MAYER·BROWN

2018 OUTLOOK

Cybersecurity and Data Privacy

KEY ISSUES

Companies should consider these issues as they continue to refine their cybersecurity and data privacy programs in 2018.

The cybersecurity and data privacy landscape raised new and challenging questions for businesses and governments around the world in 2017. We are poised to see new waves of technological disruption and legal complexity in 2018.

Technological developments that provide vast benefits will pose significant cybersecurity challenges and raise new data privacy questions. The Internet of Things ("IoT"), cloud computing, autonomous vehicles, artificial intelligence, big data and blockchain technologies are but a few of the technologies that businesses are incorporating into their operations and/or products. As these technologies emerge, grow and become more complex, so do cyber threats and data privacy challenges. Threat actors are evolving to take advantage of expanding attack surfaces, develop cybercrime as a service (with fees often paid in anonymous cryptocurrencies), and deliver new strains of ransomware and increasingly destructive attacks. Meanwhile, international regulatory regimes governing data protection are only becoming more complex.

The growing sophistication of threat actors will challenge businesses to strengthen their protections and response preparedness further. Cyber attacks that impacted international money transfer systems led to the issuance of a recent report by SWIFT/BAE Systems that illustrates how highly sophisticated malware can combine acquisition of system credentials, manipulation of logging data and other tactics to access systems covertly. Businesses will benefit from implementing and maintaining effective cybersecurity programs that include risk-based internal governance, vendor management and employee training to respond to these threats. At the same time, companies will benefit from following sound data privacy practices while also proactively adapting to new rules for international data transfers.

Against this background, key cybersecurity and data privacy issues for multinational companies in 2018 will include:

- Ongoing regulatory scrutiny of cybersecurity and data privacy;
- Vendor management as a key part of cybersecurity governance;
- Expanded cybersecurity and data privacy litigation, including in the IoT;
- Dynamic evolution of cybersecurity and data privacy policy; and
- Implementation and expansion of international frameworks.

Ongoing Regulatory Scrutiny of Cybersecurity and Data Privacy

Regulatory activity has expanded to include a variety of new actors with the potential to seriously impact private sector cybersecurity and data privacy practices. State agencies and regulatory authorities are increasingly asserting their authority to manage cyber and data privacy practices impacting their residents, while industry organizations and multiple federal departments and agencies continue to develop regulatory schemes, voluntary guidance, and best practices impacting the economy as a whole and specific industries. This trend toward more diverse regulatory activity is reflected in many of the developments that dominated 2017 and is likely to continue in the coming year.

CONTINUED CYBERSECURITY LEADERSHIP BY FINANCIAL REGULATORS

Financial services regulators have long taken a leadership role in establishing cybersecurity requirements that often are emulated in other industries. 2017 was another year of this leadership, and it appears likely to continue into 2018.

New York Cybersecurity Regulation. The New York State Department of Financial Services ("NYDFS") adopted a Cybersecurity Regulation that mandates cybersecurity standards for all institutions authorized by NYDFS to operate in New York, including many banks, insurance entities and insurance professionals. Significant provisions of the Cybersecurity Regulation became effective in 2017, and other provisions will be phased in throughout 2018 and 2019. The Cybersecurity Regulation is quite comprehensive and addresses everything from access controls and encryption to data disposal and employee training. It requires covered entities to report to NYDFS on the occurrence of a broad range of cybersecurity "events" that include attempted or successful data breaches, security incidents, hacking and intrusions. Covered entities also must make an annual certification to NYDFS regarding their compliance with the Cybersecurity Regulation. Implementation and ongoing compliance is expected to remain a significant issue throughout 2018 because of the large number of financial institutions regulated by the NYDFS.

Insurance Commissioners Adopt Model Data Security Law. The National Association of Insurance Commissioners adopted a model law establishing data security standards for companies and individuals licensed under state insurance laws. The model law builds on existing data privacy and consumer breach notification obligations by requiring insurance licensees to comply with detailed requirements for maintaining an information security program and responding to and giving notification of cybersecurity events. The model law is similar in many respects to the New York Cybersecurity Regulation. However, the model law pertains solely to insurance licensees, and, because it is only a model law, it will only apply to licensees in any given state if it is enacted into law by that state. Moreover, each state will have the freedom to modify the wording of the model law as it sees fit. States will begin considering whether to adopt the model law in 2018.

