MAYER·BROWN

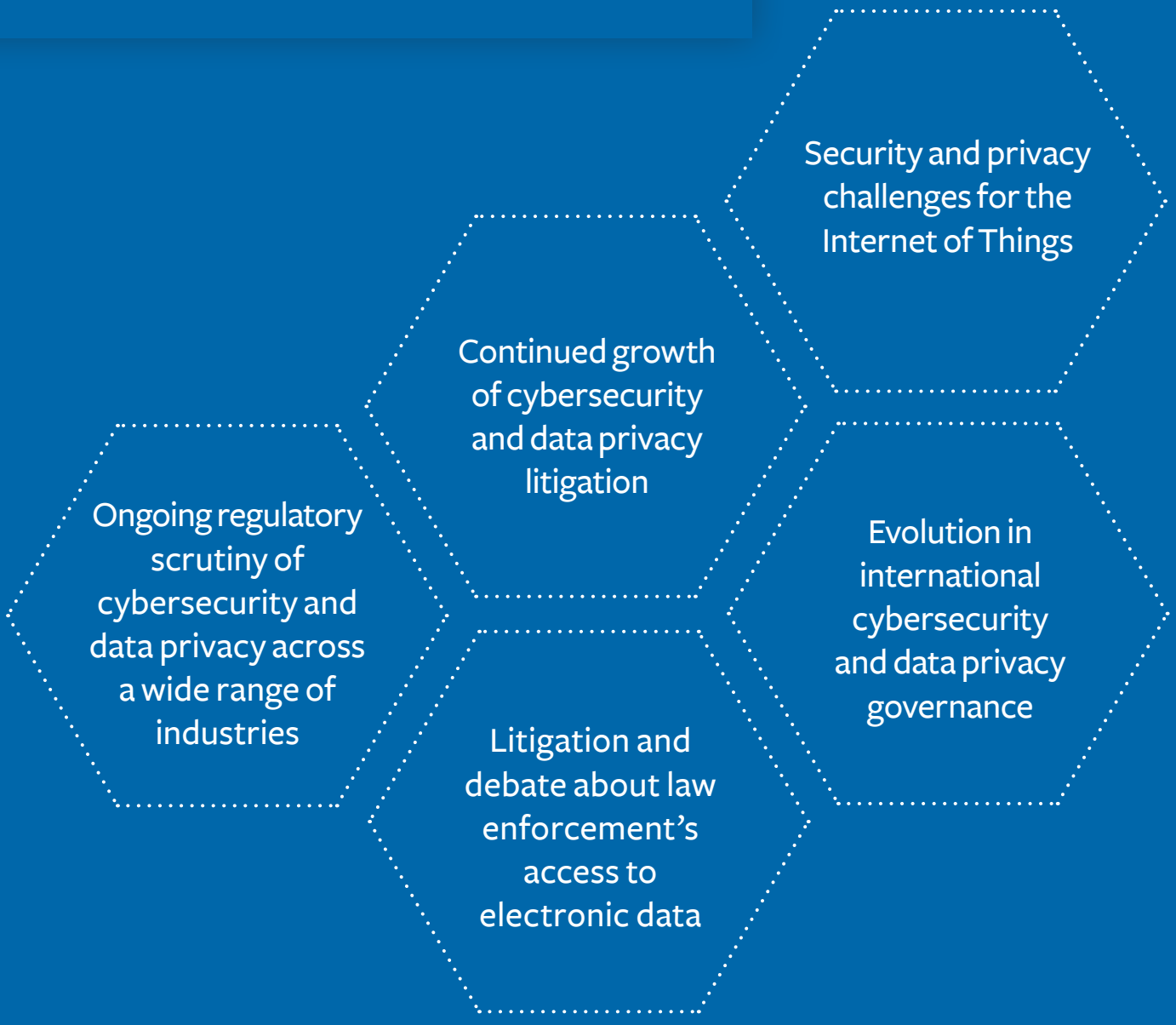
# 2017 Outlook

## Cybersecurity and Data Privacy

January 2017

# KEY ISSUES

Companies should consider these issues as they continue to refine their cybersecurity and data privacy programs in 2017.



## Cybersecurity and data privacy issues continued to grow in significance for multinational businesses over the past 12 months, further heightening the importance of preparing and responding in a strategic, coordinated and enterprise-wide manner in 2017.

