Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | April 2016

Introduction

This month's issue continues to demonstrate the breadth and variety of challenges that are arising for privacy professionals (a point also demonstrated by the enormous Global Privacy Summit sponsored in early April by the International Association of Privacy Professionals and the founding by IAPP of the Privacy Bar Section for privacy lawyers). We cover litigation developments related to whether data breaches in the context of certain electronic medical records can trigger False Claims Act liability. We address another important case in the ongoing legal developments related to insurance coverage for privacy and security claims. We also look at the continuing evolution of privacy policy being driven by the Internet of Things, through NTIA's "Request for Comment" on the federal government's appropriate role in privacy policy in this emerging area. We cover the FCC's Notice of Proposed Rulemaking to establish a new consumer privacy framework (Comments are due in May). Last, for the health care industry, I look at the early steps in Phase 2 of the HIPAA audit process, currently underway from the HHS Office for Civil Rights, including an early assessment of how companies best can prepare for these potentially burdensome audit inquiries.

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

HIPAA Phase 2 Audits Begin: Prepare but Don't Panic

The HIPAA community has been concerned about an audit process since the HITECH mandate by Congress that the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) implement an effective audit program. Phase 1 was completed several years ago. Other than for the unfortunate few who were selected for the highly burdensome audit process, this program was uneventful and not very useful. Now, Phase 2, after several fits and starts, seems to be beginning. What do we know for sure about this process? Should covered entities and business associates be concerned? And, if not concerned, why should they be preparing for these audits even if there is only a small chance of being audited?

Phase 1

The HITECH law required OCR to conduct periodic audits of covered entities and business associates to gather information about the compliance activities of the health care industry. Phase 1—conducted in 2011 and 2012—looked at 115 covered entities. The audits of this unlucky group of 115 were extensive and burdensome. HHS gathered information about these entities, and primarily seemed to use the results to develop a "better" audit protocol going forward.

What We Know about Phase 2

- **What is actually underway now?**

Now, several years later, Phase 2 seems to be beginning. While OCR has stated that "Phase Two . . . is currently underway," what is *actually* underway at this point is the beginning of an effort to gather information about potential auditees. OCR has sent letters and emails to various covered entities, primarily at this point

continued on page 2

ALSO IN THIS ISSUE

to confirm or gather contact information for subsequent communications. From these initial efforts, OCR will identify "pools of covered entities and business associates that represent a wide range of health care providers, health plans, health care clearinghouses and business associates." In the second part of Phase 2, a questionnaire will be sent to the potential auditees, to gather data about the size, type and operations of each entity. This inquiry—directed initially at covered entities—also will include the identification of business associates for a subsequent stage. OCR will select its initial pool of covered entity auditees from these initial data collection efforts. HHS has made clear that OCR "will not audit entities with an open complaint investigation or that are currently undergoing a compliance review."

- **What about the substance of the audits?**

OCR has moved from the very intensive "on site" audits in Phase 1 to a Phase 2 approach dominated by "desk audits." These will involve primarily a review of policies and procedures. The first round of these desk audits will involve covered entities. A second round will address business associates. Both of these rounds are projected by OCR to be completed by the end of 2016 (although all date projections so far have been incorrect).

It also is clear that not every audit will be the same. Some audits will review the Privacy Rule, some will address the Security Rule, some may focus on the Breach Notification Rule and (apparently) some may cross these lines. The auditees "will be notified of the subject(s) of their audit in a document request letter."

The process will involve an initial email notification of "selection" as an auditee, including a request to provide documents and other data in response to a specific document request letter. *Selected companies may have only 10 business days to respond to this initial request.* For most of the "desk audits," OCR will review these documents (employing "common audit techniques"), and will share "draft findings" with the entity. Auditees will have "an opportunity to respond to these draft findings [and] their written responses will be included in the final audit report." Depending on the results of the audit or other factors, there may also be follow-up "on-site" audit visits in some situations.

