MAYER·BROWN

2016 Outlook

CYBERSECURITY AND DATA PRIVACY

January 2016

Cybersecurity and Data Privacy: 2016 Outlook

As the cybersecurity and data privacy landscapes continue to shift around the world, the value for businesses of understanding those threats and responding in a strategic, coordinated and enterprise-wide fashion will be greater than ever in 2016.

Cybersecurity and data privacy were top priority issues in 2015 for companies in a broad range of industries. Businesses took an array of steps to identify and mitigate the legal, reputational and business risks associated with these issues. For example, many businesses strengthened internal plans and capabilities to defend company networks and to respond to cybersecurity incidents, ensured effective oversight by their boards of directors, fine-tuned vendor agreements to account for cybersecurity and data privacy interests and worked closely with policy makers at the state and federal levels. Businesses also increasingly engaged with regulatory and enforcement agencies and, where necessary, contested high-stakes class actions.

This year is poised to see cybersecurity and data privacy continue to grow in importance for companies doing business in the United States and for US businesses operating globally. Here, we highlight five priority issues that these companies should consider as they assess, refine and operate their cybersecurity and data privacy programs in 2016:

- Increasingly global governance of cybersecurity and data privacy;
- Expanding regulatory and enforcement activity;
- Continued growth in cybersecurity and data privacy litigation;
- Substantial law enforcement activity; and
- Expanding global and technological scope of policy debates.

Increasingly Global Governance of Cybersecurity and Data Privacy

Many of the most significant cybersecurity and data privacy developments for US companies may well be seen outside the United States in 2016. Multinational businesses must navigate an expanding array of international statutes, regulations and enforcement policies. Increasingly, so, too, must businesses without any international footprint. A company's data may very well cross borders—whether to be stored at an international data center (e.g., for a private cloud) or to be processed remotely (e.g., by a payroll service)—even for otherwise-domestic businesses.

Last year saw significant upheaval in the legal regimes governing cybersecurity and data privacy across the globe, most notably with the invalidation of the US-EU safe harbor scheme.

In 2016, businesses should expect to see continued evolution in the international sphere. Three trends are likely to be particularly significant:

- **Continued Evolution of Data Transfer Regimes.** The *Schrems* decision by the Court of Justice of the European Union in October 2015 invalidated the Safe Harbor regime upon which many companies relied for their transfer of personal data from Europe to the United States. Representatives from the US Department of Commerce and the European Commission had already begun negotiating a "Safe Harbor 2.0" when the *Schrems* opinion was handed down, but the likelihood of the success of the negotiations remains unclear. Some national data protection authorities in Europe have threatened that, absent sufficient progress by January 31, 2016, they will begin bringing enforcement actions and potentially start to investigate the legitimacy of other transfer methods. Such steps could have dramatic implications for companies transferring data from the European Union to the United States.
- **Expansion of Regulatory Regimes.** Companies will face a host of new and expanding cybersecurity and data privacy regulatory regimes across the globe in 2016. Companies will be required to navigate many of these regulations for the first time, even as more rules are developed in other jurisdictions. For example:
  - *Europe*. In December 2015, the European Commission released a new General Data Protection Regulation, which is to be approved by the European Parliament in early 2016 and to take effect by early 2018. This regulation will substantially revise data protection and privacy rules for covered businesses (called "data controllers" under the regulation) and impose a new breach notification requirement. The regulation will harmonize data protection laws across the European Union and will apply to foreign entities that offer goods or services to individuals in the European Union.
  - *Indonesia*. In 2016, Indonesia will implement the first data protection law in the country's history. Companies doing business in Indonesia will be subject to its various requirements regarding data collection, usage, management and transfer.
  - *Australia*. Amendments to laws in Australia now require covered businesses to disclose any "serious data breach" to the Office of the Australian Information Commissioner and take reasonable steps to notify individuals whose data has been compromised by a breach.
- **Continued International Engagement on Cybersecurity and Data Privacy.** In 2015, there was significant international discussion and debate on cybersecurity and data privacy, including between the United States and China. For example, in September 2015, President Obama and President Xi Jinping publicly confronted the thorny issue of economic espionage by agreeing that neither country's government would conduct or knowingly support the cyber-enabled theft of confidential business information, trade secrets or other intellectual property in order to provide competitive benefits to their own industries. Then, in December, China passed a new counter-terrorism law that requires Internet service providers to disclose encryption keys to government authorities and to enhance their monitoring and reporting of Internet content. This year is likely to bring continued international developments on a broad range of contentious cybersecurity and data privacy issues. These changes may have substantial consequences for businesses, potentially altering the scale and origin of the cyber threats they face, their access to foreign markets and the scope of their responsibilities in foreign jurisdictions