The Trump administration has publicly provided limited details so far about its plans for cybersecurity and data privacy policy. Reports suggest that the administration intends to pursue a thorough review of the federal government's cybersecurity policy, although no concrete steps have been taken as of the date of this publication. But even if priorities change at the federal level, the scrutiny of cybersecurity and data privacy issues that companies face from litigants, regulators, Congress, contractual counterparties and others is poised to remain high. Moreover, cyber threats and other data privacy challenges are growing, including as increasing numbers of connected devices join the Internet of Things. Effective responses will continue to depend upon clear-eyed assessments of risks and broad engagement across the enterprise to mitigate them.

Key issues for companies doing business in the United States and for US businesses operating globally, as they continue to refine their cybersecurity and data privacy programs in 2017, will include:

- Ongoing regulatory scrutiny of cybersecurity and data privacy across a wide range of industries
- Continued growth of cybersecurity and data privacy litigation
- Security and privacy challenges for the Internet of Things
- Litigation and debate about law enforcement's access to electronic data
- Evolution in international cybersecurity and data privacy governance

# Ongoing Regulatory Scrutiny of Cybersecurity and Data Privacy Across a Wide Range of Industries

The federal government has continued to use a wide range of policy tools to influence cybersecurity and data privacy practices in the private sector. For example, after extended engagement with stakeholders, the National Institute of Standards and Technology (NIST) released version 1.1 of its Cybersecurity Framework for comment in January 2017. Moreover, the Obama administration took significant steps to enhance public-private coordination. It worked to implement the Cybersecurity Information Sharing Act in a way that maximizes information sharing while meeting privacy obligations and clarified the federal approach to responding to cybersecurity incidents in the private sector.

But the federal government did not limit itself to such collaborative public-private efforts. Regulatory and enforcement agencies in the United States also continued to use their authorities to address cybersecurity and data privacy concerns in 2016. Going forward, companies will need to pay careful attention to relevant regulatory requirements, guidance and enforcement actions to meet agencies' expectations in the Trump administration.

In addition to the Internet of Things, which we address in a subsequent section, key issues include:

Going forward, companies will need to pay careful attention to relevant regulatory requirements, guidance and enforcement actions to meet agencies' expectations in the Trump administration.

**Consumer Privacy and Data Security:** Regulators at the federal and state levels have continued to focus on consumer privacy and data security issues. For example, the Federal Communications Commission (FCC) pursued rulemaking in the field, active enforcement of the Health Insurance Portability and Accountability Act (HIPAA) has continued, the Consumer Financial Protection Bureau (CFPB) reached its first consent order for alleged misrepresentations about the security of a payment network provider, and a group of 15 state attorneys general settled their enforcement actions relating to the 2013 Adobe data breach. In particular, the Federal Trade Commission (FTC) has played a leading role through both its enforcement actions and education initiatives. For example, it published a blog post in which it explained its view that the approach reflected in its data security enforcement actions is "fully consistent" with that of the NIST Framework. The FTC also has solicited comment on whether further amendments to the Safeguards Rule, issued under the Gramm-Leach-Bliley Act, would be appropriate. And the FTC has indicated its interest in consumer privacy and security issues related to connected cars and the Internet of Things more broadly. Finally, the FTC commissioners unanimously overruled the decision of an FTC administrative law judge who had dismissed the long-running data security action against LabMD, an action that now is on appeal to the Eleventh Circuit. While these examples reflect the intensity of the FTC's focus on privacy and security in recent years, the agency's approach may evolve in the new administration. In January 2017,

President Trump designated FTC Commissioner Maureen Ohlhausen as Acting Chairman of the FTC. Acting Chairman Ohlhausen has previously emphasized the importance of "regulatory humility" and not imposing "unnecessary and disproportionate costs on businesses." The extent to which such concerns will guide the FTC going forward remains to be seen.

**Cross-Cutting Issues:** Regulatory scrutiny of cybersecurity and data privacy challenges has varied by industry and by regulator. Nonetheless, a common set of issues frequently have been–and are likely to continue to be–top priorities for regulators.

