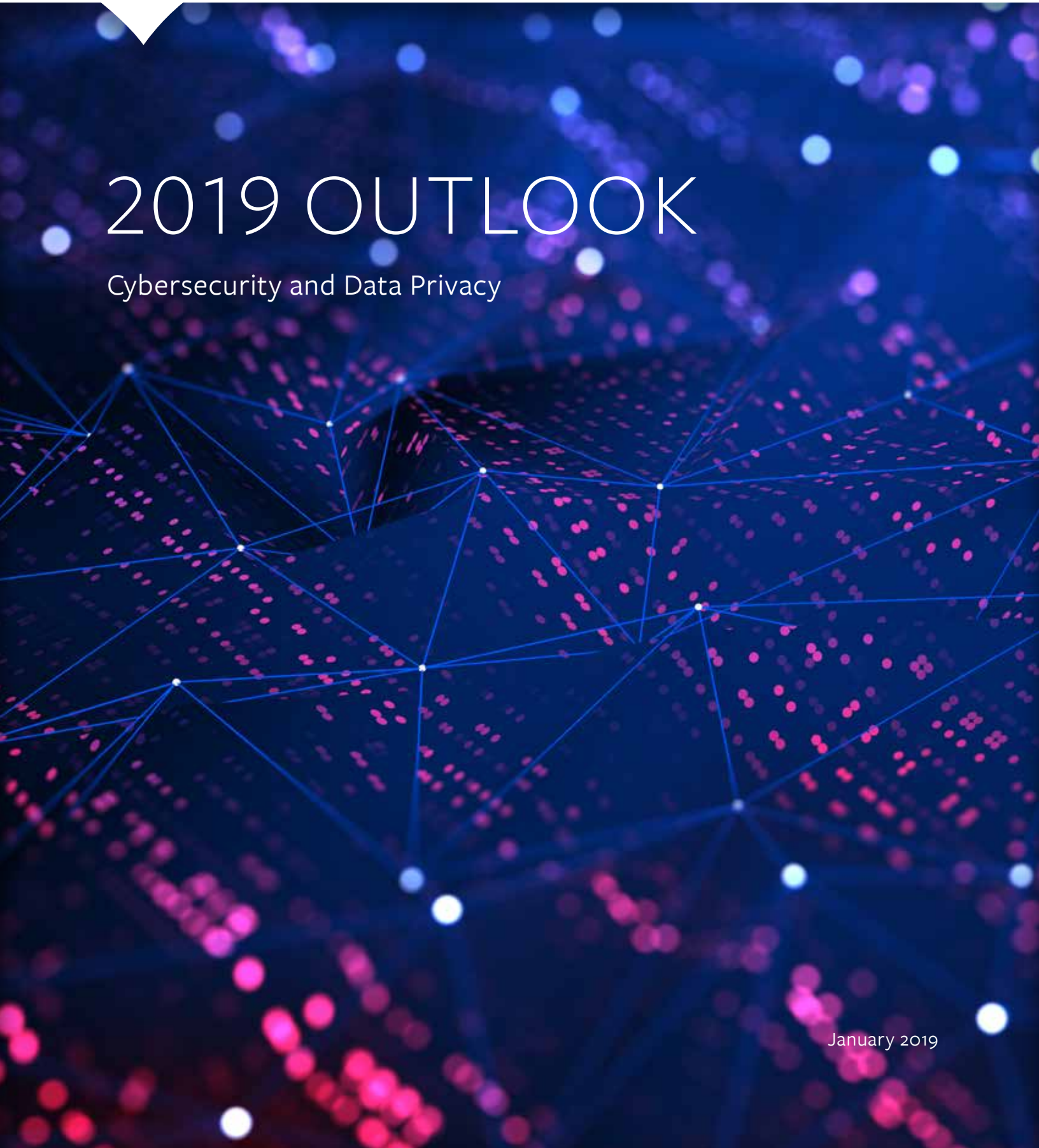
MAYER·BROWN

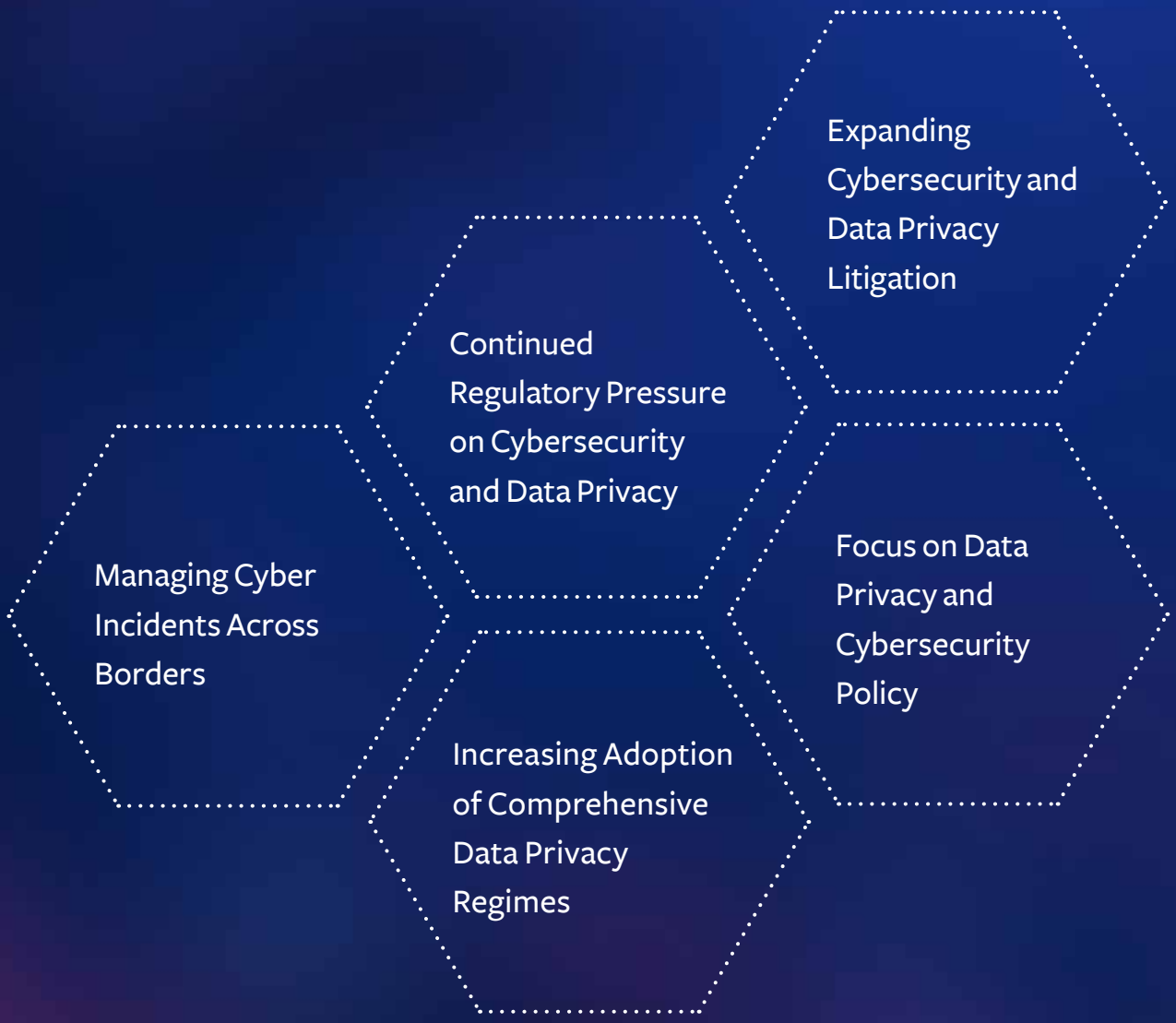


2019 OUTLOOK

Cybersecurity and Data Privacy

January 2019

KEY ISSUES


Expanding Cybersecurity and Data Privacy Litigation
Continued Regulatory Pressure on Cybersecurity and Data Privacy
Managing Cyber Incidents Across Borders
Focus on Data Privacy and Cybersecurity Policy
Increasing Adoption of Comprehensive Data Privacy Regimes

Cybersecurity and data privacy presented some of the most complex legal questions and business risks that multinational companies faced in 2018. Businesses should expect continued growth in cyber and data privacy challenges in 2019.

