Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | January 2017

Introduction

This month's issue focuses on the year ahead in privacy and security. I identify the top ten privacy and security issues to be watching in 2017. These will be issues of key importance to many companies and to the privacy and security field in general. We'll be following all of these developments over the coming year as they evolve. Also, I look at another significant regulatory development, this time at the state level. The New York State Department of Financial Services has proposed sweeping cybersecurity requirements for the entire financial services industry, applicable not only to that industry but also to the many service providers for financial services companies. This will be both an important compliance obligation and a new business and contracting challenge for the financial services industry and their service providers. Last, Megan Brown and Kathleen Scott briefly discuss the latest National Institute of Standards and Technology (NIST) report, where NIST introduces the concepts of systems engineering and risk management into privacy in an effort to develop more trustworthy federal systems.

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. Thank you for reading. ■

— Kirk Nahra, Privacy & Cybersecurity Practice Chair

The Year Ahead for Privacy and Security

It has been an interesting and turbulent year for privacy and security, with ongoing security breaches, increased enforcement, international disarray, and a variety of new litigation threats. The year ahead may be no less challenging. Here are some of the key issues and anticipated developments to be watching in 2017.

1. The Impact of the New Administration

Everyone in Washington (and around the country and the world) is watching the incoming Administration, to try to understand, predict, and prepare for a highly uncertain policy environment. This uncertainty and nervousness is prevalent even for the "first-tier" issues of this incoming group. Those who need to deal with what the Trump Administration views as second- or third-tier issues (or issues that haven't been thought about at all) face even bigger challenges, given that there are virtually no data points to predict developments on many issues that are enormously important to a broad variety of audiences.

We have three broad philosophical elements of the new Administration that could eventually impact privacy and security. First, there is a recognition of the relatively weak state of the country's cybersecurity efforts. As with many other issues, there is criticism of the status quo without any meaningful solution yet. We expect privacy and security professionals to grapple with the impact of this "philosophy" on the key issues for this field. While it is unlikely that we will see new regulations affecting security issues (as discussed below), the issue of cyber-readiness will be one to watch frequently. Second, there is a willingness in the new Administration to engage in broad surveillance of individuals in connection with national security activities. More companies will be faced with the need to deal with data demands from the government that

continued on page 2

ALSO IN THIS ISSUE

place the company in direct conflict with its customers and/or employees. The impact of these surveillance issues may be felt most broadly in connection with international privacy regulation, where the more aggressive the United States is in connection with surveillance, the less flexible we may find the European authorities and others in connection with international data flows. Third, we will watch the impact of two other themes of the new Administration – less government regulation and expenditure of less government money. This likely means no new regulations and somewhat less enforcement, rather than broader changes and a rollback on existing privacy rights, but this is clearly an area to watch carefully.

2. The General Data Protection Regulation

Around the world, the biggest privacy and security compliance and planning issue will involve preparing for the European Union's General Data Protection Regulation (GDPR), scheduled to take effect in 2018. For many companies this will be a massive undertaking – and may impact overall business strategies, business partnerships, and a broad variety of significant activities for large and small companies alike.

The new GDPR rules require time, attention, and resources. The regulation will require implementing a broader range of controls across Europe, and will have a material impact on individual consents, the use and disclosure of health care and other sensitive information, and the collection of a broad variety of other information that increasingly is being used by more and more companies around the world. There is a new and aggressive data breach notification requirement. There are unprecedented potential levels for fines. And, because it applies to all personal data, companies interested in new products and services across the entire Internet of Things will be challenged by the need to comply with this broad regulation, including many companies for whom earlier privacy laws had little or no impact.

3. Privacy Shield

The Privacy Shield program deals with another component of the international privacy regime – the transfer of personal data from the EU to a country (the United States) which – in the EU's mind – does not have adequate safeguards for this personal data. Privacy Shield replaces the Safe Harbor program, which had survived for almost 15 years but was brought down by the new information (the Snowden revelations) about how the United States government collected and analyzed personal data. Privacy Shield strengthens the protections for this data, but there is little confidence that the Privacy Shield program is free from future legal challenge, particularly with a new Administration that does not seem bound by prior agreements and has an interest in mass data surveillance. Companies are forced to evaluate implementation of a Privacy Shield program (particularly where the other alternatives are not appealing or appropriate), even though the program easily could disappear in the future. Many of the European Union policymakers seem determined to support Privacy Shield – but lawsuits and an unpredictable U.S. government may make this position challenging or untenable.