- **Cybersecurity:** Regulators continue to scrutinize whether companies have adopted and continue to refine appropriate cyber risk management programs. In particular, regulators have assessed: (i) whether a company's program includes appropriate *policies and procedures that are tailored* to reflect its assessed risks; (ii) whether the company has evaluated the risks posed by *vendors and other third parties* and incorporates such considerations into its contracting process and risk management program more broadly; and (iii) whether *senior management and board oversight* of the cybersecurity program is adequate.
- **Data Privacy:** As technology has advanced to permit greater capacity to use and store data, regulators across industries are grappling with and prioritizing data privacy issues. Issues that appear frequently across industries include: the adequacy of customer consent for data collections; management of global data flows; how to open up more data for research as well as ensure effective data anonymization; and managing privacy considerations in the context of big data–including new categories of data such as biometrics (facial recognition technology and fingerprints, for example) and images collected through the use of drones.

**Continued Regulatory Scrutiny in the Financial Services Industry:** The financial sector continued to see particular regulatory scrutiny on cybersecurity programs in 2016, as well as, to a lesser extent, on data privacy practices. Key developments included:

- **New York Regulation:** In September, the New York State Department of Financial Services proposed cybersecurity rules for banks, insurance companies and other financial services businesses licensed in New York. The proposal would require the designation of a Chief Information Security Officer, the oversight of third-party service providers, multi-factor authentication, encryption and annual certifications. The agency released a revised proposal in December 2016 that made changes regarding multi-factor authentication, encryption notice in the event of a cybersecurity incident and the scope of exemptions. It indicated that the proposal will be finalized and become effective in March 2017 with certain parts implemented over longer transitional periods.
- **Enhanced Cyber Risk Management Standards:** The federal banking regulators issued an advanced notice of proposed rulemaking for certain large financial institutions related to enhanced cyber risk management standards. Focused both on risks to individual institutions and to the sector more broadly, the contemplated standards address topics including: (i) cyber risk governance; (ii) cyber risk management; (iii) internal dependency management; (iv) external dependency management; and (v) incident response, cyber resilience and situational awareness. The comment period was recently extended to close in February 2017.

Regulatory scrutiny of cybersecurity and data privacy challenges has varied by industry and by regulator. Nonetheless, a common set of issues frequently have been–and are likely to continue to be–top priorities for regulators.

As technology has advanced to permit greater capacity to use and store data, regulators across industries are grappling with and prioritizing data privacy issues.

The trend of federal action on cybersecurity requirements for government contractors continued in 2016.

- **Enforcement Actions:** Financial regulators continued to bring cybersecurity and data privacy enforcement actions. For example, the Securities and Exchange Commission settled an enforcement action against a broker-dealer/investment adviser for: (i) failing to properly implement database user access controls; (ii) failing to implement Internet filtering or monitoring to detect data exfiltration; and (iii) allowing a compromise of a third-party server that contained stolen customer information. A wide range of other financial regulators also have taken action, from the CFPB to the Financial Industry Regulatory Authority (FINRA).

**Federal Procurement:** The trend of federal action on cybersecurity requirements for government contractors continued in 2016. For example, in June 2016, the General Services Administration, the Defense Department and NASA implemented a final rule establishing cybersecurity requirements that apply to all contractor information systems that hold government information. The rule added a new Federal Acquisition Regulation (FAR) subpart and a new contract clause to be included with new government contracts. The rule sets out fifteen "basic safeguarding . . . security controls" that contractors must employ to "protect covered contractor information systems." Among other things, the controls described in the new FAR clause include limiting system access to authorized users; verifying, controlling and limiting connections to external systems; sanitizing/destroying information system media before disposal; and updating malicious code protection mechanisms. Given the wide range of entities involved in federal contracting, these requirements are likely to influence contracting standards even outside of federal procurement.

# Continued Growth of Cybersecurity and Data Privacy Litigation

The past year saw important developments in cybersecurity and data privacy litigation. Key decisions, headlined by the US Supreme Court's decision in *Spokeo, Inc. v. Robins*, continued to address the adequacy of Article III standing of plaintiffs in data privacy and cybersecurity litigation. Moreover, disputes over the sufficiency of individual claims and, increasingly, the possibility of class certification were litigated. Each issue is likely to feature prominently in 2017, including increasingly in litigation related to the Internet of Things.

***Spokeo Inc. v. Robins:*** Under Article III of the Constitution, a plaintiff must allege that she has suffered an "injury-in-fact" to establish standing to sue in federal court. In 2016, the Supreme Court confirmed in *Spokeo* that "Article III standing requires a concrete injury even in the context of a statutory violation." (Mayer Brown has represented Spokeo throughout this litigation.) The impact of the Court's ruling has been significant, particularly in privacy and data security litigation. There are already more than 400 federal decisions citing *Spokeo*, including approximately 200 involving important privacy statutes such as the Fair Credit Reporting Act and the Video Privacy Protection Act. The significance of *Spokeo* will only grow

in 2017, as litigants and courts continue to apply its lesson that a plaintiff must allege real harm, and "cannot satisfy the demands of Article III by alleging a bare procedural violation."