Federal Regulators Take a Flexible Approach to Cybersecurity for Big Banks. The federal banking regulators released a preliminary proposal for cyber risk management standards for large and interconnected financial-sector entities in 2016. The stated purpose of these contemplated standards was to increase covered entities' operational resilience and reduce the potential impact on the financial system in the event of a failure, cyber-attack or the failure to implement appropriate cyber risk management. However, in November 2017, staff of the Board of Governors of the Federal Reserve System indicated that the regulators have decided not to move forward with the preliminary proposal because of concerns about creating prescriptive standards that would deter effective risk management. Rather, regulators intend to pursue an as-of-yet undefined more flexible approach to establishing regulatory expectations for financial sector cyber risk management.

SEC Forms Cyber Enforcement Unit. The Securities and Exchange Commission ("SEC") established a "Cyber Unit" within its existing Enforcement Division to address cyber-based threats and target cyber-related misconduct in the securities markets. The Cyber Unit brought its first enforcement action in December 2017 in the form of an emergency action in federal district court to freeze assets associated with an allegedly fraudulent and illegal initial coin offering. That action against the issuer and promoters remains ongoing. The Cyber Unit intends to target issues including hacking of material nonpublic information, false information dissemination online and threats to critical market infrastructure.

Regulatory activity has expanded to include a variety of new actors with the potential to seriously impact private sector cybersecurity and data privacy practices.

SEC Is Hacked. In September 2017, the SEC disclosed that its online database for receiving, storing and publishing corporate securities filings, known as the Electronic Data Gathering, Analysis, and Retrieval system or "EDGAR," had been compromised in 2016 by hackers who may have traded on material nonpublic information obtained through the cyber attack. The disclosure resulted in significant public criticism of the SEC for falling short of its own guidance for public companies by delaying the disclosure for such a lengthy period. During its response to the hack, the SEC announced that it would continue to review its 2011 disclosure guidance for public companies. Although the timing of any refresh of that guidance is unknown, subsequent press reports indicated that the SEC was considering changes to that guidance that could address internal notification and escalation after a breach.

FSOC Continues To Highlight Cybersecurity. The Financial Stability Oversight Council ("FSOC") continued the annual trend of highlighting cybersecurity issues and developments in its annual report. Among other items, it recommended the creation of a private sector council of senior executives to focus specifically on how cyber incidents could impact business operations and market functioning, and to work closely with the government on cybersecurity issues and baseline protection expectations for the financial sector. It also recommended additional interagency collaboration to address systemic risks associated with significant cybersecurity incidents.

REGULATORS CONTINUE TO FOCUS ON CONNECTED DEVICES

As individuals and industries increasingly rely on Internet-connected devices, federal regulators have focused their attention on how to protect these devices from potentially dangerous vulnerabilities and how to guard data privacy. For example, the Food and Drug Administration ("FDA") has in recent years issued multiple guidance documents addressing cybersecurity expectations for medical devices. The FDA has also issued safety communications identifying vulnerabilities in specific medical devices and providing recommendations. Having held public workshops on medical device cybersecurity in 2016 and 2017, the FDA can be expected to maintain its focus on this issue in the coming year.

The National Highway Traffic Safety Administration ("NHTSA") has also focused on the safety impact of cybersecurity, exerting its authority to regulate the development and distribution of connected and autonomous vehicles. In September 2017, NHTSA released updated voluntary guidance addressing the development of automated driving systems that identifies cybersecurity among the safety elements of such systems and provides high-level recommendations for businesses in line with its 2016 guidance "Cybersecurity Best Practices for Modern Vehicles." (NHTSA describes data privacy as a key issue for automotive companies but does not address it in similar depth in the guidance.) This guidance also describes "Voluntary Safety Self-Assessments" that manufacturers can consider publishing to demonstrate their consideration of cybersecurity and the other priority safety elements. NHTSA can be expected to continue refining its approach in the coming year to vehicle cybersecurity as technologies mature and become more widely distributed.

FTC Leadership and Challenges. The Federal Trade Commission ("FTC") likewise has continued to focus on a broad range of cybersecurity and data privacy issues. For example, it, too, has considered these topics in the IoT context, including by hosting a forum in 2017 on cybersecurity and data privacy for connected vehicles. Recent enforcement actions, such as a settlement with a toy manufacturer that allegedly collected information relating to children through Internet-connected toys without appropriate parental consent and failed to appropriately secure that information, also reflect the heightened focus on security and privacy issues with respect to IoT devices.