Moreover, significant portions of the U.S. economy cannot rely on Privacy Shield as a means of bringing data to the United States (although there are other data transfer options). Privacy Shield depends on whether a company is subject to the jurisdiction of the Federal Trade Commission (FTC). Insurers – generally speaking – are not subject to the FTC and therefore cannot take advantage of Privacy Shield. The same is true for not-for-profit entities. So, even if this program stands, it is not a viable solution for a considerable number of entities. But, with more businesses becoming increasingly global – through research, multinational employment, Internet customers around the world, wellness programs, vendors around the world, and a broad variety of creative programs across country lines – these international privacy challenges cannot be ignored.

4. Government Privacy and Security Leadership

In any new Administration, there is a shuffling of leadership, both in political positions and among other senior leaders who take the opportunity to move on. This year, we will see more of these changes than in many transitions. For privacy and security, the key issue will be the senior leadership of the key privacy enforcement agencies – including the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights, the Federal Communications Commission (FCC) and others – as well as the fate of the primary "day to day" senior staff who constitute the bulk of the thought leadership and institutional memory of these offices. We also will see whether the new Administration will continue important developments implemented by the current Administration to improve privacy efforts within the government (under the leadership of Marc Groman).

continued on page 3

For HHS (which oversees the HIPAA Rules), we can expect to see a new director of the Office for Civil Rights (OCR), with a likely "interim" leader" as well. No names have surfaced in the gossipy world of the presidential transition.

As for senior staff at OCR, we have the rare situation where it will be beneficial for both individuals and the industry to maintain as much of the senior leadership of the office as possible (with a reasonable expectation that this will actually take place). The bigger issue with OCR is whether the new Administration will force or lead any different directions in enforcement or otherwise. We certainly have seen no discussion of these issues as part of the campaign or the transition. My expectation is that we will see few new rules, little or no rollback of existing rights, and a generally similar enforcement policy going forward, coupled with the budgetary wild card that could reduce enforcement simply through reduced staff.

The FCC – a new player in overall privacy and security enforcement – may see the biggest change. The FCC, over the past year, has prepared and finalized an important and challenging set of privacy rules for large portions of the telecommunications industry. While there were many significant issues for debate about these rules, they were moving forward. Now, there may be wholesale changes at the top of the agency that may result in an entire rollback of this privacy program. For the industry, this is a major issue – and will be for a broad variety of related businesses and consumers as well.

On the whole, we likely will see new leadership in most key privacy positions (although not immediately), and a resulting likelihood of somewhat less enforcement and perhaps some pushback on existing regulatory compliance obligations.

5. The Federal Trade Commission

A broader issue for the privacy community involves the future of the Federal Trade Commission and its privacy and security watchdog role. The FTC has a broad overall role in enforcement and setting policy for privacy and data security enforcement. The appointment of future FTC commissioners is very much a first- or second-tier priority for the new Administration. There is a realistic likelihood that new commissioners will have a distinctly different view on ongoing enforcement in many areas, with the realistic possibility that this will include data security. We also are much more likely to see the FTC take a lesser role in overall thought leadership on privacy and security issues generally (although many of the existing staff will remain in place and will continue to bring their strong expertise to these issues). We will need to watch whether the FTC really does change, and whether any other agency (perhaps aggressive state attorneys general?) steps into any void that is created.

6. Big Data

In the privacy world, we are seeing an intensifying debate about how best to regulate big data. This debate is blending with a parallel discussion about whether our current approach to regulation in the United States – which focuses on regulation of "sectors" like health care, financial services and telecommunications – makes sense where the historic lines of these sectors no longer fit today's world. In the health care field, for example, we are seeing the increased importance of HIPAA's gaps, due to the massive growth in health care data that is being generated, used, and disclosed by entities that are outside the HIPAA regulatory structure (think websites, mobile applications, and wearables, for example). We are seeing a blurring of HIPAA/non-HIPAA lines (think wellness programs and the interest of employers in evaluating the health of their workforce). We also are seeing the related developments of HIPAA entities bringing into their systems a broad variety of data that is not normally thought of as "health" data, but where data analytics folks at these companies are finding relevant health care connections (such as income, marital status, number of cars, shopping habits, etc.). The debate on what to do with these developments has been building – there is a growing consensus that something should be done about these concerns, but little consensus on what this reform or new regulation should look like. *See generally*, Nahra, "Moving Toward a New Health Care Privacy Paradigm," *Privacy in Focus* (November 2014).

