profound consequences for the Commission's assertion of jurisdiction—over not only broadband providers, but also edge providers—regarding customer privacy, information and data security, and data breach notification requirements.

First, in the 2014 *Verizon v. FCC* decision, the D.C. Circuit suggested that the Commission could reasonably interpret Section 706 of the 1996 Telecommunications Act as an independent grant of authority to the agency to assert regulatory

continued on page 4

Better Late than Never: FTC Data Security Initiative a Potentially Useful Guide to "Reasonableness" *continued from page 2*

As the FTC has warned, companies should be paying attention to the FTC on questions of data security and cybersecurity. In the absence of clear rules of the road or standards of care, cautious companies can expect the FTC to continue to demand that companies meet its view of "reasonable" security. This initiative is one more signal of what that actually means. ■

For additional information, please contact:

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

[1]FTC Press Release, June 30, 2015 (available at: https://www.ftc.gov/news-events/press-releases/2015/06/ftc-kicks-start-security-business-education-initiative).

[2]FTC Data Security Database (available at: https://www.ftc.gov/datasecurity).

[3]FTC "Start with Security: A Guide for Business" (available at: https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business).

[4]*See, e.g., Prepared Statement of the FTC, Data Breach on the Rise: Protecting Personal Information From Harm,* Before the Committee on Homeland Security and Government Affairs, United States Senate (Apr. 2, 2014) ("The FTC conducts its data security investigations to determine whether a company's data security measures are reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.").

[5] TC Data Security Database (available at: https://www.ftc.gov/datasecurity).

[6]Likewise, the litigants in the LabMD proceeding have hotly contested the FTC's approach, which LabMD has argued amounts to 20:20 hindsight. *See In the Matter of LabMD, Inc.*, No. 9357, 2014 WL 2331045, LabMD's Pre-Trial Brief.

power over providers of information service, which then included broadband service. The court based its decision on Section 706's statutory language directing the FCC to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans" by utilizing measures that "promote competition… or other regulating methods that remove barriers to infrastructure investment," as well as to "take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition." The court then indicated its agreement with the FCC that regulations, such as the open Internet rules, could enable a "virtuous cycle" of innovation and investment, in which new products and services help drive end-user demand for broadband, which in turn drive network deployment and upgrade, which in turn lead to further innovative network uses.

It is important to note that in suggesting the Commission could reasonably construe Section 706 as a direct grant of authority from Congress, the D.C. Circuit identified two limiting principles to distinguish Section 706 from a broader general policy statement: (1) the Commission's subject matter jurisdiction is limited to "all interstate and foreign communication by wire or radio;" and (2) the regulation must be designed to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans." Given that providers of online content, applications, and services have long been treated as providers of "information services" subject to the FCC's Title I authority, advocates of expanded regulations will almost certainly contend that any regulatory power provided by Section 706 can be extended to cover edge providers if the FCC can show that such regulations are designed to encourage the timely deployment of broadband infrastructure.

Second, when the FCC reclassified broadband service from an information service to a telecommunications service subject to the Act's Title II common carriage requirements, it chose not to forbear from applying Section 222 of the Act to broadband providers. Section 222 is the core privacy provision that has traditionally protected a telephone customer's proprietary call-related information from disclosure or use by carriers under certain circumstances. That call-related information is defined as "customer proprietary network information," or CPNI, by the Act. However, the FCC asserted in the 2015 Open Internet Order and a subsequent Section 222 Enforcement Advisory that Section 222, combined with Section 201(b) of the Act, requires a broadband provider to take reasonable measures to protect a customer's sensitive personally identifiable information, beyond just CPNI. The FCC is only beginning to delineate through recent enforcement actions the scope of what constitutes "personal information" that would be protected by Section 222.

In arguing for the application of Section 222's statutory language to broadband providers, the Commission found that "if consumers have concerns about the privacy of their personal information, such concerns may restrain them from making full use of broadband Internet access services and the Internet, thereby lowering the likelihood of broadband adoption and decreasing consumer demand." Therefore, in finding that the protection of customers' personal information may contribute to the "virtuous cycle" of innovation and investment, the Commission made no distinction about whether a consumer's privacy concerns stemmed from the practices of broadband providers or edge providers. Given that the Commission has consistently asserted jurisdiction over edge providers as providers of "information services" and that it views itself as having the authority under Section 706 to adopt Internet privacy regulations, it is not difficult to foresee the FCC extending any of its Section 222 rules for broadband providers to reach edge companies.