At the same time, the FTC has faced challenges in pursuing enforcement actions based on potential future harm to consumers arising from purported failures to implement appropriate cybersecurity practices. There are two ongoing and disputed enforcement actions—*LabMD* and *D-Link*—which may shed light on the scope of the FTC's authority in this area. *LabMD*—a long-running data security action in which a medical testing company challenged the FTC's

authority—was argued before the Eleventh Circuit in June 2017, and a decision is expected in the coming months. A district court in California dismissed certain FTC claims in *D-Link*, a case in which the FTC alleged that the company's routers and other connected products lacked adequate security. The district court concluded, for instance, that the FTC had not stated an unfairness claims because it did "not allege any actual consumer injury in the form of a monetary loss or an actual incident where sensitive personal data was accessed or exposed" but, rather, relied upon the "mere possibility of injury."

Last month, Acting FTC Chairman Ohlhausen addressed this issue as part of an ongoing dialogue to "inform [FTC] case selection and enforcement choices going forward" at the FTC's Informational Injuries Workshop. Workshop questions included "How might frameworks treat past, current and potential future outcomes in quantifying injury?" It remains to be seen how questions like this will be answered if President Trump's recent FTC nominees are confirmed, and how the new composition of the FTC may alter the agency's jurisprudence and enforcement priorities.

Vendor Management as a Key Part of Cybersecurity Governance

The amount of data stored and processed by third-party vendors, including cloud providers, grew at a staggering pace during 2017, and we expect will continue to do so during 2018. Similarly, vendor technology and service offerings have become, and we expect will continue during 2018 to become, increasingly more sophisticated, allowing flexibility for companies and their vendors to design solutions to address evolving data privacy and cybersecurity laws and growing cyber threats. 2018 will be a year to re-examine and enhance operational and technical security requirements, contractual requirements, and vendor management practices to account for the changing landscape. Accordingly, vendor management, including updating and enhancing existing vendor relationships and contractual terms, will be a critical component of each company's cybersecurity and data privacy efforts in 2018.

VENDOR REGULATORY REQUIREMENTS

A number of older privacy laws and regulations tended to apply to the owner of the data versus a third-party vendor acting as a processor. Companies addressed these legal requirements through contractual clauses designed to require their vendors to assist them in complying with these requirements. More recently, the regulatory trend is to directly impose more accountability and responsibility for protection of data on third-party vendors or to indirectly impose them by

expressly requiring that companies pass through data privacy and security requirements to their vendors. Many of these new regulations will take effect in 2018 and beyond.

Vendor management, including updating and enhancing existing vendor relationships and contractual terms, will be a critical component of each company's cybersecurity and data privacy efforts in 2018.

New York State Financial Services Regulation. For example, the recent New York State Department of Financial Services cybersecurity regulation imposes third-party service provider requirements (among others, discussed above). These third-party service provider requirements, which take effect on March 1, 2019, obligate covered financial institutions to develop–and pass through to their vendors—written minimum cybersecurity policies designed to ensure the security of systems or data in the control of, or accessible by, third-party providers.

GDPR Vendor Requirements. The new European General Data Protection Regulation ("GDPR"), which will replace EU Directive 95/46/EC (the "Directive") in May 2018, places direct obligations on processors (e.g., vendors), including obligations to implement an appropriate level of security and to notify the controller of a data breach without undue delay. It also imposes requirements to be included in a contract with a processor, such as the requirement to delete or return all personal data to the controller after the end of the provision of the services related to the processing.

EVOLVING PRIVACY LAWS

GDPR. The implementation of the GDPR is expected to be a significant focus in contracting with vendors going forward. A business established outside the European Union will be subject to the GDPR if it processes personal data in relation to the offering of goods or services to individuals within the EU or monitors the behavior of individuals in the EU. Accordingly, businesses that previously were not subject to the Directive may become subject to the GDPR.

Under the GDPR, businesses must notify the relevant EU data protection authority of a data breach without undue delay and, where feasible, within 72 hours, unless the breach is unlikely to result in a risk to the individuals concerned, and notify individuals of a data breach without undue delay if a breach is likely to result in a high risk to the individuals concerned. In order for the company, as data controller, to meet these new notification requirements, corresponding notification obligations need to be included in vendor contracts.

The GDPR will introduce significant other changes and additional requirements that will also need to be addressed in vendor contracts, such as data subjects' "right to be forgotten," the requirement to implement data protection by design and by default, and the requirement for data protection impact assessments.

