Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | October 2016

Introduction

This month we tackle a series of issues helping to frame the privacy and security debate as we move towards 2017. While we continue to read daily about security breach incidents and increasing methods of reducing security risk, Megan Brown writes about a recent report from the National Institute of Standards and Technology (NIST) that addresses "cyber fatigue." Megan and her colleagues, Madi Lottenbach and Christen B'anca Glenn, also look at a series of NIST initiatives related to digital security and privacy. Megan and Madi then review what may be the most significant new privacy regulation to address in 2017 – the Federal Communications Commission's (FCC) new broadband privacy proposal, which likely will be finalized shortly. Last, I look at some of the Federal Trade Commission's (FTC) most recent actions and efforts related to data security, and look ahead to some important issues to watch in this area.

As always, please let me know if you have questions or comments on any of these topics, or if we can be of assistance in connection with any of these developments. Please let me know if you have thoughts on topics you would like us to address in future issues of *Privacy in Focus*. I can be reached at 202.719.7335 or knahra@wileyrein.com. ■

-Kirk Nahra, Privacy Practice Chair

The FTC and Data Security

The Federal Trade Commission (FTC) has long been known as the nation's leading data security enforcement agency, with a portfolio of more than 60 enforcement actions since the groundbreaking BJ's Wholesale settlement in 2005. At the same time, in the past few years, the FTC also has faced significant challenges to its claimed authority in this area. What can we expect to see in 2017 and beyond from the FTC about data security? There are three main avenues to watch in the year ahead.

FTC Program Development

For about a decade, the FTC built its data security enforcement record through a series of enforcement actions, arising from various scenarios related to security breaches and other security concerns, where companies allegedly failed to implement reasonable and appropriate data security measures. These cases were initiated by the FTC through its investigatory authority, and then typically resulted in settlements with the affected companies. Through these actions, the FTC built what Professors Solove and Hartzog have called "the common law of privacy." See Solove and Hartzog, "The FTC and the New Common Law of Privacy," 114 Columbia Law Review 583 (2014). Relying on its general enforcement authority under Section 5 of the FTC Act, and utilizing the program it developed under its specific Gramm-Leach-Bliley Act (GLB) authority (where the FTC has residual authority over "financial institutions" that are subject to the law but not directly subject to enforcement by another federal agency), the FTC developed data security principles through its pursuit of individual cases. The FTC's cases relied on the key prongs set out under the GLB "safeguards" rule. Standards for Safeguarding Customer Information;

continued on page 2

ALSO IN THIS ISSUE

Final Rule – 16 CFR Part 314 (May 23, 2002). This standard requires companies to:

- Designate an employee or employees to coordinate the information security program.
- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
- Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- Oversee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring your service providers by contract to implement and maintain such safeguards.
- Evaluate and adjust your information security program in light of the results of the testing and monitoring of the program, any material changes to operations or business arrangements, or any other circumstances that the company knows or has reason to know may have a material impact on the information security program.

For many years, and more than 60 data security actions, the FTC moved forward to build its common law through settlements with affected companies. Relying on its authority from 15 U.S.C. § 45(a), which prohibits "unfair ... practices in or affecting commerce," these settlements identified problematic practices and provided guidance to other companies on how the FTC viewed the concept of "reasonable and appropriate" data security.

Challenges to FTC Authority

Then, after all these settlements, Wyndham Hotels challenged the FTC's overall authority in this area, asserting (among other arguments) that Section 5 did not authorize the FTC to require such data security practices. After hotly contested litigation, the FTC prevailed over Wyndham, through the Third Circuit's decision in *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015). Essentially, the court held that there were data security practices that could be subject to enforcement under 15 U.S.C. §45(a), and that Wyndham had sufficient notice of these practices to make enforcement constitutionally appropriate.