**Circuit Court Data Breach Decisions:** In 2016, the central issue in data breach cases was what types of alleged injuries qualified as injuries-in-fact under Article III. In April, in *Lewert v. P.F. Chang's China Bistro, Inc.*, the Seventh Circuit found that an intentional data breach created a substantial risk of future injury. The Seventh Circuit observed that "it is plausible to infer" that the hackers intended to use the stolen data eventually, and concluded that time, effort and money spent to mitigate those risks were sufficient injuries to establish standing. In September, in *Galaria v. Nationwide Mutual Insurance Co.*, a divided Sixth Circuit panel held that risks posed by a targeted attack on consumer information, "coupled with" reasonable mitigation costs, constituted injury-in-fact. *Galaria* was not selected for publication—meaning it does not bind other panels—and the strong dissent questioned whether a defendant should be held responsible for a hacker's criminal acts. The majority in *Galaria* described its analysis as consistent with *Lewert*, but acknowledged that the Third Circuit reached a different result in *Reilly v. Ceridian Corp*. Whether a broader circuit split indeed exists on these points and others may well be clarified in 2017.

There are already more than 400 federal decisions citing *Spokeo*, including approximately 200 involving important privacy statutes such as the Fair Credit Reporting Act and the Video Privacy Protection Act.

**Adequacy of Claims and Class Certification:** The adequacy of the claims in data privacy and cybersecurity actions, and their susceptibility to class treatment, also continue to be important issues in litigation. In October 2016, for example, an Illinois federal district court dismissed a data breach action, holding that, while the alleged injuries satisfied standing, the plaintiffs failed to state any claim. For most of the claims, this was because none of the plaintiffs alleged that they had suffered any cognizable damages under case law governing the respective claims. *In re Barnes & Noble Pin Pad Litigation* (N.D. Ill.). The plaintiffs alleged that they suffered injuries in the form of time lost mitigating the increased risk of identity theft and the loss of value of their personal information, but not the requisite actual damages. Even when such damage allegations survive dismissal, plaintiffs may be creating problems for themselves at the class certification stage. In attempting to allege injury, plaintiffs very likely will raise individualized issues concerning damages that should preclude class certification. In the coming year, courts will continue to address the sufficiency of allegations in cybersecurity and data privacy cases, and increasingly are likely to consider class certification in such cases.

In the coming year, courts will continue to address the sufficiency of allegations in cybersecurity and data privacy cases, and increasingly are likely to consider class certification in such cases.

**Connected Device Lawsuits and the Internet of Things:** Lawsuits surrounding the Internet of Things continue to percolate. In recent years, plaintiffs have filed suit after breaches of home security systems and attacks on connected medical devices, toys and automobiles. Some of these cases have been dismissed, in whole or in part, for lack of standing, and others are continuing into 2017. For example, a motion to dismiss claims stemming from the breach of certain web-based learning toys is currently pending in the *In re VTech* litigation.

# Security and Privacy Challenges in the Internet of Things

The rapid growth of the use of connected devices across the economy—generally referred to as the Internet of Things or IoT—has created new cybersecurity and data privacy risks. Recent attacks and research have demonstrated that these risks can be significant: attacks on connected devices can lead to illegal tracking or surreptitious recording, the theft of personal data, ransomware attacks or even threats to individual safety. Moreover, the distributed denial of service attacks leveraging the Mirai botnet in late 2016 made clear that criminals and other hostile actors will use connected devices to attack other systems.

As noted above, a number of pieces of litigation related to connected devices already have been filed. Managing such litigation risk will be an important goal for companies that design, sell or employ such technologies. In addition, other important considerations for companies going forward include:

**Understanding New Challenges:** The IoT presents a series of challenges that generally distinguish it from the enterprise environment. For example: (i) the vast number of connected devices presents a correspondingly large attack surface; (ii) IoT devices are able to capture new forms of data and employ new ways of aggregating and using that data; (iii) IoT devices present new challenges in terms of how to effectively communicate with end-users in a variety of sectors; (iv) manufacturers may find that IoT devices are inaccessible after they have been sold or otherwise put into operation, making it more challenging to deliver security updates and patch the device; and (v) the limited computing power of some devices may make it difficult to employ certain security measures. Understanding these distinctive challenges can help mitigate associated risk.