State Breach Notifications Requirements. The number of states with data breach notification laws has grown to 48 (plus the District of Columbia, Guam, Puerto Rico and the Virgin Islands). A number of these laws have broadened the definition of personal information (e.g., a user name and password) in recent years. Many national and international companies do not distinguish data by state residency. When data that are subject to different state requirements are intermingled, companies may have to observe the strictest state standards for all the data.

Localization Statutes. Vendor management is complicated by countries that have passed localization statutes, which limit or prohibit exporting certain information outside the country that has enacted such a statute. The most prominent examples are China and Russia. These laws will continue to impact the structure of vendor solutions, requiring local cloud instances and/or local providers in those countries with such statutes.

2018 is likely to see major cases on Article III standing, liability in the IoT, location privacy, government access to data stored abroad, and the authority of the FTC.

THIRD-PARTY ACCESS BY MEANS OF LEGAL PROCESS

Concerns around third-party access to data stored in the cloud will continue to impact the structure of cloud solutions. Federal agencies have a variety of tools for seeking electronically stored data. The extent to which data stored in a cloud environment can be—or should be—accessed through legal process directed at the cloud provider (in particular, where the

cloud environment resides in a different country from the customer) is currently in litigation, as described below. The Department of Justice released guidance in December 2017, recommending that prosecutors seek data directly from the enterprise, rather than its cloud storage provider, if doing so will not compromise the investigation.

GROWTH AND EVOLUTION OF CLOUD SOLUTIONS

We expect businesses to continue to adopt cloud solutions at a rapid pace during 2018. Cloud providers will continue to become more sophisticated in understanding the need to develop solutions designed to meet regulatory requirements, including enhancements of cloud solutions specifically designed for health care companies, financial services companies and companies subject to similar industry-specific regulation. Further, cloud contracting practices have become more mature. For example, providers will likely agree to adhere to certain industry standards and/or agree that security protocols, while they may change over time, will not become less stringent than those in place on the contract date. Customers and vendors will continue to look to implement multiple cloud instances where appropriate as a means to address data localization requirements and attempt to minimize third-party access to data through legal process served on vendors.

Expanded Cybersecurity and Data Privacy Litigation, Including in the IoT

The trends in cybersecurity and data privacy litigation seen in 2017 are poised to continue in 2018. As discussed above, questions regarding the precise scope of FTC authority to regulate cybersecurity remain pending in federal court. In addition, lower court splits over questions about Article III standing in data privacy and cybersecurity litigation are likely to deepen. Litigation relating to the IoT is also likely to continue to grow in importance in the coming year, and the Supreme Court is poised to decide two blockbuster cases relating to location privacy and the government's ability to compel production of data stored overseas.

Ongoing Litigation Over Standing in Privacy and Cybersecurity Cases. In 2016, the Supreme Court's *Spokeo* decision confirmed that the bare allegation that a statute has been violated does not-without adequate allegations that the violation produced a concrete and particularized injury-meet the Article III standing requirements necessary to proceed in federal court. (Mayer Brown has represented *Spokeo* throughout the litigation.) Though lower courts assessing standing under a wide variety of laws have wrestled with how to apply this decision, *Spokeo* has had particular impact in the data privacy and cybersecurity contexts. Although the Supreme Court denied *Spokeo*'s second petition for certiorari in January 2018, the Court will likely have to revisit the issue of what constitutes the concrete harm necessary for standing in the near future, as lower courts' interpretations of the *Spokeo* holding continue to diverge.

Similarly pending before the Supreme Court is a petition for certiorari filed by health insurer CareFirst. The petition seeks review of the DC Circuit's ruling that plaintiffs adequately pled standing based on an increased risk of identity theft due to a recent data breach. The DC Circuit's analysis largely tracked the Seventh Circuit's decision in *Neiman Marcus,* which reasoned that hackers' theft of credit card information created a sufficient risk of future financial injury to satisfy Article III, such that cardholders need not wait for credit card fraud to occur before having standing to sue. And, by joining the Seventh (and Sixth) Circuits on this issue, the DC Circuit deepened a split with the Second, Third, Fourth and Eighth Circuits, all of which have declined to find standing in comparable circumstances. If the Supreme Court decides to hear the *CareFirst* case, its resolution will have extremely important implications for data breach litigation.