- **Is this an enforcement process?**

No. OCR has made clear that the "audits are primarily a compliance improvement activity." The overall process "will enable OCR to better understand compliance efforts with particular aspects of the HIPAA Rules." In addition, "[*g*] *enerally (emphasis added)*, OCR will use the audit reports to determine what types of technical assistance should be developed and what types of corrective action would be most helpful." Also, through the audit process, "OCR will develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches."

However, throughout this process, HHS has reserved the right to turn a particular entity's audit results into a compliance investigation. "Should an audit report indicate a serious compliance issue," OCR may initiate a compliance review to further investigate.

What You Should Be Doing Now

- **Is panic appropriate?**

Definitely not. Throughout 2016, OCR will conduct desk audits of roughly 200 companies, covering a broad range of covered entities and business associates. The likelihood of being selected is small. Moreover, while there clearly will be some burden associated with providing audit responses, HHS has also made clear that its intention is that Phase 2 be less burdensome to the affected entities than Phase 1 was.

- **But what about enforcement?**

While OCR has consistently reserved its right to take enforcement action against auditees, the likelihood of this enforcement is small. The goal of this overall audit process is to gather information about the state of the industry. Enforcement clearly is not a primary purpose. OCR has hundreds (and probably thousands) of open complaints and breach reports where it can engage in enforcement investigations (and it does not have sufficient resources to move these investigations quickly). It does not need the audit process to expand this pool.

The only realistic scenario for potential enforcement would involve a situation where there is an almost complete failure of compliance activity from an auditee. If your company's response to an audit letter is "what is HIPAA," that could be a problem. Much beyond that, the risk of enforcement action is small as a result of these audits.

- **So I shouldn't even pay attention to this?**

Wrong. This is an important effort, just not one that likely will lead to specific enforcement. First, if you are selected, you will have only a short window to provide information. It will be useful to take measures now to gather information about your policies and procedures (as well as a list of your business associates and subcontractors) to be prepared to respond to an audit request.

More significantly, the steps needed to prepare for an audit are exactly the same steps that you would need to take in connection with an investigation. HHS conducts far more investigations—based on complaints, breach reports

continued on page 3

and otherwise—than it will ever conduct audits. *Your company's likelihood of facing a compliance investigation is far greater than the risk of an audit.* And, unlike the compliance audit, enforcement is a real possibility in a compliance investigation (even though OCR—for the time being—remains reasonable and understanding of sincere compliance efforts, even in investigations). So, preparing for an audit not only will prepare you for the audit—but will also prepare you for the far more likely and risky response to a compliance investigation.

- **What should we expect from the overall audit process?**

Phase 1 was not particularly helpful, at least to the health care industry. While HHS has issued certain guidance over the past few years (including some helpful documents in recent months, such as the guidance for mobile app developers on when HIPAA applies and the individual access guidance), there is little indication that the audit program played any part in this guidance. We can expect more this time, but likely not too much.

We also can expect that the industry will be subject to some real criticism. Presumably, covered entities will do reasonably well on the Privacy Rule (although HHS remains concerned about compliance with relatively simple elements such as the individual access right). On the Security Rule, I expect more difficulty, mainly because compliance with the documentation components of the Security Rule is very hard. These Security Rule failures—from the core risk assessment element to various detailed processes—have been the failures that have resulted in enforcement activities in recent years.

The business associate community remains an enormous wild card on HIPAA compliance. This community covers an enormous range of entities, from some of the largest companies in the world to small entities and even individuals. Moreover, involvement with PHI and ePHI varies tremendously, independent of entity size (a small consulting firm might be focused on health care claims data, while an enormous business may provide services to only a handful of health care companies with very limited involvement in ePHI). Accordingly, I expect it will be difficult for HHS to draw conclusions across the board for business associates. In addition, particularly on the Security Rule, I expect business associates of virtually all stripes to fare badly in an audit process. For many companies—particularly those that are not exclusively or primarily in the health care industry—this failure may not reflect a failure of actual security, but will be a failure to meet HIPAA's process and documentation requirements. Audits aside, HHS is going to face a real challenge over the next few years concerning how to apply HIPAA's standards to enforcement investigations involving business associates.