While the Wyndham case was proceeding, the FTC faced a second challenge, from LabMD. The LabMD case (which has an extremely complicated and continuing procedural history) originally presented two issues. First, like Wyndham, LabMD asserted that the FTC had no authority in this area. Then, LabMD also asserted that the FTC was not able to take action against an entity regulated by the Health Insurance Portability and Accountability Act (HIPAA). (LabMD is a "covered entity" under the HIPAA Rules, subject to primary enforcement from the HHS Office for Civil Rights.) While these challenges were proceeding, an FTC Administrative Law Judge (ALJ) denied FTC authority on a third ground—ruling that the FTC could only act in situations where there was consumer harm. While that ALJ decision (not surprisingly) was overturned by the FTC commissioners, these issues are continuing in litigation.

So, in 2017 and beyond, we can expect continued attacks on the FTC's authority to pursue cases in this area, on both general grounds related to overall notice and consumer harm, and in connection with whether specific activities constitute unfair practices. While many companies will still find a settlement preferable (because the settlement terms tend to impose a requirement for reasonable and appropriate security and do not typically involve monetary payments), some companies will follow Wyndham and LabMD in making the FTC work harder on its cases.

Legislative Developments

For much of this period where it has engaged in data security enforcement activity, the FTC also has pursued a legislative agenda. This approach has included two related concepts—a federal data breach notification law and a proposal for statutory standards related to data security. The data breach proposal could fill in existing gaps in the law today, by creating a consistent and broadly applicable federal standard rather than relying on a complicated variety of state laws applicable in most (but not all) states. In addition, a national approach with preemption of state laws could create consistency and reduce ambiguities and compliance challenges, to the benefit of both companies and consumers.

continued on page 3

Despite maintaining in litigation that it has authority to pursue these data security cases, the FTC also has asked Congress to implement national data security standards. The FTC's desire for statutory data security standards has always been somewhat odd. The FTC has pursued its generally applicable data security enforcement program without expressly applicable statutory standards. It has asserted—aggressively when challenged—that it has the authority to pursue these cases. If the Wyndham or LabMD challenges had resulted in the denial of FTC authority, the need for a statute would have become acute. Now, with the FTC (so far) maintaining its authority, the need for a law is less clear. Nonetheless, the FTC's current commissioners (just three because of appointment tensions) all recently testified before Congress on the need for these proposals. To date, Congress has been unmoved by these pleas on both legislative ideas (and has so far been unmoved by the broad variety of major security breaches). While proposals are written and some move through committee, there has been little progress on these laws in many years. So, with a new President and Congress coming in 2017, we will watch to see if there is movement in this area. Any limitations on the FTC's authority through ongoing litigation should push Congress more assertively to enact legislation on these issues.

Regulatory Developments

There is a third prong of this debate which has received less publicity—and which may ultimately have a broader impact on how the FTC defines its data security authority. As part of a "systematic review of all current Commission regulations and guides" the FTC has initiated a regulatory proceeding to review its standards under the Gramm-Leach-Bliley rule. 81 Fed. Reg. 61632 (Sept. 7. 2016). The first step in this process is a "Request for Comment" related to the current GLB Safeguards rule, where the FTC seeks input on a broad variety of issues involving the current standards, primarily whether the rule is too strong or too weak, and what should be done to change the Safeguards rule in the future. Companies have until November 7, 2016, to submit their comments.

Presumably, the FTC will move forward with some proposed changes to this rule. The big question is whether the FTC will move from a relatively general standard under GLB (with the general parameters identified above), to create a more prescriptive approach. If it does this for GLB requirements for "financial institutions," and GLB was the standard for the FTC's "non-GLB" enforcement activities, will these new GLB requirements become part of the broader enforcement arsenal? And if so, will this result in even more challenges to the FTC's authority from affected companies? Companies in all industries should watch this current regulatory proceeding (which presumably will result in a proposed new rule as a next step, following the request for comments), as this new rule likely will define the standards that the FTC will apply not only in connection with GLB-regulated entities but also on a broader basis across its entire enforcement authority.