Consumer Watchdog's "Do Not Track" Petition and the FCC's Future Role

Perceiving a new-found potential for the Commission to vastly expand its privacy authority following last year's *Verizon* decision and this year's Open Internet Order, Consumer Watchdog filed a petition (the Petition) with the Commission on June 15th requesting the Commission to initiate a rulemaking proceeding to require edge providers to honor users' "Do Not Track" requests. The Petition cites the Commission's own arguments for applying Section 222's privacy protections to broadband providers as the basis for applying "Do Not Track" regulation to edge providers under Section 706. It argues that consumers are concerned about the privacy of their personal information online and that online tracking and data collection practices of edge providers pose the same threat to widespread broadband adoption as any privacy practice of broadband providers. In addition, since edge providers collect the same

continued on page 6

A Privacy and Data Security Checklist for All

Many companies know they have to follow privacy and data security rules. Companies in the health care industry know about Health Insurance Portability and Accountability Act (HIPAA). Financial services companies know about GLB. Some companies know about COPPA or CAN-SPAM.

There are dozens of federal laws, and hundreds (probably thousands) of state laws addressing privacy and data security. Becoming fully educated on all of these laws and how they can apply to a complicated business that deals with significant consumer information is a full-time job, often for a team of people. However, there are certain issues that affect virtually every company, regardless of industry. Here's a quick checklist of privacy and data security topics for any company – and some thoughts about how best to identify and think through your legal obligations.

Employee Data

Essentially, every company has employees. You have personal data about those employees, including (in most cases) their Social Security numbers (SSNs). You also have a wide range of other information about them, including their benefits, their pay, their job performance, and other sensitive or risky pieces of information. You also need to recognize that your employees can create risks as well – in how they perform their jobs, how they protect the personal data that your company maintains, and whether they can be trusted with this information. So, having an effective approach to (1) how personal data about employees is gathered, used, and disclosed; (2) how you will monitor and oversee employee behavior; and (3) effective security practices to control how your employees act is critical. You must understand this data, understand how your employees use data, and what your most significant risks are in this area.

Overall Data Security

Any company that has customers or employees has an obligation to protect the security of sensitive personal data. While there are a series of federal legislative proposals that may create new federal obligations for most companies, the most general set of information security requirements comes from the Federal Trade Commission (FTC). These rules apply generally to every company. While they are not detailed, they require an important focus on effective security practices, ranging from employee access to disposal of paper records to physical security to protecting information networks.

To meet the FTC's requirements for a "reasonable and appropriate" data security program, the company must:

- Develop and implement a written comprehensive information security program that is appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of the customer information at issue.
- Develop a security program that (1) ensures the security and confidentiality of customer information; (2) protects against "any" reasonably anticipated threats to security or integrity of information; and (3) protects against unauthorized access that could result in substantial harm or inconvenience.
- Designate specific employees to coordinate security.
- Identify reasonably foreseeable risks and assess sufficiency of safeguards.
- Oversee service providers by due diligence and requiring contractual security standards.
- Evaluate and adjust its program in light of changes.

These requirements have significant flexibility, but require a thoughtful, proactive security program that stretches across a company's full operations and keeps pace with ongoing changes in both business operations and technological evolution connected to information security. The FTC has just released guidance for businesses addressing these overall data security requirements. The guidance is available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

Cybersecurity

While the FTC's requirements focus on "data security" and the protection of personal information, most companies also should be considering broader cybersecurity protections. While not precisely a "privacy" issue, cybersecurity risks are growing, visible across wide audiences, and applicable to virtually every company. Effective cybersecurity practices will protect your overall information networks at the broadest level – and therefore will protect how your business operates, and all of the data that you maintain, whether personal data or sensitive corporate information. Every company

continued on page 6

A Privacy and Data Security Checklist for All *continued from page 5*

should be acting in this area – and watching carefully for new federal requirements coming down the road in the short term.