Conclusion

So, Phase 2 is underway. It is real, and it is relatively important. It is moving, although not quickly, and will be a significant undertaking for any entity selected for the audit program. For the broader range of covered entities and business associates—the overwhelming portion of the industry that will not be selected for an audit—this process should provide a motivation to get your ducks in a row, to evaluate your HIPAA compliance activities and to be prepared in the event of a much more risky AND more likely enforcement investigation.

For more information on the Phase 2 audit process and other HIPAA developments, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

NTIA Seeks Comments on the Federal Role in IoT

The National Telecommunications and Information Administration (NTIA) announced a new federal inquiry seeking public comment on the current technological and policy landscape for the Internet of Things (IoT), with an eye toward issuing a "green paper" that would identify possible roles for the federal government in this area. The Request for Comments broadly covers a wide range of issues that could be relevant to the interests and operations of companies in a variety of market segments that are poised to drive IoT growth, including, among others, markets for consumer goods, unmanned aircraft systems, eHealth, smart transportation (connected cars), energy distribution (smart grids), smart cities, public safety, industrial and manufacturing, agricultural and resource management, and big data analytics. The Request poses 28 questions on IoT for consideration. Comments by interested stakeholders are due May 23rd.

The new inquiry is part of the U.S. Department of Commerce's Digital Economy Agenda, which seeks to create a coordinated, strategic framework for the

continued on page 4

Department's Internet-related work. NTIA will use the input it receives to build on the Department's broader agenda promoting economic growth and opportunity to help develop an approach that will foster IoT innovation. Specifically, after if receives comments, NTIA will publish a green paper identifying key issues affecting deployment of these technologies, highlighting potential benefits and challenges, and outlining possible roles for the federal government in fostering the advancement of IoT technologies in partnership with the private sector. A "green paper" is a tentative government report on policy proposals for discussion without a commitment to action; final policies are released in a "white paper."

Why Businesses Should Care

NTIA's inquiry is poised to shape federal policy responses on IoT. The private sector should engage in this proceeding because NTIA activity is likely to shape emerging domestic and international regulatory and policy issues in IoT. Because there is no uniform federal policy in IoT, or in privacy and security generally, thought-leadership by non-regulatory agencies like NTIA will fill a void and could be particularly influential.

NTIA, in the Department of Commerce, is an Executive Branch agency charged with advising the President on telecommunications and information policy issues. Among its many activities, NTIA develops "policy on issues related to the Internet economy, including online privacy, copyright protection, cybersecurity, and the global free flow of information online." It does this in part by seeking public comment, and through multistakeholder proceedings to evaluate issues. A major recent NTIA focus has been on privacy and security. Examples include facial recognition privacy practices, considerations related to unmanned aerial systems, and mobile applications, to name just a few.

NTIA's papers are influential internationally, because NTIA is often seen overseas as the U.S. "Ministry" of communications, despite being a relatively small agency. NTIA is the sole U.S. agency that oversees ICANN/domain name issues, and the IoT item specifically requests comment on whether there are domain name issues implicated in the IoT. Further, NTIA administers federal use of spectrum, and coordinates with the Federal Communications Commission (FCC) on commercial allocations, which will impact the reach of IoT innovation.

NTIA's analysis and advocacy play an increasingly influential role in raising the profile of issues, and providing support for regulatory proposals. One recent example is a major Privacy NPRM issued by the FCC, which directly relies on "best practices regimes, including those proposed by the FTC and the National Telecommunications and Information Administration (NTIA)." The FCC is drawing from NTIA efforts to develop a Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices, among other third party efforts, agency guidance and reports. NTIA work has driven best practices and policy on varied technology law and policy issues.