Expanding Regulatory and Enforcement Activity

Like their international counterparts, regulatory and enforcement agencies in the United States continued to expand their activities addressing cybersecurity and data privacy issues in 2015. As different federal and state agencies pursued their own distinct agendas, businesses faced a growing patchwork of regulatory requirements—a trend that is set to continue in 2016. The likely common denominators of these are more expansive and detailed rules and more frequent enforcement of those rules. Consequently, companies in a wide variety of industries should expect greater scrutiny and more substantial compliance costs as yet more agencies enter the regulatory field, new rules are implemented and regulated entities are examined for compliance with these new rules. In particular, companies should expect:

- **Greater Regulatory and Enforcement Activities by the Federal Trade Commission (FTC) Across a Broad Range of Fields.** In 2015, the US Court of Appeals for the Third Circuit affirmed the FTC's ability to regulate cybersecurity practices through its "unfairness" authority under Section 5 of the FTC Act. Likewise, the FTC signaled its intent to aggressively enforce existing privacy laws and to focus on such evolving areas as big data, tracking consumers across devices and privacy notices for mobile applications. Companies should expect the FTC to pursue these topics throughout 2016, including through guidance regarding best practices, white papers, workshops and enforcement actions. For example, in June 2015, the FTC released a guide highlighting lessons learned from its 50-plus law enforcement actions concerning data security. Additionally, the FTC has made clear that it may bring enforcement actions on a wide range of theories relating to the use of big data, de-anonymization and the potential disparate effects on certain consumers arising from the use of collected data. As with other topics, other regulators at the state and federal levels are likely to collaborate with the FTC or otherwise follow its lead.
- **Continued Expansion of Cybersecurity Regulation by Financial Services Regulators.** Federal regulators of banks and other financial services companies have long been active in the oversight of cybersecurity at regulated entities. Often, their actions have set the tone for other regulated industries, as other federal and state regulators have adopted similar principles for their respective industries. This trend of financial services regulators acting aggressively on cybersecurity is on track to continue at the federal and state levels. For example, the New York State Department of Financial Services is set to embark on a major rulemaking in 2016. This regulator of New York-chartered banks and insurance companies (including non-US banks doing business in New York) is expected to propose new requirements regarding; cybersecurity policies and procedures; management of third-party service providers; multi-factor authentication; appointment of a Chief Information Security Officer; application security; audits; and notice in the event of a cybersecurity incident.
- **Amendments to State Data Breach Notification Requirements.** The patchwork of state data security and data breach notification laws continues to grow more complex in the continuing absence of federal standards. Companies should expect this trend to continue in 2016. For example, the California legislature revised its data breach laws effective January 1, 2016, to expand and clarify the existing notice requirements and to specify forms for notices. Entities around the country will need to consider California's new requirements, as well as any potential incompatibility with other states' notice requirements. (And companies will need to remain cognizant of

their obligations under relevant state data security regulations, such as by implementation of a written information security program to satisfy Massachusetts law, where applicable.)

- **Increased Regulation and Examination of Cybersecurity in the Securities and Commodities Markets.** Regulatory agencies with supervisory authority over broker-dealers, investment advisers and financial market utilities have made it clear that cybersecurity will be an increasing focus of supervisory exams. In 2014 and 2015, for example, the Financial Industry Regulatory Authority (FINRA) and the Securities and Exchange Commission (SEC) reviewed the cybersecurity practices of a sample of broker-dealers and investment advisers and determined that there was a need to incorporate cybersecurity preparedness assessments in regulatory examinations. Similarly, in 2015, the Commodity Futures Trading Commission (CFTC) held a roundtable with industry experts to identify cyber threats to its regulated financial market utilities, and the National Futures Association (NFA) adopted requirements and guidance related to "Information Systems Security Programs." Entities in these industries should expect this focus to be reflected in regulatory guidance issued and examinations performed in 2016.
- **Federal Communications Commission (FCC) Rulemaking To Develop Privacy Rules for Internet Service Providers.** The FCC's reclassification of Internet service as a telecommunications service last year opened the door to new privacy regulations for providers of broadband Internet service. FCC Chairman Tom Wheeler has stated that this rulemaking could begin in early 2016. These new rules could address data breach notification, customer consent to share data, data protection and other significant issues for Internet service providers.