Internet of Things Litigation. Cybersecurity and data privacy litigation relating to IoT devices also continued to grow in 2017 and appears likely to be increasingly prominent in 2018. Putative classes have brought suit over alleged vulnerabilities in medical devices, cars, baby monitors and other connected products. Other plaintiffs have claimed that such products have impermissibly collected or used their personal data. Many of these complaints face a threshold infirmity: no one has suffered a concrete injury from the perceived product flaw. Plaintiffs consequently have been developing new theories of economic loss or other forms of injury in an attempt to establish constitutional standing in federal court. As with traditional data breach and data privacy litigation, how federal courts resolve these standing questions will have a substantial effect on the course of IoT litigation in the coming years. Of course, standing is not the only hurdle putative class representatives face: they must also state a

cognizable claim and secure class certification, two hurdles that many, if not most, current IoT plaintiffs will be unable to surmount. Nonetheless, despite the many potential weaknesses in these lawsuits, they may still pose substantial risks to businesses and may lead to settlement, as seen in the 2017 *We-Vibe litigation*.

Blockbuster Privacy Litigation Before the Supreme Court. Two blockbuster privacy cases on location privacy and government access to data held abroad are currently before the Supreme Court. The forthcoming decisions are likely to speak to critical principles that will affect consumers' expectations of privacy in connected services and how businesses deliver such services to consumers and commercial clients.

First, the Court is returning to questions of location privacy in *Carpenter v. United States*, a case that may build upon its earlier decisions in *United States v. Jones* (attachment of a GPS tracking device to a vehicle on public roads constituted a "search" for purposes of the Fourth Amendment) and *Riley v. California* (warrantless search of cell phone incident to arrest violated Fourth Amendment). Specifically, the *Carpenter* case raises the question whether the government needs a warrant to access historical cell phone location records. The Court heard oral arguments in November 2017, with the Justices' questions focusing on the pervasiveness of private collection of consumer data and law enforcement's ability to access customer data in similar contexts. The Justices' determinations about individuals' expectations of privacy in cell phone data may have implications for private sector access and use of such data and related civil litigation.

Second, in *United States v. Microsoft*, the Court is taking on a question that has substantial implications for the cloud computing industry: whether the government may compel production of data that is located abroad but within the control of providers found in the United States. The case involves the federal government's challenge to a Second Circuit decision quashing a warrant under the Stored Communications Act (a title of the Electronic Communications Privacy Act ("ECPA")) that would have forced the provider to produce email data housed on a server in Ireland. Briefing will be completed by the end of January 2018.

A decision in both of these cases is expected by the end of June 2018.

Dynamic Evolution of Cybersecurity and Data Privacy Policy

The past year was a busy one when it comes to cybersecurity and data privacy policy, with significant activity on a range of policy issues in both the executive branch and Congress, as well as in numerous states. In its

first year in office, the Trump Administration sought to make a mark on cybersecurity issues, and its active involvement is expected to continue in 2018. Further activity is also expected in a number of areas in the coming year, especially as relates to data breach and data privacy, standard setting, and digital privacy issues.

In its first year in office, the Trump Administration sought to make a mark on cybersecurity issues, and its active involvement is expected to continue in 2018.

Executive Order on Cybersecurity. In May 2017, President Trump issued an executive order on cybersecurity, with its most immediate impacts being on federal networks and on critical infrastructure (especially so-called "Section 9" high-risk critical infrastructure targets). The order directed the Department of Homeland Security and other federal agencies to work with Section 9 entities to evaluate how to use government resources to support cyber risk management for critical infrastructure. The administration has also begun an effort to encourage private entities to address botnet and other attacks, recently soliciting comment on a draft report that encourages federal agencies to work with industry to improve the overall security of the digital ecosystem against such threats. The administration aims to release a final version of the report, which was called for in the executive order, in May 2018. The executive order also directed efforts to consider cybersecurity risks in the energy and defense industrial sectors and the risk management efforts of the various federal agencies.

New Federal Data Breach Legislation. In September 2017, Equifax, the consumer reporting agency, announced that it had suffered a data breach attack affecting 145 million data subjects by hackers gaining access to personal data, including Social Security numbers. Policymakers were quick to react. At least seven bills that include new security rules for consumer-reporting agencies were introduced in Congress, and several more bills were introduced that targeted how other companies collect, manage, use and secure consumer data.