This same debate also is growing in other sectors, as personal data is being generated (through the Internet of Things) from a broad variety of new sources of data. Coupled with new computing mechanisms and improved analytic models, big data is hitting virtually every industry (and, more importantly, affecting virtually every consumer). The Obama Administration has been promoting a significant variety of important and thoughtful white papers and other policy statements on the risks and opportunities from big data. The positions have been even-handed – big data can bring important benefits to our system and our economy, and may often be helpful to individuals – but this data is being used in new and untested

continued on page 4

ways and creates risks of discrimination and other unfair practices.

In 2017, while there will be continued significant growth in big data itself, we can expect this debate to slow down and become significantly quieter. I don't think it will go away, but there is little reason to believe that Congress or any relevant regulatory agency will be using 2017 to develop reasonable new regulations or legislative proposals on these points. As with other areas (and as discussed below), this means that there is a significant opportunity for the private sector to build out appropriate standards for this industry, and to develop best practices to fill in the current gaps in the regulatory structure, since the likelihood of a regulatory solution clearly has decreased.

7. Research and De-Identification

We also can expect to see an ongoing debate about two interrelated issues – improving research and effective de-identification of data. These topics are becoming more important (and more integrated) due to big data and the Internet of Things. There is a recognition across the government of the need to ensure that important research opportunities can be capitalized upon – leading to an ongoing rulemaking proceeding to revise the "Common Rule" that regulates most human subjects research. Now, following almost a year of reviewing comments, the fate of this rule in a new Administration is unknown. Nonetheless, there clearly will be more interest going forward in making personal data available for research purposes and to maintain important individual protections while still permitting research to move forward efficiently.

Whenever there is talk about research, we also hear the discussion about de-identification. De-identification – in theory – presents a win-win for a broad variety of public purposes, including research, public health, and overall data analytics. There remains a significant ongoing debate about whether existing de-identification practices work in today's environment (where there is a broader array of data available and better technologies available to potentially re-identify). We are seeing de-identification frameworks being developed both in specific segments of the U.S. regulatory structure (including an approach modeled on the FTC de-identification framework for the telecommunications industry), as well as various models around the globe (some of which effectively do not permit de-identification or permit it only in very limited circumstances). There is a challenge for industry in this area – to demonstrate the value in de-identified information, and to evaluate and educate the public and relevant regulators and advocates on how best to protect the data that has been effectively de-identified. There is significant value here – and some of it is being lost because of bad examples of re-identification (where relevant de-identification frameworks were not followed) or misperceptions about how this data is used. This debate will continue – but it will be important for industry and the public at large to support strong, risk-based de-identification methods and a broader understanding of how de-identified data can benefit the public at large in a variety of ways.

8. Security Breach Class Action Litigation

On a different path, class action litigation continues to be a major challenge for any company subject to a large data breach. Cases now are brought routinely when there is a large reported breach. While the plaintiffs' bar continues to face substantial challenges in proving actual injury (which is a threshold legal issue to get a case started (standing), as well as a meaningful element of causation and damages), they haven't stopped trying. And there are just enough large and small wins to keep these cases coming. We are seeing theories concerning "breach of contract" injury, where there are allegations that a portion of an insurance premium or other contract payment, for example, goes towards data security protections. We are seeing arguments about the "assumed" risks associated with sensitive information. We are seeing a new range of claims related generally to weak data security practices. In general, the cases keep coming, even without major victories. It won't take many big wins for the current wall of protection for defendants to come tumbling down.

We also may see over the next few years an enhanced role for these cases as a substitute privacy regulator – if we see a diminishment in the activity of government regulators. We may see privacy advocates being willing to step into more situations where, today, they might lobby the FTC or HHS to bring an enforcement action. If those agencies slow down in their efforts, we are likely to see policy-oriented privacy and security litigation growing as a concern across the full range of industries affected by the privacy and security debate.

9. Breach Notification Legislation

We have seen half a decade of legislative proposals from Congress about breach notification legislation – to create a consistent federal standard on top of, or instead of, at least 47 states' laws. Many of

continued on page 5

these proposals are roughly similar, and there is a consensus in Congress on many (but not all) of the key issues. And, with each major breach – Target, Sony, Anthem, Yahoo, Yahoo again – many of us think that "this one" will finally be the tipping point for actual legislation.

So, it will be critical to see if any of the latest breaches – or any new ones in 2017 – finally lead Congress to act in this area. A parallel impetus for legislation could be significant court rulings (maybe in the pending LabMD case?) where the FTC's overall authority to act in data security cases is cut back.

10. Managing Compliance with Less Enforcement

Lastly, there is a real possibility that the relevant enforcement agencies – due to budget cuts, staffing cuts, leadership changes, overall philosophy, or distraction from other activities – will significantly reduce enforcement activity. Already, in many situations, there is no realistic threat of enforcement. This may only get worse over the next few years. There also is a reduced likelihood of new legislation addressing some of the concerns that have been raised about big data and other emerging privacy issues.