HIPAA

While the focus of HIPAA privacy and security rules is on the health care industry, these rules set out obligations that apply to a large volume of companies across many industries. Your company must consider HIPAA's requirements if any of these categories apply to you:

- You are in the health care business as a health care provider or health plan;
- You contract with companies in the health care business (a service provider to these health care companies);
- You contract with companies who contract with companies in the health care business (and onwards downstream indefinitely); or
- You provide health care benefits to your employees (the broadest and least understood category of requirements).

In addition, there are many companies who must pay attention to and analyze HIPAA's requirements because the companies use or disclose health care information, even if they are not directly regulated by the HIPAA rules. Accordingly, while HIPAA is not an overall privacy and security rule, it covers a large range of companies, many of whom may not be aware of their responsibilities.

Website Privacy Policy

For any company that operates a website, it has now become common practice to develop an appropriate website privacy policy. The detail and challenge for these policies varies significantly based on what the website does and what information is collected. While there is a limited number of laws defining specific responsibilities for these policies, at a minimum most companies must (1) ensure that they do not run afoul of the FTC, by making sure that the privacy policy is complete and accurate; and (2) meet the specific requirements of California's law on website privacy practices, including the core components for such a policy and the recent changes involving "Do Not Track" commitments. The key to these policies is to be accurate and thorough, so that individuals (or

continued on page 7

Consumer Watchdog's "Do Not Track" Petition – A Harbinger of the FCC's New Role as Internet Privacy Cop? *continued from page 4*

sensitive personal information as broadband providers, the Petition argues that the Commission must maintain regulatory parity between the edge providers and broadband providers. Consumer Watchdog contends that a failure to do so would in effect grant a regulatory advantage to the edge providers and implicate concerns of market distortions. Finally, the Petition argues that existing remedies under the Federal Trade Commission's (FTC) enforcement authority are insufficient to protect users from online tracking of personal information and that, accordingly, it is necessary for the FCC to adopt enforceable rules with meaningful remedies and penalties. This effort suggests that, for many privacy advocates long frustrated by the FTC's lack of general rulemaking authority, the FCC could become the fertile new ground for advocating in favor of new privacy rules for the Internet.

Whether it's the offering of broadband Internet access service by traditional edge providers such as Google through Google Fiber, or broadband carriers becoming producers of online content and services, such as Verizon's acquisition of AOL, the distinction between broadband providers and edge providers has and will become increasingly blurred. Thanks to the FCC's recent assertion of authority to adopt open Internet rules, the traditional regulatory framework governing the practices of broadband and edge providers also is breaking down. FCC Chairman Tom Wheeler recently stated that the Commission will initiate a proceeding this Fall to promulgate Section 222 rules in the broadband context. Providers of online content, applications, and services should follow the development of that proceeding—along with the disposition of Consumer Watchdog's "Do Not Track" Petition—very closely, as the privacy rules governing the practice of broadband providers may become the baseline rules governing the entire broadband ecosystem. ■

For additional information, please contact:

Shawn H. Chang
202.719.4456
schang@wileyrein.com

Eve K. Reed
202.719.7404
ereed@wileyrein.com

others who may be checking) can understand and evaluate your information sharing practices.

Telemarketing/Email marketing

Most companies do marketing through various channels. For many legislators, regulators, and privacy advocates, marketing (and the use of consumer data for marketing) is one of the "evils" that must be regulated by law.

Marketing activities have been regulated by practice. The Do Not Call laws (including the various federal components and the supplementing state laws) are one of the most successful privacy laws (at least from the consumer perspective), as individuals seem to care about these issues and have in droves signed up for the Do Not Call registries. These issues only affect your company if you conduct telemarketing. If you do, this is a big deal.

On a broader level, the CAN-SPAM law that deals with e-mail marketing has a broader application to a wide range of companies. This law applies to a wide variety of communications, not all of which are obviously "marketing." In addition, this provision applies to both personal and commercial communications, and requires a series of complicated (although relatively modest) steps to comply with the law. Aside from obvious marketers, such as retailers, this law is affecting the business practices of trade associations, universities, professional services firms, and many others. Canada has recently adopted its own version of CAN-SPAM which requires more aggressive front-end consent from individuals. If your company engages in any activity that could be construed as marketing through e-mail, then you must make sure that you are complying with these provisions. You also must evaluate any other marketing practices that you employ, and carefully evaluate how you use and disclose information about your customers.