Conclusion

The FTC, while not alone in privacy and data security enforcement, remains the most visible and active regulator of a broad variety of privacy and data security practices. While its authority remains under challenge, the agency continues to investigate a vast array of data security practices. While its overall set of cases certainly provides a good road map for appropriate data security practices for virtually all companies, the FTC also continues to break new ground with each new settlement. Companies in every industry—including those whose only involvement with personal data is through company employees—should be paying close attention to these FTC developments, and taking action to ensure that the company is engaged in appropriate practices to protect the personal data held by the company. ■

For more information please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

Digital Security and Privacy Are Being Addressed Across the Federal Government

Security and privacy are complementary concepts; without security, consumers cannot have privacy. Privacy and security—particularly in our increasingly connected economy—are complex and require agile responses and engaged consumers, who update their devices and use good cyber hygiene. Given the number of diverse global contributors to the tech sector, from OS providers to manufacturers, to application developers and network operators and end users, there is no single solution or approach.

Sweeping and difficult policy issues will not soon be resolved in Congress, but in the meantime, several activities are underway to address connectivity, security, and privacy in the digital ecosystem.

- The National Telecommunications and Information Administration (NTIA), located within the U.S. Department of Commerce, will address Internet of Things and consumer expectations about security in Austin, Texas on October 19, 2016. NTIA has convened a multistakeholder process concerning *Internet of Things Security Upgradability and Patching*. NTIA says that there has "sometimes been limited consideration for supporting future security patches, even though many devices will eventually need them," and "manufacturers can struggle to effectively communicate to consumers the security features of their devices." This process will consider how to develop a common lexicon or best practices. More information can be found here.
- The National Institute of Standards and Technology (NIST) is examining mobile threats and security across the federal government, creating a Mobile Threat Catalogue that purports to list varied threats across mobility. Some can be addressed through simple end-user cyber hygiene, while others require nation-state engagement to address global issues and trust. Comments are being taken and are due November 10, 2016. More information can be found here.
- NIST is looking at privacy controls and privacy risks associated with security controls. It proposes adding to existing security guidance "privacy considerations that are relevant to, or arise from, security controls." It is updating NIST Special Publication 800-53, Appendix J. NIST has held public workshops and the comment period closed on September 30, 2016. Information can be found here.
- NIST released on October 4, 2016, Special Publication 800-150, a Guide to Cyber Threat Information Sharing, which "provides guidelines for establishing and participating in cyber threat information sharing relationships. This guidance helps organizations establish information sharing goals, identify cyber threat information sources, scope information sharing activities, develop rules that control the publication and distribution of threat information, engage with existing sharing communities, and make effective use of threat information in support of the organization's overall cybersecurity practices." This publication addresses privacy and the potential impacts on privacy of various sharing activities. ■

For more information on these and other digital security matters, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Madi Lottenbach
202.719.4193
mlottenbach@wileyrein.com

Christen B'anca Glenn
202.719.3753
cglenn@wileyrein.com

FCC Prepares to Adopt Rules on Broadband Privacy

The Federal Communication Commission (FCC or Commission) will vote on whether to adopt rules for broadband privacy during its next open Commission meeting on October 27, 2016. This comes after heated debate at the FCC and on Capitol Hill, and pertinent developments in the U.S. Court of Appeals for the Ninth Circuit.

On October 6, 2016, FCC Chairman Wheeler announced in a blog post that he had circulated a draft Order to adopt broadband privacy rules taking into account feedback received in response to the Commission's Notice of Proposed Rulemaking (NPRM). Although the proposed Order would still regulate privacy and security, and still single out Internet service providers (ISPs), the Chairman indicated that the proposed Order differs from earlier proposals in that it will align more closely with the approach long taken by the Federal Trade Commission (FTC).

Details remain uncertain, but the FCC has released a Fact Sheet summarizing the draft Order. According to the Chairman:

- "Under the proposed rules, an ISP would be required to notify consumers about what types of information they are collecting, specify how and for what purposes that information can be used and shared, and identify the types of entities with which the ISP shares the information."
- "In addition, ISPs would be required to obtain affirmative 'opt-in' consent before using or sharing sensitive information. Information that would be considered 'sensitive' includes geo-location information, children's information, health information, financial information, social security numbers, web browsing history, app usage history, and the content of communications such as the text of emails. All other individually identifiable information would be considered non-sensitive, and the use and sharing of that information would be subject to opt-out consent."
- "The proposed rules also require ISPs to take reasonable measures to protect consumer data from breaches and other vulnerabilities. If a breach does occur, the rules would require ISPs to take appropriate steps to notify consumers that their data have been compromised."