The distributed denial of service attacks leveraging the Mirai botnet in late 2016 made clear that criminals and other hostile actors will use connected devices to attack other systems.

**Non-Regulatory Guidance:** The federal government response to the development of the IoT has included important non-regulatory elements. For example, the Department of Homeland Security released version 1.0 of "Strategic Principles for Securing the Internet of Things," which provides "a set of non-binding principles and suggested best practices to build toward a responsible level of security for the devices and systems businesses design, manufacture, own, and operate." NIST also recently released Special Pub. 800-160, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," which provides engineering recommendations for securing connected systems. In addition, the National Telecommunications and Information Administration has been leading a multi-stakeholder process in support of the Department of Commerce's ongoing efforts to identify key issues affecting deployment of these technologies, and recently released a "green paper" on "Fostering the Advancement of the Internet of Things."

**Regulatory Scrutiny:** Regulatory agencies also have brought their authorities to bear on the IoT, including through the issuance of policy guidance for entities subject to their jurisdiction. For example, in 2016 the National Highway Traffic Safety Administration

(NHTSA) released two non-binding guidance documents, one on autonomous vehicles and the other on the cybersecurity of modern vehicles. The autonomous vehicles guidance included cybersecurity and data privacy as priority issues on which NHTSA sought pre-market engagement with manufacturer and developers, and the best practices document identified key components for manufacturers' cybersecurity programs. Likewise, the Food and Drug Administration recently released final guidance on "Postmarket Management of Cybersecurity in Medical Devices," adding to its 2014 final guidance on "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."

# Litigation and Debate About Law Enforcement's Seizure of Electronic Data

As more customer records and other sensitive data are held in the cloud, and as consumer expectations of privacy evolve, businesses have an important stake in law enforcement access to such data. Recent developments in this area, described further below, include litigation about the use of a search warrant to seize data located in another country, litigation seeking to compel a company to bypass the encryption on its device, and the expansion of search warrant authority under Rule 41 of the Federal Rules of Criminal Procedure. Businesses should expect to see more litigation and debate about law enforcement agencies' access to electronic data in 2017.

**Microsoft/Ireland Warrant Case:** In July 2016, the Second Circuit quashed a search warrant that required Microsoft to produce the content of a customer's emails stored on a server located in Ireland. The court held that execution of the warrant would be an "unlawful extraterritorial application" of the Stored Communications Act (SCA), which the court noted was passed in 1986 when "Congress had as reference a technological context very different from today's Internet-saturated reality." This context, along with the SCA's structure and language, indicated to the Second Circuit that there was no Congressional intent to apply the SCA to data located outside the United States. However, this issue is far from resolved. The Department of Justice (DOJ) has proposed legislation that would allow US investigators to seek data located overseas (and vice versa), provided the US government has entered into a reciprocal agreement with the country where the data is located and the agreement meets certain statutory requirements. Additionally, on January 9, 2017, members of the House of Representatives reintroduced the Email Privacy Act, which would amend the Electronic Communications Privacy Act to require law enforcement agencies to use a warrant in order to access emails or other electronic documents stored in the cloud. This bill is similar to a bill that was unanimously approved by the House in 2016, but which did not pass the Senate.

**DOJ/Apple iPhone Encryption Litigation:** In February 2016, a magistrate judge in the Eastern District of New York denied DOJ's request for an order requiring Apple to "bypass the passcode security on an Apple device." The case arose from an iPhone 5 that federal agents

Regulatory agencies also have brought their authorities to bear on the IoT, including through the issuance of policy guidance for entities subject to their jurisdiction.

More litigation on the encryption front appears likely, particularly as encryption technology becomes more advanced.

had seized pursuant to a lawful search warrant at a residence. The court found that the government's application failed to satisfy the statutory requirements for such an order. It also discussed several discretionary factors, including the request's imposition of an unreasonable burden on Apple. The court looked to: the number of other DOJ requests for Apple's assistance; the assistance sought by the government was not something Apple would do in the ordinary course of business; Apple had never voluntarily offered the government the type of assistance requested; and providing the requested assistance would divert resources from Apple's normal business operations. Ultimately, the New York litigation became moot when the government gained access to the device by other means. This was only one of multiple requests Apple has received to unlock its encryption, including one involving an iPhone used by the shooter responsible for the San Bernadino attack in December 2015. That contentious and high-profile case ended when the government was able to access the phone's stored data with the assistance of a third party. More litigation on the encryption front appears likely, particularly as encryption technology becomes more advanced.