International

Many companies also need to consider the implications of international data privacy laws. The European Union has led the way on data privacy requirements for many years, and is in the middle of a substantial reevaluation of overall data privacy requirements. More countries add their own laws each year. These laws typically are different from U.S. law. You must pay attention to these international issues – and develop an effective compliance strategy – if (1) you have employees in other countries; (2) you have customers or vendors in other countries; or (3) you rely on data from other countries. Each of these areas creates compliance risks and obligations. Are you using a cloud vendor? Then the international laws may be triggered. Many companies take a quick look at these issues and decide they aren't relevant. That is often wrong, and can be quite risky. Consider this issue carefully in your privacy and security planning.

Vendors

Virtually every company has vendors. Any vendor that receives any personal information from your company – about employees, customers or others – can create legal risks and compliance obligations. You should have privacy and security contracts with these vendors. You should have a plan for monitoring and overseeing their behavior. You should have an approach to vendor risk management. And you need a plan in the event that one of these vendors has a security breach involving your company's information.

Breach Notification

The last "generally applicable" privacy and data security provision involves the laws in virtually every state addressing notification to individuals in the event of a security breach. While these laws apply (in most situations) to only a limited range of personal information (such as Social Security numbers and credit card numbers), these are pieces of information that are held at least to some extent by virtually every company, at least as an employer. Now states are adding other data elements (such as health care information in California) that expand the reach of these statutes. And, since these laws apply to protect individuals residing in a state, the laws apply to any kind of company, large or small, regardless of industry or geographic location. In addition, there are several federal proposals that are working their way through Congress that may make these requirements applicable at a national level.

These laws, at a minimum, require notification to individuals in the event that their personal information is subject to a security breach (as defined by each law). Some laws require notification to state attorneys general, as well. While typically not required by laws, these notifications often (as is becoming a standard practice) incorporate credit monitoring protection and other protections for individuals. There are certain relatively common terms to these laws, but there also are a wide

continued on page 8

variety of state specific provisions that turn any breach involving individuals in multiple states into a significant compliance challenge. Because these notification letters typically become public, they also increase the likelihood of litigation or enforcement, as well as adverse publicity. While the explicit goal of these laws is to provide notification to individuals, so that they can take action as appropriate (for example, to protect against identity theft), these laws also have had the effect of improving overall information security practices.

Action Items

So, what do you need to do about these laws? While companies vary in their knowledge of and planning for these obligations, here are some key steps to consider regardless of your level of regulation or preparation.

Do you know what kind of information you have and what happens to it?

Each company has its own privacy/data security risk profile, based on the industries you work in, the kinds of data you have, and the businesses and consumers to whom you provide services. Every company needs to think about the information you have and what you do with it, as a starting point. These steps include:

- Evaluate any place in your company where you collect, store, and disclose sensitive data (especially SSN and credit card information) – this review of SSN usage is the single biggest risk reduction step you can take.
- Pay attention to employee data as well as customer data.
- Can you identify where this information is disclosed?
- Are you paying attention to the right rules?

Then, once you have a sense of the personal data gathered by your company, think about the regulatory requirements for this information and for your business.

- Are you following the various marketing rules?
- Do you collect information from children online?
- Have you thought about your health care benefits program?
- Are you disposing of sensitive information properly?
- Have you told your employees how you monitor them?
- Do you have an appropriate information security program?

Moving beyond privacy issues, companies then must turn to the generally applicable principles regarding information security. These steps are both required by enforcement practices (for all industries) and detailed legal requirements (for certain industries) and protect your company against lawsuits, customer complaints, and business disruption. In thinking about information security:

- Is someone assigned responsibility for data security?
- Do you have documentation for a regulator?
- Does your program encompass paper and electronic information?
- Have you trained your employees on basic information security?
- Do you have appropriate contracts and oversight of vendors?
- Are you ready to act if there is a problem?

All of these proactive steps are designed, at least in part, to reduce the likelihood of an actual problem. One key element of protecting your company is to make sure that if a problem arises, you are prepared to act quickly to reduce potential harm and protect the company and your customers as much as possible. In considering these issues:

- Do you know who is in charge?
- Do your employees know where to go in the event of a problem?
- Do you have a good program to identity and fix problems?
- Have you evaluated the requirements for security breach mitigation and notification?
- Have you considered whether cyber-insurance or other data breach insurance is right for you?