Continued Growth in Cybersecurity and Data Privacy Litigation

There were important developments in cybersecurity and data privacy class action litigation in 2015. Significant decisions, such as the US Court of Appeals for the Seventh Circuit's decision arising from the Neiman Marcus breach, were issued by courts of appeals. In addition, the US Supreme Court heard argument in *Spokeo v. Robins*, which considers whether the violation of a right that triggers statutory damages can substitute for injury-in-fact for purposes of Article III standing.

The pace of data breach litigation continued to increase in 2015. Plaintiffs filed nearly 250 class actions respecting some 35 different data breaches last year. This year, litigation continues to be likely in the aftermath of large-scale data breaches and, increasingly, more smaller-scale data breaches as well. Indeed, 2016 is poised to continue trends seen in 2015, including: significant disputes over whether consumer plaintiffs have alleged cognizable injury for Article III standing—and thus may proceed past the pleading stage; litigation over indemnification for expenses sustained by third parties as a result of a data breach (e.g., disputes regarding insurance coverage under cybersecurity policies); and the pursuit of data breach-related derivative lawsuits in a limited number of cases.

In addition, 2016 is almost certain to see courts more frequently decide issues that are relatively novel in the data breach context. These include:

- **Class Certification.** Data breach plaintiffs routinely employ tactics from the outset of litigation in an attempt to overcome the predominance requirement for class certification. For instance, to avoid the issue of having to prove damages on an individual basis, they have attempted to assert claims for injunctive relief under state consumer fraud statutes—which allow for recovery of attorneys' fees—to require that companies

implement specific data security safeguards. What is more, in non-data breach class actions, a number of courts have been willing to certify class actions to resolve common issues, even where individual issues of injury and the amount of damages exist and would have to be addressed in a more individualized proceeding after the common issues are resolved. In spite of such maneuvering, class certification is likely to remain a major hurdle for data breach class action plaintiffs in 2016 (despite some notable exceptions in 2015). However, the risk that companies will have to defend data breach litigation on the merits against a certified class is growing, making it increasingly important—from a litigation perspective—for businesses to take reasonable cybersecurity measures prior to a data breach.

- **Discovery.** In 2016, it is likely that we will see more decisions on the scope of discovery in the data breach context. In 2015, for example, a federal magistrate judge found that certain documents created by a task force established by in-house and outside counsel to educate the attorneys about a breach and to enable them to provide legal advice to the affected company were privileged. A key issue in this decision was whether the documents at issue were created for a legal or business purpose.
- **Summary Judgment.** This year may provide significant developments with respect to summary judgment in data breach litigation. Three noteworthy issues to be considered at this stage are: (i) the proper standard of care (i.e., what security safeguards was the affected company required to implement); (ii) what types of injuries are legally compensable (e.g., whether time spent to respond to a data breach or fees paid for data breach protection are recoverable); and (iii) causation and actual injury (i.e., whether plaintiffs can prove that the data breach caused those injuries).

While data breach cases continue to proliferate and to dominate headlines, recent studies have reported a significantly greater number of data privacy lawsuits in the last few years. Data privacy lawsuits have pursued complaints under statutes ranging from the Telephone Consumer Protection Act (TCPA) to the Fair Credit Reporting Act (FCRA). This trend is also likely to continue in 2016, as plaintiffs try to fit new technologies and new uses under existing laws. The increasing connectivity of devices and their use throughout consumers' day-to-day lives appears certain to produce a steady stream of aggressive legal claims.

Substantial Law Enforcement Activity

Highly publicized cyber intrusions in 2015 underscored the increasing productivity, sophistication and diversification of cyber threat actors' schemes. Such schemes targeted intellectual property, proprietary pricing data and medical information, among other types of sensitive information. They also damaged companies' systems, imposed significant financial and reputational costs and even threatened national security interests. Law enforcement agencies continue to evolve to address these threats to the private sector, and businesses should expect 2016 to see substantial law enforcement activity, further raising the importance of developing productive relationships with relevant authorities before a crisis arises.