The draft Order therefore would, among other things, adopt a new definition of "sensitive information" that was not previously considered or discussed in the original NPRM. Industry members and others will not have an opportunity to comment on the revised definition before the Commission's vote at the end of the month.

Background

The FCC voted, 3-2, to release a Notice of Proposed Rulemaking on April 1, 2016, proposing to extend a heightened-form of its Customer Proprietary Network Information (CPNI) rules to broadband providers and adopt new data security rules. The NPRM did not propose to apply these rules to edge providers. Comments were due on May 27 and reply comments on July 6.

Industry Opposition

Industry comments explained that the proposed unbalanced regulation will harm the speed and availability of broadband service, while edge providers continue to use consumer information without limit. Industry commenters also took issue with proposed data security rules, which would require protections for all consumer information without making the critically important distinction between sensitive and non-sensitive consumer information. Several commenters have therefore urged the Commission to pursue a policy mirroring the FTC model—a case-by-case and technology-neutral approach to privacy enforcement, evaluating the sensitivity of data and personalized nature of customer communications at issue. In a June blog post, CTIA, CTA, Mobile Future, USTelecom, and the Wireless Internet Service Providers Association called on the FCC to correct "Chairman Wheeler's plan to abandon the FTC's well-tested and effective approach to online privacy and replace it with heightened and inconsistent rules for broadband providers."

Federal Trade Commission Concerns

In response to the FCC's NPRM, the FTC filed comments identifying several concerns with the FCC's approach. The FTC stated it is "not optimal" that the proposed privacy rules would apply exclusively to broadband providers. The FTC also cautioned that the FCC's overly broad proposal, including its definition of "personally identifiable information," could unnecessarily limit the use of non-sensitive data to the detriment of consumers. "While almost any piece of data could be linked to a consumer, it is appropriate to consider whether such a link is practical or likely in light of current technology." The FTC further questioned features of

continued on page 6

the FCC's proposed consumer "opt-in" requirements, recommending the FCC consider instead adopting the FTC's model, which "calls for the level of choice to be tied to the sensitivity of data and the highly personalized nature of consumers' communications in determining the best way to protect consumers."

Criticism from Capitol Hill

The U.S. Senate Commerce Committee has voiced serious concerns as well, both during its July hearing on the broadband privacy NPRM and its FCC Oversight Hearing in September. Noting the FTC's well-established record for protecting consumer privacy, Chairman Thune and others questioned the wisdom of departing from the FTC's approach. And during the FCC Oversight hearing, Chairman Thune severely criticized Chairman Wheeler for "pursu[ing] a highly partisan agenda that appears driven by ideological beliefs more than by a sober reading of the law." He also pointed out that under Chairman Wheeler's leadership in the last three years, there have been nearly twice as many partisan votes than in the previous 25 years combined.

Decision by the Ninth Circuit U.S. Court of Appeals

Meanwhile, the U.S. Court of Appeals for the Ninth Circuit recently held that the FTC lacks jurisdiction to sue AT&T for allegedly failing to adequately disclose its data throttling policy to customers with unlimited data plans—an act constituting an unfair and deceptive practice according to the FTC. The court reasoned that the FTC's common carrier exemption is status-based, precluding any FTC action against common carriers, instead of activity-based, which would only preclude action on service-related activities of common carriers. FTC Chairwoman Edith Ramirez indicated during an FTC Oversight Hearing in September that the agency will seek en banc review of the decision.

Should the decision stand, it could have implications for the FCC's broadband privacy proposal. Representatives from industry, Congress, and federal agencies have called on the FCC to defer to the FTC or, at a minimum, pursue an FTC-based approach to privacy. The role of the FTC in broadband privacy, however, could shrink if the court's opinion stands.

Industry will continue to watch developments at the FCC in the privacy and security arena. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Madi Lottenbach
202.719.4193
mlottenbach@wileyrein.com

Wiley Rein is excited to announce the launch of our Internet of Things (IoT) blog, **WileyConnect**. The blog is a source for timely updates and thoughtful insights about technology law, litigation, regulation, and policy affecting innovators and consumers across the IoT ecosystem. Recent posts have focused on topics such as automated vehicles, cybersecurity guidelines, and efforts to deliver pizzas and burritos by drone. Visit WileyConnect to subscribe today!