Best Practice Development and Standard Setting. 2017 saw continued emphasis on security best practices developed through open and transparent multistakeholder processes. The National Institute of Standards and Technology at the Department of Commerce published its second draft version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity and sought further comments through mid-January 2018. In 2017, the National Telecommunications and Information Administration at the Department of Commerce convened a multistakeholder process on security upgradability for the IoT.

Attention to Digital Privacy. As discussed above, a Supreme Court is set to hear a dispute over whether US companies can be compelled to produce data stored overseas in response to certain forms of legal process. The case addresses the territorial reach of ECPA and highlights the challenges associated with applying a law Congress drafted in 1986 to present-day technology. Reforming ECPA to bring it into the digital age continues to receive broad-based support in Congress. In 2017, the House passed its version of ECPA reform, and several update bills were introduced in the Senate last summer, including the International Communications Privacy Act, which would clarify how US law enforcement can obtain information stored overseas. In addition to issues of access to data stored in the cloud, Congress also voted to reauthorize Section 702 of the FISA Amendments Act, the statute that allows collection in the US of data from non-US persons located abroad without a warrant, in January 2018. The six-year reauthorization, which President Trump signed into law, made various amendments to the statute, but excluded more extensive changes sought by privacy advocates. As a result, many of the policy debates over Section 702 remain open for the years ahead.

Revised Vulnerabilities Equities Process. The vulnerabilities equities process ("VEP") originates from a directive issued by President Bush (43), which was tweaked by President Obama and applied to when and how the government discloses information about IT vulnerabilities it discovers or acquires. Following the introduction of legislation in May 2017 that would codify the vulnerability equities review process, the Trump Administration announced its own updated and more transparent VEP process that drew praise from many in

industry. The revised VEP articulates the process and factors for deciding whether the government should disclose vulnerabilities or retain them for certain law enforcement and national security purposes.

Hack Back. In October 2017, Reps. Tom Graves (R-GA) and Kyrsten Sinema (D-AZ) introduced the Active Cyber Defense Certainty Act ("ACDC"). The ACDC would amend the Computer Fraud and Abuse Act to allow individuals and companies to engage in certain active defense measures-or "hacking back"-to protect their networks in the event of cyber attacks. The bill would allow victims to hack back to disrupt cyber attacks, monitor attackers' behavior, and gather information to attribute the attack within limitations (for example, reciprocal attacks that result in financial harm or collateral damage are prohibited). Though the bill has gained additional co-sponsors since its introduction, it remains controversial. For example, critics have said that the bill does not sufficiently address the potential collateral consequences of allowing civilians to disrupt ongoing malicious cyber activity.

New State Laws. In 2017, we saw several states move forward with legislation addressing security and data privacy concerns. Following the enactment of the final cybersecurity regulations for New York's financial services sector in March, state financial regulators in Colorado and Vermont adopted their own cybersecurity rules that would apply to certain entities doing business in their states. In April 2017, New Mexico became the 48th state to enact a data breach notification law (only Alabama and South Dakota remain without such a law), which, like a small group of others, imposes a specific notification deadline of 45 days after the discovery of a breach. State policymakers also reacted to the major breaches of 2017. In New York, for example, the SHIELD Act was introduced, which would require companies to adopt "reasonable" safeguards to protect sensitive data, increase reporting requirements and provide a safe harbor for companies that meet certain certification standards. On the privacy side, Washington state became the third state–after Texas and Illinois–to enact a law regulating the commercial collection and use of biometric information, although the Washington law does not provide a private right of action.

Implementation & Expansion of International Frameworks

Cybersecurity and data privacy have been topics of focus around the world, and several significant developments in this realm will affect international businesses in 2018. Among these developments are various data protection authorities in the European Union ("EU") issuing guidance on how to comply with the upcoming General Data Protection Regulation; the EU-US Privacy Shield undergoing its first joint annual review; China's Cybersecurity Law ("CSL") coming into force in 2017; and other evolving data protection requirements in the Asia-Pacific region.

General Data Protection Regulation: The GDPR will come into force on May 25, 2018. The GDPR brings with it a number of significant changes from the EU Directive, including significant fines, breach notification requirements, a change in jurisdictional scope, new data subject rights and direct processor requirements. To address concerns regarding how to comply with the various new requirements, several data protection authorities, as well as the Article 29 Working Party ("A29WP") have been releasing and will continue to release guidance concerning the GDPR. For example, the A29WP has released guidelines on the right to data portability, data protection officers ("DPOs") and data protection impact assessments ("DPIAs"), as well as draft guidance on data breach notification and how to obtain consent. The UK's ICO has also released draft guidance on contracts between controllers and data processors and how to obtain consent under the GDPR. Additional guidance is expected in 2018.