- **Prosecuting Cybercriminals.** The number of cybercrime investigations and prosecutions is expected to increase in 2016 and continue the long-term trend of growing collaboration among domestic and foreign agencies to target threat actors around the world. For example, the US Department of Justice plans to disrupt and dismantle 1,000 cyber threat actors and to resolve 90 percent of national security and criminal cyber cases during the next fiscal year. These ambitious targets reflect the vast augmentation of resources that

the government has brought to bear against the cyber threat. Since 2002, the FBI's number of cyber intrusion investigations has grown by more than 80 percent. And, since 2010, the US Secret Service's cybercrime investigations have resulted in more than 5,000 arrests associated with more than $12 billion in actual and potential fraud losses.

- **International Engagement.** To continue at this pace and reach or exceed their targets, federal law enforcement agencies will need to cooperate extensively with their domestic and international counterparts. For example, in 2015, a prosecution for an alleged hacking and insider trading scheme was the result of collaboration among a who's who of law enforcement agencies: the US Department of Justice, SEC, US Department of Homeland Security, US Secret Service, FBI, FINRA, UK Financial Conduct Authority and the Danish Financial Supervisory Authority. Similarly, the arrest, extradition and prosecution of Vladimir Drinkman for a data breach conspiracy involving over 160 million compromised credit card numbers resulted from coordination among law enforcement agencies in multiple countries. International cooperation of this sort will continue to define many of the most high-profile cybercrime investigations.
- **Partnership with the Private Sector.** For years, law enforcement agencies have viewed partnerships with private entities as critical to promoting cybersecurity. According to a 2010 White House report, "[p]rivate-sector engagement is required to help address the limitations of law enforcement and national security." As is discussed in greater detail below, the Cybersecurity Information Sharing Act is expected to augment both the government and the private sector's access to information about cyber threats and to bring new private-sector players into the conversation. Overall, law enforcement agencies expect that this broader private sector participation will help them to investigate threat actors and disrupt their attacks and schemes.

Expanding Global and Technological Scope of Policy Debates

Policy debates shifted in 2015 as cybersecurity and data privacy issues attracted both national and global prominence. Policy developments in 2016 likely will continue this trend. For example, it is expected that: (i) industry will take advantage of significant legal authorities approved in 2015, such as the Cybersecurity Information Sharing Act and new "cyber sanctions," both of which will require effective collaboration between the private sector and government; (ii) long-standing debates about privacy and security will be moved to the global stage (and likely become more political as the US presidential election approaches); and (iii) the proliferation of toys, devices and machines that are connected to the Internet will present new cybersecurity and data privacy challenges.

- **Cybersecurity Information Sharing Act of 2015.** In December 2015, the multiyear debate over the appropriate mechanisms and legal protections for cybersecurity information sharing came to a close with passage of the Cybersecurity Information Sharing Act. This legislation provides new authorities for private sector businesses to monitor and defend their networks and share cyber threat information with the federal government and other private sector entities. With the ground rules for information sharing between and among the private sector and government now set, 2016 presents opportunities for businesses to take advantage of the authorities and liability protections this law offers.
- **Cyber Sanctions.** The US government is poised to use economic sanctions in 2016 as a new tool to deter foreign hackers from stealing vital assets from businesses—whether source code or confidential negotiating

positions. Last year, President Obama issued Executive Order 13694, which created a new sanctions program aimed at actors outside of the United States who threaten US national security or target the country's critical infrastructure, computer networks, intellectual property, economic resources or other vital assets. An initial set of regulations was published in the *Federal Register* on December 31, 2015, and it could only be a matter of time before the first entities are added to the sanctions list.