Private industry should engage in NTIA efforts, which will drive legal, regulatory and policy decisions affecting IoT. Activities at NTIA and other non-regulatory agencies can impact federal policy but are not governed by administrative law and are not subject to judicial review; private participation is therefore critical to ensure full consideration.

A brief summary of the Request is provided below. At a high level, the Request seeks comment on the challenges and opportunities arising from IoT; the technological issues that could hinder IoT development, such as spectrum availability, interoperability, and the availability of network infrastructure; cybersecurity, privacy, and other consumer protection concerns; the appropriate role for government in these issues; and international engagement on IoT.

Summary of Request for Comments

NTIA seeks public comment on the following IoT issues:

General. NTIA generally seeks public comment on whether the challenges and opportunities arising from IoT are similar to those that governments have previously addressed with other technologies. NTIA also asks how it should define IoT in light of several competing definitions, and whether there are ways to divide or classify the IoT landscape to improve the precision with which public policy issues are discussed. Finally, NTIA seeks comment on current or proposed laws, regulations, or policy positions on IoT that strike an appropriate balance between fostering growth and protecting users, and whether there have been any significant studies of the IoT policy landscape or whether any future studies are planned.

Technology. Recognizing that technology is the heart of IoT, NTIA asks what technological issues may hinder the development of IoT. The Request specifically highlights interoperability, insufficient/contradictory/proprietary standards/platforms, spectrum availability and potential congestion/interference, and the availability of network infrastructure. NTIA also asks what governments can do to help mitigate these technical issues, and whether government/private sector partnerships may be beneficial.

Infrastructure. NTIA seeks comment on how IoT will place demands on existing infrastructure architectures or business models, and whether there are ways to prepare for or minimize IoT disruptions to these infrastructures. NTIA also asks what role governments could play in bolstering and protecting the availability and resiliency of

continued on page 5

these infrastructures to support IoT.

Economy. Positing that IoT already has begun to alter the U.S. economy, NTIA asks how the government should quantify and measure the IoT sector; what impact the proliferation of IoT will have on industrial practices; and what impact the growth of IoT will have on the U.S. workforce.

Policy Issues. NTIA seeks comment on the main policy issues that affect or are affected by IoT, and how the government should address or respond to these issues. The Request particularly highlights cybersecurity, privacy, and other consumer protection concerns.

International Engagement. The Request notes that efforts already are underway in foreign jurisdictions, standards organizations, and intergovernmental bodies to explore the potential of, and develop standards, specifications, and best practices for IoT. Given this, NTIA seeks input on how best to monitor and/or engage in various international fora on IoT issues. NTIA specifically asks if there are Internet governance issues now or in the foreseeable future specific to IoT and whether there are factors that could impede the growth of IoT outside the U.S., such as data or service localization requirements or other barriers to trade.

Additional Issues. Finally, NTIA asks whether there are IoT policy issues that could be appropriate for multistakeholder engagement, similar to the NTIA-run processes on privacy and cybersecurity, and how the government and the private sector should collaborate to ensure that infrastructure, policy, technology, and investment are working together to best fuel IoT growth.

Wiley Rein attorneys are available to provide guidance about the NTIA process and to assist those interested in submitting comments or otherwise engaging the government process. For further information on these issues and related oportunities, please contact:

Scott D. Delacourt
202.719.7459
sdelacourt@wileyrein.com

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Anna M. Gomez
202.719.7261
agomez@wileyrein.com

Umair Javed
202.719.7475
ujaved@wileyrein.com

Madeleine Lottenbach*
202.719.4193
mlottenbach@wileyrein.com

*Supervised by principals of the firm

Sixth Circuit: Notice of a Data Breach Alone Is Insufficient to Support an FCA Case