**Revisions to Fed. R. Crim. P. 41:** On December 1, 2016, amendments to Rule 41 went into effect. In part, Rule 41 details the geographic limits of search warrants and generally prohibits a judge from approving a warrant when the target of the search is located outside of his or her district. The amendments allow a judge to approve out-of-district remote access computer search warrants in two circumstances: (i) when a suspect has hidden his or her online location and identity using technical means; and (ii) when the crime involves the hacking of computers in five or more judicial districts. Although the DOJ's stated position is that these are "narrow circumstances" that do not authorize any search that is not already lawfully permitted, critics of the amendments argue that they remove geographic limits for remote electronic searches, including in places where US law enforcement generally lacks the ability to obtain and execute a search warrant, such as outside the United States.

# Evolution in International Cybersecurity and Data Privacy Governance

Cybersecurity and data privacy have been topics of focus around the world, and several significant recent developments in this realm will affect multinational businesses in 2017. Among these developments are: major changes in the European Union, including the forthcoming General Data Protection Regulation and Brexit; evolving restrictions on international data transfers; and new data localization laws in China and Russia.

**General Data Protection Regulation:** In 2016, the European Parliament approved the new General Data Protection Regulation (GDPR), which will come into force on May 25, 2018. The GDPR is intended to update and make data protection law more consistent across the

European Union member states. The GDPR will apply to data controllers and processors across all sectors, and even organizations established outside the European Union will have to comply if they are offering goods or services or monitoring individuals inside the European Union. Non-EU companies will need to consider whether their activities are covered by the GDPR and whether they must appoint an EU representative to monitor compliance with numerous new requirements, including breach notification, impact assessments and "the right to be forgotten."

**Brexit:** Many companies are concerned about the impact of Brexit on data protection and cybersecurity in the United Kingdom. The procedural details and timing of the UK's departure from the EU are still under consideration, and there are several possible outcomes, creating substantial uncertainty. In particular, while the UK government has confirmed that the UK will apply the GDPR coming into force in May 2018, many questions have been raised about what impact Brexit will have on UK businesses' ability to transfer data to and from businesses and other entities with the EU.

**Data Transfers:** The topic of international data transfers attracted significant attention in 2016 starting with the European Commission and the US Department of Commerce signing the EU-US Privacy Shield agreement, a much-anticipated framework for protecting personal data transferred from the EU to the United States. After the invalidation of the Safe Harbor framework in 2015, companies in the United States are now able to self-certify with the Commerce Department, attesting to their compliance with the Privacy Shield's principles, to enable data transfers from the EU. Privacy Shield-certified companies will need to ensure that their existing contracts with any third parties to which they further transfer EU data comply with the Privacy Shield's onward transfer requirements. It is important to note, however, that the future of the Privacy Shield agreement is uncertain. The agreement has already been challenged in the European Court of Justice under the same legal claim that led to the Safe Harbor framework's invalidation. More recently, questions have been raised about the US commitment to the Privacy Shield agreement in a Trump administration. For example, although intended to be "consistent with applicable law," the recent Executive Order on Enhancing Public Safety in the Interior of the United States has raised questions about privacy rights guaranteed by the Privacy Shield and the Judicial Redress Act. Companies that have certified or are considering the process should carefully track developments in this dynamic space.

Data transfer developments were not limited to Europe. For example, new rules on data transfers issued by Argentina's Data Protection Authority addressed two forms of model clauses to be used for cross-border data transfers—one for transfers to a data controller and another for transfers to a data processor. Argentina's new rules also provide a list of countries that, in the authority's view, offer an adequate level of data protection.

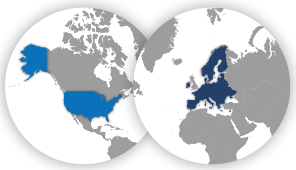
**Data Localization Rules:** Rules requiring data to remain within their country's jurisdiction will merit close scrutiny by companies doing business in China and Russia in 2017.

## European Union

In 2016, the European Parliament approved the new General Data Protection Regulation, which will come into force on May 25, 2018.