Therefore, companies face a real challenge – how to maintain a focus on compliance and good business practices in light of a reduced likelihood of enforcement. We see these pressures regularly – will a company push the envelope more? Will marketing have a louder voice while compliance and legal isn't listened to? Will company leaders – facing budget and revenue pressures – be willing to cut more corners, particularly in situations where it is unlikely something bad will become visible? All in all, this will be a challenging time for privacy officials. There will be a need for forceful leadership and creative strategies to address this likely reduction of attention across companies. Part of this message needs to be that many people are watching even if it isn't tied to enforcement – the news media, consumers, customers, and class action lawyers all aren't going away. Nonetheless, privacy officials need to be cognizant of this possibility, and have a realistic plan for addressing potential changes in attitude towards privacy and security compliance.

Conclusions

We are living in interesting and uncertain times. The commercial privacy and security issues that are so important to a growing range of industries and their consumers have not been a focus of any material discussion for the new Administration. At the same time, with the expansion of the Internet of Things and improved capabilities for big data analytics, there is no doubt that data and the ability to manage and analyze data have never been more important. Businesses will not stop using data just because there is less enforcement. So, for any entity (or related service provider) looking to be competitive and responsible in the years ahead, the ability to recognize and understand these key developments will be critical. This requires thought, and time, and attention, and planning. It also requires the ability to think beyond the pressures of the day, to develop thoughtful and responsible approaches to the collection, analysis, use, and disclosure of the increasing volume of personal information and related data that is driving success across a growing range of industries. ■

For more information, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

NIST's New Privacy Report: Taking a More Scientific Approach to Privacy

On January 4, 2017, the National Institute of Standards and Technology (NIST) published An Introduction to Privacy Engineering and Risk Management in Federal Systems (Report). The Report introduces the concepts of systems engineering and risk management into privacy in an effort to develop more trustworthy federal systems. As the authors described in an accompanying blog post, the Report is one step in the process of moving privacy closer to science than art.

In taking a more scientific approach to privacy, as NIST has done in the security realm, the Report introduces a set of privacy engineering objectives to assist system engineers in implementing privacy policies and requirements. The objectives are **predictability** ("enabling reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system"); **manageability** ("providing the capability for granular administration of personal information including alteration, deletion, and selective disclosure"); and **disassociability** ("enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system"). And, the privacy risk model introduced will allow agencies to conduct more consistent privacy risk assessments.

NIST attempted to create privacy processes that are repeatable and measurable.

Finally, the Report provides a general roadmap for NIST's privacy engineering and risk management guidance moving forward. As NIST has achieved thorough security guidance such as the *Risk Management Framework*, it plans to expand privacy guidance to accomplish "privacy-positive outcomes" for federal systems.

As the title of the Report makes clear, this guidance is intended for federal agencies. However, as we have seen in the security arena, it is important for the private sector to be engaged and watchful in this process, as NIST's work is becoming increasingly influential, especially among regulators. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Kathleen E. Scott
202.719.7577
kscott@wileyrein.com

SPEECHES & EVENTS

What Companies Need to Know About Data Transfers Under the New EU Privacy Regime

Bloomberg Law Privacy Outlook 2017

Kirk J. Nahra, Panelist

February 28, 2017 | Washington, DC

Letting the Genie Out of the Bottle: Can Digitally Driven Biomedical Innovation Maintain Privacy?

ABA Health Law Section's 18th Annual Conference on Emerging Issues in Healthcare Law

Kirk J. Nahra, Panelist

March 9, 2017 | New Orleans, LA

Hot Topics in Privacy and Security

NAID 2017 Annual Conference

Kirk J. Nahra, Speaker

March 23, 2017 | Las Vegas, NV

Navigating the HIPAA Enforcement Landscape

The 26th National HIPAA Summit: The Leading Forum on Healthcare EDI, Privacy, Confidentiality, Data Security, and HIPAA Compliance

Kirk J. Nahra, Speaker

March 29-31, 2017 | Washington, DC

Privacy Boot Camp

IAPP Global Privacy Summit 2017

Kirk J. Nahra, Speaker

April 18, 2017 | Washington, DC

New York Cyber Regulations to Impose New and Significant Burdens on the Financial Services Industry

The New York State Department of Financial Services (DFS or Department) continues down its path toward a new set of cybersecurity requirements for the financial services industry. In a press release issued December 28, 2016, the Department announced an updated proposed regulation intended to become effective on March 1, 2017, that "will require banks, insurance companies, and other financial services institutions regulated by DFS to establish and maintain a cybersecurity program designed to protect consumers and ensure the safety and soundness of New York State's financial services industry." There is a new 30-day comment period on this proposal (and the department made meaningful changes to this proposed regulation based on the last set of comments). While the final version may still change modestly, this proposal will impose significant new compliance obligations on the financial services industry, with a relatively short compliance timetable.