In an important case for HITECH-certifying companies, the U.S. Court of Appeals for the Sixth Circuit affirmed a district court's decision to dismiss a False Claims Act (FCA) case premised on an alleged data breach. In *United States ex rel. Sheldon v. Kettering Health Network*, No. 15-3075, 2016 U.S. App. Lexis 4236 (6th Cir. Mar. 7, 2016), the relator alleged that the defendant, Kettering, violated the FCA by falsely certifying compliance with the Health Information Technology for Economic and Clinical Health (HITECH) Act to receive "meaningful use" incentive payments allegedly exceeding $75 million. Specifically, the court rejected allegations that Kettering's failure to run specific reports and notification of two potential data breaches evidenced the company's knowing non-compliance with HITECH requirements.

Health Data Protection Requirement

Under the HITECH Act, the U.S. government will pay eligible health care providers incentives for adopting electronic health record technology. However, to receive such incentives, health care providers, like Kettering, must certify compliance with a set of "meaningful-use objectives" and accompanying measures of compliance. One of the meaningful-use objectives requires providers to protect electronic health information created or maintained by the electronic health record technology adopted through implementation of appropriate technical capabilities. To that end, to obtain incentive payments, providers are required to periodically certify that they have taken certain actions, such as security risk analyses and addressing the encryption/security of data stored in electronic health

continued on page 6

Sixth Circuit: Notice of a Data Breach Alone Is Insufficient to Support an FCA Case

continued from page 4

record technology. They must also certify compliance with the security and privacy standards established under HIPAA, including regulations requiring the implementation of policies and procedures to prevent, detect, contain, and correct security failures, among other requirements.

Here, Sheldon alleged that certifications Kettering submitted to receive incentive compensation under HITECH were false because Kettering did not comply with the meaningful-use objectives. Sheldon's complaint relied on two letters she received from Kettering informing her that employees—one of whom was her former husband—improperly accessed her electronic personal health information (e-PHI), which she argued evidenced Kettering's failure to comply with HITECH. Sheldon also argued that Kettering's failure to regularly run "CLARITY" reports designed to monitor improper access to e-PHI rendered Kettering's certifications false.

Appellate Analysis

The Sixth Circuit, affirming the district court's decision to dismiss, rejected Sheldon's position, writing that her "claim that [Kettering's] individual breaches each constituted violation of the HITECH Act is an incorrect conclusion of law." Notably, because compliance under the Act is "premised on the process of analyzing and reviewing security policies and procedures; attestation of compliance is not rendered false by virtue of individual breaches."

Indeed, the court indicated that the language of the governing regulation "plainly contemplates occasional breaches of e-PHI" and agreed that the "regulations . . . do not impose a strict liability standard that requires hospitals to prevent all privacy breaches." As such, the court held that Kettering's notices to relator regarding inappropriate access to her e-PHI could not, by themselves, render "false" Kettering's certifications of HITECH compliance.

Like the district court, the Sixth Circuit also rejected Sheldon's argument with respect to the CLARITY reports, holding that there is nothing in HITECH requiring Kettering to use a particular e-PHI product or vendor to run a specific type of monitoring report.

While the Sixth Circuit did not go as far as to say that repeated data breaches could not be indicative of a provider's failure to comply with HITECH, providers should find some comfort in knowing that a circuit court has rejected the proposition that data breach notifications alone evidence non-compliance with HITECH for purposes of the FCA.

For more information, please contact:

Brandon J. Moss
202.719.7554
bmoss@wileyrein.com

No Coverage for Bank Claims Arising from Data Breach

A New York intermediate appellate court, applying New York law, has ruled that an insurance coverage claim, arising out of the theft of electronic credit card data and a subsequent suit by a bank arising out of the alleged misuse of that data, did not involve "property damage," within the meaning of a comprehensive general liability policy. *See RVST Holdings, LLC v. Main Street America Assurance Co.*, No. 521419, 2016 WL 634611 (N.Y. App. Div. Feb. 18, 2016). This decision further reinforces that there is very limited coverage for "data breach" claims outside the coverage afforded by specialized "cyber" policies.