- **Encryption.** As countries increasingly ask technology companies for law enforcement access to communications, the question of encryption has become a global issue. Last year saw the rise of the public debate over encryption, and 2016 is likely to see it play out on a global stage. This significant policy debate may well become even more polarized during the year of a presidential election in the United States, posing potential hindrances to passing legislation or reaching international consensus.
- **Internet of Things.** There was a significant increase in policy debates in 2015 concerning cybersecurity and data privacy issues raised by the Internet of Things. From consumer products to industrial machinery, the cybersecurity and data privacy implications of the Internet of Things were scrutinized by Congress and executive branch policymakers. Automotive cybersecurity and data privacy issues, for example, were the focus of multiple pieces of proposed legislation and of regulatory study. Likewise, the Food and Drug Administration recently issued guidance on post-market management of cybersecurity in medical devices. This year will likely see continued growth in policymakers' attention to the Internet of Things as the number, kind and capability of connected devices continues to grow.

Cybersecurity and data privacy present novel, complex and global issues across the legal, policy and regulatory spectrum. These developments pose challenges that demand a proactive, risk-based response. Businesses must address these risks in a holistic fashion that reflects the strategic interests of their organizations and is effectively coordinated across their enterprises. From board oversight to the drafting of an outsourcing contract, from policy development to breach response, and from regulatory rulemaking to litigation, businesses should understand the risks they face and deliver a considered and multifaceted response. As the cybersecurity and data privacy landscapes continue to shift around the world, the value for businesses of understanding those threats and responding in a strategic, coordinated and enterprise-wide fashion will be greater than ever in 2016.

For more information about the topics raised in this 2016 Outlook, please contact any of the following Cybersecurity & Data Privacy practice team lawyers.

Matthew Bisanz
+ 1 202 263 3434
mbisanz@mayerbrown.com

Kendall C. Burman
+1 202 263 3210
kburman@mayerbrown.com

Marcus A. Christian
+1 202 263 3731
mchristian@mayerbrown.com

Rajesh De
+1 202 263 3366
rde@mayerbrown.com

Laura R. Hammargren
+1 312 701 8146
lhammargren@mayerbrown.com

Charles E. Harris
+1 312 701 8934
charris@mayerbrown.com

Gabriela Kennedy
+852 2843 2380
gabriela.kennedy@mayerbrownjsm.com

Robert J. Kriss
+ 1 312 701 7165
rkriss@mayerbrown.com

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

Mark A. Prinsley
+44 20 3130 3900
mprinsley@mayerbrown.com

Joshua M. Silverstein
+1 202 263 3208
jsilverstein@mayerbrown.com

Jeffrey P. Taft
+ 1 202 263 3293
jtaft@mayerbrown.com

Howard W. Waltzman
+1 202 263 3848
hwaltzman@mayerbrown.com

Evan M. Wooten
+1 213 621 9450
ewooten@mayerbrown.com

Oliver Yaros
+44 20 3130 3698
oyaros@mayerbrown.com

Guido Zeppenfeld
+49 211 86224 169
gzeppenfeld@mayerbrown.com

Mayer Brown is a global legal services organization advising many of the world's largest companies, including a significant portion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world's largest banks. Our legal services include banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; US Supreme Court and appellate matters; employment and benefits; environmental; financial services regulatory & enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

Please visit our web site for comprehensive contact information for all Mayer Brown offices. www.mayerbrown.com

Any advice expressed herein as to tax matters was neither written nor intended by Mayer Brown LLP to be used and cannot be used by any taxpayer for the purpose of avoiding tax penalties that may be imposed under US tax law. If any person uses or refers to any such tax advice in promoting, marketing or recommending a partnership or other entity, investment plan or arrangement to any taxpayer, then (i) the advice was written to support the promotion or marketing (by a person other than Mayer Brown LLP) of that transaction or matter, and (ii) such taxpayer should seek advice based on the taxpayer's particular circumstances from an independent tax advisor.

Mayer Brown comprises legal practices that are separate entities (the "Mayer Brown Practices"). The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe-Brussels LLP, both limited liability partnerships established in Illinois USA; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales (authorized and regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown, a SELAS established in France; Mayer Brown Mexico, S.C., a sociedad civil formed under the laws of the State of Durango, Mexico; Mayer Brown JSM, a Hong Kong partnership and its associated legal practices in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. Mayer Brown Consulting (Singapore) Pte. Ltd and its subsidiary, which are affiliated with Mayer Brown, provide customs and trade advisory and consultancy services, not legal services. "Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.

"Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.

This publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

© 2016 The Mayer Brown Practices. All rights reserved.