Organizations Covered

The proposal applies to a "covered entity," which means "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law, or the Financial Services Law." This covers a very broad range of companies licensed to do business in these industries in New York. The proposal also will have a significant impact on thousands of entities that are "third party service providers" to the financial services industry.

This proposal will supplement other cybersecurity frameworks, including those applicable under the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLB). Unlike those laws, however, this proposal applies not only to the security of personal information, but also to "information systems" generally, as well as to "business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity." Accordingly, while companies that have implemented strong security programs under HIPAA or GLB may be in reasonably good shape under these regulations (although a new review and some additional elements certainly will be required), many companies that have not had to follow these other laws will face the need to develop a more systematic approach to overall cybersecurity policies and procedures.

Risk Assessment

As with many data security or cybersecurity requirements, a key element of this regulation involves a "risk assessment." There are specific required elements of this risk assessment (including the obligation for these steps to be ongoing). Specifically, under the current proposal, each regulated entity must conduct a "periodic" risk assessment of the entity's information systems "sufficient to inform the design of the cybersecurity program" as required by the regulation. The assessment must be "updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations." In general, the risk assessment "shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized, and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems."

In addition, the risk assessment must be formalized and documented. The formal assessment must include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;

(2) criteria for the assessment of the confidentiality, integrity, security, and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks.

Cybersecurity Program

The "Cybersecurity Program" required by the regulation is keyed to the company's risk assessment, which then triggers most of the remaining elements

continued on page 8

of the program. Specifically, each Covered Entity will need to develop and implement a cybersecurity program that will:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

(3) detect Cybersecurity Events;

(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;

(5) recover from Cybersecurity Events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

These requirements – particularly as to documentation of these steps – will become reality in two situations – an investigation or inquiry following an actual cyberattack, or a more generalized audit or review by the department, as "All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request."

The overall cybersecurity policy required by these provisions "shall be based on the Covered Entity's Risk Assessment" and address the following areas "to the extent applicable to the Covered Entity's operations":

(1) information security;

(2) data governance and classification;

(3) asset inventory and device management;

(4) access controls and identity management;

(5) business continuity and disaster recovery planning and resources;

(6) systems operations and availability concerns;

(7) systems and network security;

(8) systems and network monitoring;

(9) systems and application development and quality assurance;

(10) physical security and environmental controls;

(11) customer data privacy;

(12) vendor and Third Party Service Provider management;

(13) risk assessment; and

(14) incident response.

Service Provider Impacts

One of the most significant impacts from this regulation will be on the relationships between financial institutions and their service providers. The regulations impose a meaningful new contractual challenge for these providers, and will likely create real tensions, new contracting burdens, and operational challenges for vendors who will now face multiple and likely inconsistent security obligations depending on their range of financial institution customers.

Under the regulation as it now stands, each covered financial institution "shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers," again derived from the risk assessment. These policies need to address, "to the extent applicable":

(1) the identification and risk assessment of Third Party Service Providers;

(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and

(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

For covered entities, this means new obligations before contracts can be entered into, and during the relationship on an ongoing basis. For the service providers, there will be a need to renegotiate many contracts, along with a new and potentially very burdensome obligation to demonstrate to customers the strength of a cybersecurity program along with the need to operationalize the specific requirements of each regulated customer. It is clear – if the language remains the way it is – that this regulation will impose

continued on page 9

meaningful new requirements on these contracting relationships, many of which will be burdensome without necessarily advancing specific cybersecurity goals. Companies will need to plan for these obligations now.

Compliance Deadlines and Challenges

In general, companies are likely to have 180 days from March 1, 2017, to comply with most of the requirements. (There are certain defined requirements that have longer transition periods). Regulated companies and their service providers will need this time to prepare for and meet these significant new compliance obligations.

Some companies – those that have developed meaningful cybersecurity programs based on good business decision-making – may find that these new regulations do not impose substantial new requirements. As with many regulations and standards like this, even for these proactive companies, the new regulations may indicate some areas for new or increased focus. For the rest of the industry and their service providers – which, we can project, accounts for thousands of companies – these new requirements will create the obligation for meaningful change and increased rigor in cybersecurity programs, adding to both business risk and overall legal compliance obligations. ■

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
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