The Present Decision

The policyholder, a fast-food company, stored its customers' credit card information on its computer network, which was infiltrated by unknown individuals. These individuals unlawfully obtained the customers' credit card information and used that information to make fraudulent charges. The claimant, a bank, filed suit against the policyholder, alleging that the policyholder had negligently failed to exercise reasonable care in safeguarding the information of the claimant's cardholders. The claimant asserted that this negligence caused it to sustain damages related to its reimbursement of the fraudulent charges. The insurer refused to defend or indemnify the policyholder for the underlying suit, and the policyholder filed a declaratory action against the insurer seeking coverage. The trial court granted summary judgment to the policyholder.

On appeal, the court held that the insurer had no duty to defend because the underlying action arose out of the policyholder's negligent handling of electronic data, which did not constitute a claim for "property damage" under the policy. The court noted that both the insurer and the policyholder agreed that the allegations in the underlying complaint were based upon losses due to the theft and subsequent misuse of electronic data. The parties also agreed that the electronically stored information at issue in the underlying action qualified as "electronic data" under the policy's definition of that term. The court explained that,

continued on page 7

while the policy covered damages arising out of damage to tangible property, the policy specifically excluded "electronic data" from the definition of "tangible property." The court also observed that the policy excluded "damages arising out of the loss of electronic data." Therefore, the court held that the underlying action's claim for damages arising out of the policyholder's negligent handling of electronic data was not a claim for "property damage" under the policy.

The Emerging Trend

Under older policy forms, some policyholders sought coverage under "Coverage A" (property damage) of CGL policies for "data breach" claims. Although the better view is that electronic data cannot constitute "tangible property" under any definition of the term, *see*, *e.g.*, *Am. Online, Inc. v. St. Paul Mercury Ins. Co*., 207 F. Supp. 2d 459, 466 (E.D. Va. 2002) ("Computer data is not tangible property."), *aff'd*, 347 F.3d 89 (4th Cir. 2003) and *State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More*, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) ("Alone, computer data cannot be touched, held or sensed by the human mind; it has no physical substance. It is not tangible property."), the case law under older policy forms was mixed. *See Computer Corner, Inc. v. Fireman's Fund Ins. Co.*, 46 P.2d 1264 (N.M. Ct. App. 2002) (finding coverage for suit for loss of data from reformatting hard drive; "computer data is tangible property"); *Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, No. CIV. 99-185 TUC ACM, 2000 WL 726789 (D. Ariz. Apr. 18, 2000) (concluding that loss of data on computer network constituted "property damage").

More recently, however, policies have expressly excluded claims involving damage to (or loss of use of) electronic data. For example, many CGL policies bar coverage for "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." *See* ISO Form No. CG 00 01 12 04 (added in 2004). The *RVST Holdings* decision illustrates that these types of limitations will be given effect.

For more information please contact:

Edward R. Brown
202.719.7580
erbrown@wileyrein.com

Laura A. Foggan
202.719.3382
lfoggan@wileyrein.com

FCC Issues NPRM on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services

On April 1, the Federal Communications Commission (FCC) released a Notice of Proposed Rulemaking (NPRM) proposing to establish a new consumer privacy framework for broadband Internet access service providers (ISPs). The proposed rules would not apply to the privacy practices of web sites, apps, and other "edge services."

Importantly, the NPRM proposes protections for types of information beyond that traditionally considered "Customer Proprietary Network Information" (CPNI). In addition to providing guidance on the information that should be considered CPNI in the broadband context (e.g., service plan and traffic information), the FCC proposes a new category of protected information, Customer Proprietary Information (CPI), including both CPNI and other personally identifiable information (PII) acquired by ISPs about their customers. The new transparency, control, and security rules proposed in the NPRM would apply to this broader category of information.

The NPRM proposes a three-tiered consent framework for ISP use and sharing of customer proprietary information.