The GDPR brings with it a number of significant changes from the EU Directive, including significant fines, breach notification requirements, a change in jurisdictional scope, new data subject rights and direct processor requirements.

Privacy Shield. The Privacy Shield was adopted in July 2016 as the successor to the invalidated EU-US Safe Harbor framework to allow for the transfer of personal data from the EU to US companies that certify under the framework. As

part of the first annual joint review of the Privacy Shield, both the EU Commission and the A29WP released reports regarding the adequacy of the Privacy Shield.

The EU Commission published its report regarding the Privacy Shield framework in October 2017. The report found the Privacy Shield to provide an adequate level of protection for the transatlantic transfer of personal data, but it also made a number of recommendations for improvements. For example, the report recommended that the US Department of Commerce proactively and regularly monitor for false claims to reduce the risks of inaccurate information and to help identify possible compliance issues that may require further attention.

Similarly, the A29WP released the results of its review of the Privacy Shield framework in December 2017. While the A29WP acknowledged that the Privacy Shield is an improvement over the Safe Harbor framework, it also identified several "important unresolved issues" with the Privacy Shield as it is currently operated. For example, the A29WP indicated that there is a lack of guidance and clear information on the principles of the Privacy Shield. The A29WP called upon the EU Commission and US authorities to immediately restart discussions and to address the identified concerns by the second annual joint review; otherwise, the A29WP warned that it will bring claims regarding the adequacy of the Privacy Shield before EU national courts for a preliminary ruling.

In the meantime, the adequacy of the Privacy Shield stands, so US companies can continue to rely on this framework to receive personal data from the EU.

China's Cybersecurity Law. The CSL took effect in June 2017. The law is controversial as it requires data collected or generated in China during business operations to be stored in China unless the entity subjects itself to a security assessment and shows that cross-border transfer of the data is necessary for its business. For most businesses, there is a grace period for compliance with the cross-border transfer provisions until December 31, 2018.

Other Developments in the Asia-Pacific Region. Several other countries across the Asia-Pacific region are also moving toward tighter regulations and stronger enforcement with regard to cybersecurity and data privacy. For example, Australia passed the Privacy Amendment (Notifiable Data Breaches) Bill 2016 in February 2017, requiring organizations, as soon as practicable, to notify the Office of the Australia Information Commissioner and affected individuals of data breaches that are likely to result in serious harm. The Amendment will take effect in February 2018. In addition, South Korea recently amended legislation to require all mobile app service providers to inform a user of necessary and optional access rights to the user's smartphone and to obtain the user's permission before enabling those access rights. India's Computer Emergency Response Team ("ICERT") published a notice that described the types of "cyber security incidents," including certain types of attacks, that it believed should be reported to it under the Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013. Finally, several countries have released draft bills concerning cybersecurity, including Singapore, Vietnam and Taiwan.

Conclusion

Cybersecurity and data privacy continue to be focus areas for regulators, policymakers, legislators, litigants and private sector companies across industries and around the world. Tracking developments across this space can yield substantial benefits as companies seek to stay ahead of the curve on evolving expectations and new challenges. As cybersecurity threats increase and regulators around the world refine data privacy regimes, businesses that anticipate emerging cyber risks and are prepared to navigate new data privacy regulations will be well positioned to succeed in the year ahead.

CONTRIBUTORS

For more information about the topics raised in this 2018 Outlook, please contact any of the following contributing Cybersecurity & Data Privacy practice team lawyers. Learn more about our full team and practice here: mayerbrown.com/experience/cybersecurity-data-privacy

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

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

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

Samantha Booth
+1 650 331 2029
sbooth@mayerbrown.com

Qi Chen
+852 2843 5798
qchen@mayerbrownjsm.com

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

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

Veronica R. Glick
+1 202 263 3389
vglick@mayerbrown.com

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

Mickey Leibner
+1 202 263 3711
mleibner@mayerbrown.com

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

Linda L. Rhodes
+1 202 263 3382
lrhodes@mayerbrown.com

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

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

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

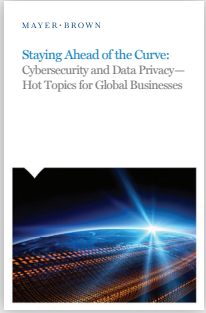
Joel R. Spencer
+1 202 263 3243
jspencer@mayerbrown.com