## United Kingdom

Many companies are concerned about the impact of Brexit on data protection and cybersecurity in the United Kingdom.



## United States-European Union

The European Commission and the US Department of Commerce signed the EU-US Privacy Shield agreement.

## China

China's comprehensive Cybersecurity Law (CSL) was passed in 2016 and will come into force in June 2017.

## Russia

Russia has been conducting inspections to verify compliance with its data localization law.

- China's comprehensive Cybersecurity Law (CSL) was passed in 2016 and will come into force in June 2017. The nation's first comprehensive cybersecurity regulation, it applies to network operators and operators of critical information infrastructures (CIIs), with heightened requirements, such as data localization and restrictions on cross-border data transfers, being imposed on the latter. Operators of CIIs are required to store within China "citizens' personal information and important data" gathered and produced while carrying out their operations, with exceptions subject to performance of a "security assessment." As of the date of writing, neither the scope of the CIIs nor the security assessment is known. Penalties for non-compliance include fines and the revocation of the business's license.
- Russia has been conducting inspections to verify compliance with its data localization law, which requires that Russian personal data be stored in data centers located within Russia, subject to exceptions. A court blocked online access in Russia to LinkedIn in November 2016, for example, for violation of the law.

# Conclusion

Regulators, policymakers, litigants and contracting parties continue to pay close attention to businesses' cybersecurity and data privacy practices. The constant stream of significant developments in these fields requires companies to respond nimbly and strategically. 2017 is poised to deliver yet more cybersecurity and data privacy challenges for businesses, including as the Trump administration pursues its priorities at the federal level. Developing effective, multidisciplinary responses based on a clear understanding of assessed risks and expertise across the enterprise will be crucial to managing those risks in the year ahead.

# Contributors

For more information about the topics raised in this 2017 Outlook, please contact any of the following contributing Cybersecurity & Data Privacy practice team lawyers.

Learn more about our full team and our Cybersecurity & Data Privacy practice.


Rajesh De
Global Cybersecurity & Data Privacy Practice Leader
+1 202 263 3366
rde@mayerbrown.com

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

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

David A. Tallman
+1 713 238 2696
dtallman@mayerbrown.com

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

Luke P. Levasseur
+1 202 263 3469
llevasseur@mayerbrown.com

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

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

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

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

Rebecca S. Eisner
+1 312 701 8577
reisner@mayerbrown.com

Lei Shen
+1 312 701 8852
lshen@mayerbrown.com

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

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

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

Xiaoyan Zhang
+86 21 6032 0228
xiaoyan.zhang@mayerbrownjsm.com

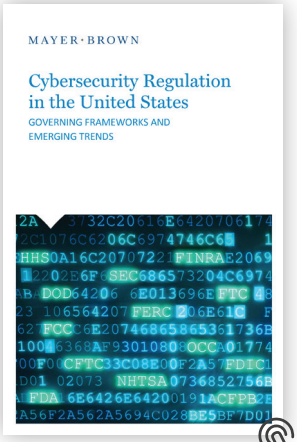
Charles E. Harris, II
+1 312 701 8934
charris@mayerbrown.com

David A. Simon
+1 202 263 3388
dsimon@mayerbrown.com

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

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

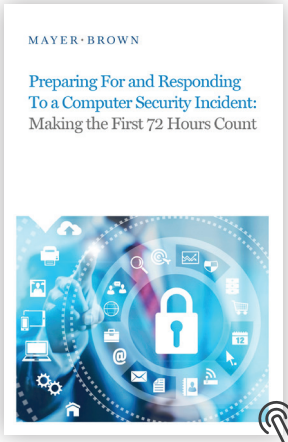
# Recent Thought Leadership




## Cybersecurity Regulation in the United States:

### Governing Frameworks and Emerging Trends

This 80-page handbook explores how to satisfy regulatory requirements in a manner that is consistent with business needs and that complements a risk-based approach to cybersecurity across the enterprise.




## Preparing For and Responding To a Computer Security Incident:

### Making the First 72 Hours Count

This 60-page book offers insights on how to prepare for a computer security incident and how to implement a timely, effective response.

## About Mayer Brown

Mayer Brown is a global legal services organization advising clients across the Americas, Asia, Europe and the Middle East. Our presence in the world's leading markets enables us to offer clients access to local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, CAC 40, DAX, Hang Seng and Nikkei index companies and more than half of the world's largest banks. We provide legal services in areas such as 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 and enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

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