- Consent Implied: No additional customer consent beyond creation of a customer-ISP relationship is needed for use of customer data necessary to provide broadband services, for marketing the type of broadband service purchased by a customer, and for certain other purposes consistent with customer expectations (e.g., contacting public safety).
- Opt-out: ISPs would be allowed to use (and share with affiliates) customer data to market other communications-related services unless the customer affirmatively opts out.
- Opt-in: All other uses and sharing of CPI would require express, affirmative "opt-in" consent from customers.

Among other matters, the NPRM also seeks comment on:

- Transparency requirements for ISPs, mandating notice to customers about how data is used and collected, and how privacy preferences can be changed;
- New data security mandates for ISPs, including requirements to adopt specified risk management

continued on page 8

practices, training, customer authentication, and corporate governance;

- Federal data breach notification obligation for all telecommunications carriers;
- Specific business practices, such as whether deep packet inspection, persistent tracking, and financial inducement should be prohibited or have heightened notice obligations;
- Dispute resolution mechanisms, including whether ISPs should be prohibited from compelling arbitration in customer agreements;
- Alternative proposals for BIAS privacy frameworks, which the FCC has received from industry associations and other organizations; and
- The legal authority upon which the proposed rules would be based, which is primarily Section 222 of the Communications Act, but also includes Sections 201, 202, 303(b), 303(r), 316, 705, and 706 of the Act.

Comments and Reply Comments on the NPRM will be due May 27 and June 27, 2016, respectively. (WC Docket No. 16-106 ; FCC 1b-39). For a detailed summary of the NPRM, click here.

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Scott D. Delacourt
202.719.7459
sdelacourt@wileyrein.com

Bennett L. Ross
202.719.7524
bross@wileyrein.com

Thomas J. Navin
202.719.7487
tnavin@wileyrein.com

SPEECHES & EVENTS

Privacy Bootcamp
Kirk J. Nahra, Speaker
IAPP Global Privacy Summit 2016
April 3, 2016 | Washington, DC

The Changing Face of Health Care Privacy
Kirk J. Nahra, Speaker
IAPP Global Privacy Summit 2016
April 6, 2016 | Washington, DC

Are You and Your Insurer Connecting on Cyber Risk?
Laura A. Foggan, Speaker
Northeast Corporate Counsel Forum 2016
April 21, 2016 | Atlantic City, NJ

Cybersecurity: Navigating a Terrain Fraught with Peril
Kirk J. Nahra, Speaker
International Franchise Association's 49th Annual Legal Symposium
May 16 & 17, 2016 | Washington, DC

Top New Privacy & Security Topics to Watch for in 2016
Kirk J. Nahra, Speaker
Blue Cross Blue Shield Association 2016 National Summit
May 18, 2016 | Orlando, FL

Contributing Authors

Edward R. Brown	202.719.7580	erbrown@wileyrein.com
Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Scott D. Delacourt	202.719.7459	sdelacourt@wileyrein.com
Laura A. Foggan	202.719.3382	lfoggan@wileyrein.com
Anna M. Gomez	202.719.7261	agomez@wileyrein.com
Umair Javed	202.719.7475	ujaved@wileyrein.com
Madeleine Lottenbach*	202.719.4193	mlottenbach@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Brandon J. Moss	202.719.7554	bmoss@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Thomas J. Navin	202.719.7487	tnavin@wileyrein.com
Bennett L. Ross	202.719.7524	bross@wileyrein.com

*Supervised by principals of the firm

To update your contact information or to cancel your subscription to this newsletter, visit:
http://www.wileyrein.com/newsroom-signup.html

This is a publication of Wiley Rein LLP, intended to provide general news about recent legal developments and should not be construed as providing legal advice or legal opinions. You should consult an attorney for any specific legal questions.

Some of the content in this publication may be considered attorney advertising under applicable state laws. Prior results do not guarantee a
similar outcome.