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

Matthew A. Waring
+1 202 263 3273
mwaring@mayerbrown.com

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

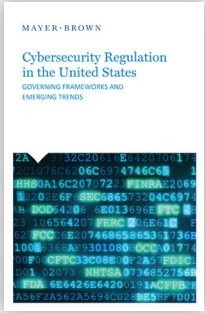
PUBLICATIONS



Staying Ahead of the Curve: Cybersecurity and Data Privacy—Hot Topics for Global Businesses

Staying Ahead of the Curve: Cybersecurity and Data Privacy—Hot Topics for Global Businesses, highlights key developments and priorities in these critical fields, from the Internet of Things and the cloud to complying with China's new cybersecurity law and Europe's General Data Protection Regulation.

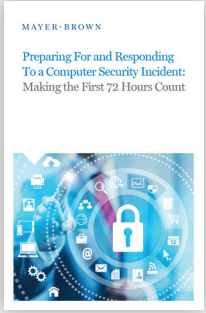
To request a copy of this guide, please visit: mayerbrown.com/staying-ahead-of-the-curve-cybersecurity-and-data-privacyhot-topics-for-global-businesses-09-28-2017



Cybersecurity Regulation in the United States: Governing Frameworks and Emerging Trends

Cybersecurity Regulation in the United States: Governing Frameworks and Emerging Trends offers insights on the regulatory frameworks applicable across key sectors of the United States economy, as well as emerging regulatory trends across sectors.

To request a copy of this guide, please visit: mayerbrown.com/Cybersecurity-Regulation-in-the-United-States-Governing-Frameworks-and-Emerging-Trends-09-29-2016



Preparing For and Responding To a Computer Security Incident: Making the First 72 Hours Count

Preparing For and Responding To a Computer Security Incident: Making the First 72 Hours Count offers insights on how to prepare for a computer security incident and how to implement a timely, effective response.

To request a copy of this guide, please visit: mayerbrown.com/preparing-for-and-responding-to-a-computer-security-incident-making-the-first-72-hours-count

ABOUT

CYBERSECURITY & DATA PRIVACY

With our global platform and our experienced and practical team of cybersecurity and data privacy lawyers, our firm can serve clients across a full range of domestic, international and cross-border privacy issues.

The cybersecurity landscape is evolving more rapidly than ever before, and the threats to businesses' critical information and assets—as well as to their bottom lines—are only increasing. Breaches continue to grow in scale and sophistication, regulators are crowding the field with an expanding and shifting array of requirements and de facto standards, and litigation remains perilous. Now, more than ever, businesses must think strategically about the cyber threats they face—whether to consumer or employee information, intellectual property or product safety—and take practical steps to address the associated legal, business and reputational risks.

Mayer Brown brings a comprehensive and integrated approach to cybersecurity and data privacy challenges, offering our clients strategic thinking and practical legal advice. Our practice is composed of more than 50 lawyers worldwide from disciplines that include litigation, regulatory, corporate, government affairs and global trade, intellectual property, enforcement, employment, insurance and technology transactions. We leverage our broad and deep experience in these key disciplines to build tailored teams to address the specific issues that our clients face. This approach to our Cybersecurity & Data Privacy practice distinguishes us from other firms that rely on "one size fits all" privacy and security lawyers who attempt to cover the waterfront of these ever-increasing and complex issues.

The firm's global platform enables us to provide exceptional service to our clients across the globe. Mayer Brown and affiliated lawyers located throughout the Americas, Europe and Asia have deep knowledge and a practical understanding of the cybersecurity and data privacy statutes and regulations in their home countries and surrounding regions. This experience and global capability allows us to address a client's most complex international cybersecurity and data privacy issues, whether they require advice on creating an enterprise-wide privacy framework, counsel on international data transfers, or assistance in responding to a data breach in multiple jurisdictions. Together, our lawyers help clients respond proactively to international developments such as the Safe Harbor decision or the release of the General Data Protection Regulation in Europe or changes to the Personal Data (Privacy) Ordinance in Hong Kong. In addition, our practice maintains an extensive network of local counsel in countries where we do not have offices and with whom our lawyers liaise as needed.

About Mayer Brown

Mayer Brown is a global legal services organization advising clients across the Americas, Asia and Europe. 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.