WileyConnect Blog Launch Bash: On Thursday, October 27, 2016, Wiley Rein will be celebrating the launch of WileyConnect at the Wiley Rein office in Washington, DC. **For event details and to RSVP to our TECHTASTIC blog launch bash, click here.**

Consumer Cyber Fatigue: Concerns Implicate IoT, Mobile Privacy, and Security

The National Institute of Standards and Technology (NIST) researchers have noticed something the private sector has known for a while: Consumers get tired of being asked to remember ever-lengthier and changing passwords, use two-factor authentication, and answer challenge questions. As policymakers look to privacy and security in various settings, including mobile, broadband and Internet of Things (IoT), connected cars, and other areas, security must be user friendly and flexible.

In a recent post, NIST highlights a study with surprising—if common-sense—results. Inundated with information about security breaches, as well as advice about mitigations, "a majority of the typical computer users" had "experienced security fatigue that often leads users to risky computing behavior at work and in their personal lives." (The study is published in *IT Pro*, Sept./Oct. 2016.)

Researchers found that consumer behavior seen as "irrational" to security experts may be reasonable given consumers' overload and lack of confidence that burdensome steps will protect them from a barrage of attacks that seem like someone else's responsibility.

This finding validates comments filed in the Federal Communications Commission's (FCC) recent broadband privacy proceeding, in which the agency proposed a variety of prescriptive security obligations that overlooked varied consumer preferences and evolving approaches. As one commenter, Consumers' Research, noted, "over-notification is not just irritating," it can harm consumers by "making them less likely to pay attention." Consumers' Research Comments, FCC Dkt No. 16-106. The tech sector shares those concerns: Repeated notices leave consumers "desensitized, tuned out and unable to differentiate" between important and less important information. Consumer Technology Association Comments, Dkt. No. 16-106. It is better to leave solutions to the market and avoid mandates that lead to over-notification or lock in static solutions.

NIST researchers suggested three principles that might help combat consumer security fatigue: "limit the decisions users have to make related to security; make it easy for users to do the right thing related to security; and provide consistency (whenever possible) in the decisions users need to make." These principles can help the private sector, but should not drive government mandates or limitations on choice. User groups will have different needs, preferences, and abilities. As a result, authentication technologies (from biometrics to adaptive authentication to multifactor) are evolving to address these concerns. Each solution has its own tradeoffs, so enterprises and consumers should have flexibility.

In the end, NIST should look to the role that sustained, clear consumer education could play to combat these trends. This study reinforces how challenging this area is, and how poorly suited it is to mandates or single solutions. More research and input will help identify workable solutions that help consumers and improve security. ■

For more information on these and other digital privacy and security challenges, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

SPEECHES & EVENTS

Cyber Threats Faced by Public Entities
Benjamin C. Eggert, Speaker
Public Risk Management Association
October 19, 2016 | Online Webinar

Non-HIPAA Health Data
Kirk J. Nahra, Speaker
Privacy + Security Forum 2016
October 25, 2016 | Washington, DC

WileyConnect Blog Launch Bash
Wiley Rein LLP
October 27, 2016 | Washington, DC

Post-Election Review: Health Care Privacy and Security Under a New Administration
Kirk J. Nahra, Speaker
Bloomberg BNA
December 6, 2016 | Online Webinar

Managing Big Data in an Evolving Legal Environment
Kirk J. Nahra, Speaker
AHLA's Institute for Health Plan Counsel
December 9, 2016 | Chicago, IL

Acclimating to Changing Regulatory, Legislative & Enforcement Activities and Breach Notification Requirements
Kirk J. Nahra, Moderator
ACI's 21st National Advanced Global Legal and Compliance Forum on Cyber Security and Data Privacy & Protection
January 30, 2017 | Washington, DC

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Christen B'anca Glenn	202.719.3753	cglenn@wileyrein.com
Madi Lottenbach	202.465.4193	mlottenbach@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com