Last, beyond thinking about your own business activities, you also need to think about your business partners, both your customers and your own service providers. Effective compliance is a legal requirement and a business imperative in dealing with potential customers. For your own vendors,

continued on page 10

Consumer Privacy Advocates Quit the Process on Facial Recognition; NTIA to Press Ahead on July 28

In June, privacy advocates pulled out of a National Telecommunications & Information Administration (NTIA)-convened multistakeholder process intended to develop a voluntary code of conduct for the use of facial recognition technology (FRT). NTIA's process was looking at use cases and prioritizing areas of concern.

FRT can be used for authentication, identification, or tracking, and is being integrated into industries like banking, health care, retail, transportation, and social media. Privacy groups have raised concerns about the technology and its evolution and use. So NTIA undertook bringing stakeholders together to identify basic concerns, possible solutions, and areas of agreement, with the goal of creating a code of conduct.

Participants in NTIA's efforts included several trade associations and individual technology companies. Speaking for consumers were the Center for Democracy & Technology, Center for Digital Democracy, Consumer Federation of America, Common Sense Media, Electronic Frontier Foundation, American Civil Liberties Union, Consumer Action, and Consumer Watchdog. The process had been ongoing for more than a year.

At a June 11 NTIA session, no common ground could be found after the groups became stuck on the basic question of consumer consent to the use of facial recognition technology, and the right to opt out. This was of critical importance to privacy groups, but some industry representatives proposed tabling it in favor of other areas of potential agreement. The advocates decided to leave after a session break, and they followed up a few days later with a letter pulling out of the process. The advocates wrote, "we do not believe that the NTIA process is likely to yield a set of privacy rules that offers adequate protections for the use of facial recognition technology." So they stated they were terminating their participation.

Industry codes of conduct have been adopted and used in other areas related to privacy and consumer protection, but multistakeholder efforts on controversial issues like this may just be too difficult. The objecting consumer groups wrote that they "hope that our withdrawal signals the need to reevaluate the effectiveness of multistakeholder processes in developing effective rules of the road that protect consumer privacy – and that companies will support and implement." It remains to be seen whether such groups will seek to rejoin the NTIA effort, or shift their focus to regulators and policymakers. NTIA announced that it will convene the next meeting of the facial recognition multistakeholder group on July 28. ■

For more information on facial recognition issues, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

SPEECHES & EVENTS

Tip of the Spear: The Latest on Cybersecurity and Hacking, from the FTC, Congress and Courts
Megan L. Brown, Speaker
Baton Rouge Bar Association Bench Bar Conference
July 25, 2015 I Point Clear, AL

Roundtable on How Privacy Issues Affect the Lawyer
Megan L. Brown, Panelist
Baton Rouge Bar Association Bench Bar Conference
July 25, 2015 I Point Clear, AL

Cybersecurity in the HIPAA Context
Kirk J. Nahra, Speaker
Cybersecurity Preparedness for the Healthcare Sector: How to Implement the Proper Internal Controls for Network and Data Security
August 25, 2015 I New York, NY

service providers create significant risk and must be overseen effectively. Make sure you are thinking about the following points:

- Assess the company's role as a vendor and as a company that hires vendors.
- Develop an "off-shoring" approach.
- Develop a realistic vendor approach for due diligence, oversight, monitoring, and contracting that, for the most part, is "one size fits all."
- Make sure company employees are aware of these responsibilities – and don't take on too much or give away too much.

Final Thoughts

Privacy and data security are not going away. New laws and regulations are placed on the books regularly. Enforcement, while still modest, is growing. Litigation also is growing. And ongoing developments involving the risks and benefits of "big data" present the certainty that the complexity of this environment will continue to grow.

Effective privacy and data security practices are an essential component of the business operations of any business. There is a need for broad understanding of these issues across senior management (and the Board of Directors), and a risk if information practices are not handled carefully and thoughtfully. While the challenges may seem daunting, the most important step is to understand your general level of exposure, and to undertake a creative, thoughtful, and thorough assessment of your privacy and data security activities, so that these growing risks can be managed effectively. ■

For more information, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Shawn H. Chang	202.719.4456	schang@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
Eve K. Reed	202.719.7404	ereed@wileyrein.com