Cyber attacks became even more sophisticated and severe in 2018, with incidents ranging from exfiltration and extortion schemes, to attacks on critical infrastructure, threats to connected products, and vast data breaches. Even technically simple (but often highly costly) business email compromise attacks spiked in 2018, underscoring the continuing importance of implementing defensive best practices. The data privacy landscape also continued to grow more complex, as the General Data Protection Regulation ("GDPR") went into force in the European Union ("EU")—and affected business practices around the globe. Other jurisdictions are already following suit, passing similar laws that will require significant compliance efforts.

2019 is poised to continue this trend of increasing complexity—and consequences—for cybersecurity and data privacy challenges. The adoption and new use cases for disruptive technologies—whether autonomous vehicles, artificial intelligence, connected products or much more—will help drive the evolution of the cybersecurity and data privacy legal landscape, along with the introduction of new regulatory regimes, expanding litigation risk and scrutiny from policy makers across jurisdictions.

The stakes are high. A report issued by the White House Council of Economic Advisers in 2018 estimated that malicious cyber activity cost the US economy between $57 billion and $109 billion in 2016 alone. For individual companies, the effects can be devastating. Cyber incidents have led to the departure of companies' most senior executives, disrupted mergers and acquisitions, and caused massive financial and reputational costs. Data privacy compliance issues have resulted in both substantial legal penalties and loss of the consumer trust on which companies depend.

Against this background, key cybersecurity and data privacy issues for multinational companies in 2019 will include:

- Managing Cyber Incidents Across Borders
- Continued Regulatory Pressure on Cybersecurity and Data Privacy
- Expanding Cybersecurity and Data Privacy Litigation
- Increasing Adoption of Comprehensive Data Privacy Regimes
- Focus on Data Privacy and Cybersecurity Policy

Managing Cyber Incidents Across Borders

Recent years have seen steady growth in the sophistication and severity of cyber attacks on multinational businesses. Increasingly, these incidents are not limited to a single jurisdiction, but stretch across borders, often in a manner that makes responding to the incident substantially more complex. A breach of a customer database, for example, may trigger notification obligations in multiple countries, and a ransomware attack may encrypt systems across a company's global footprint. Similarly, a forensic investigation may require a company to act across borders, such as by working with third-party hosting companies in different countries. Moreover, cyber incidents involving connected products may affect multiple jurisdictions at once for any company that sells into multiple markets. In these and many other cases, the cross-border nature of the incident can make responding significantly more complicated, whether because of competing regulatory imperatives and legal risks in different jurisdictions, increased challenges coordinating actions across globally distributed teams, or practical obstacles in reaching affected systems.

Cross-border cyber incidents are likely to become more frequent in 2019.

Here, we identify key issues that companies may face in responding to these incidents—and that companies will likely benefit from thinking through and addressing in relevant incident response plans and playbooks in advance.

Managing Forensic Investigations on a Global Basis. Performing an effective forensic investigation on a global basis can substantially reduce legal risk in the wake of a cyber incident that crosses borders. Managing the investigation so that key artifacts are secured, appropriate analyses are performed in a timely manner, and sound conclusions are reached using a documented methodology, can position a company well for potential litigation, enable it to interact more confidently with regulators, and support more effective engagement with law enforcement. For example, a sound forensic investigation (and a proper understanding of the confidence that should be laid upon findings) can help to determine which geographic regions may be affected by a data breach and what data may have been rendered unavailable, corrupted or subject to unauthorized access or loss. As data privacy regimes continue to expand and develop in 2019, answering such questions is likely to be essential to effectively navigating legal and regulatory obligations—including individual and regulatory notification requirements—that may have been triggered by such an incident.

Managing Legal Risk on a Global Basis. Cross-border cyber incidents can raise legal questions under the laws of numerous jurisdictions, including some in which the affected company may not routinely do business. Consequently, the coming year is likely to see companies facing pressure to manage the geographically and substantively diverse legal issues raised by cross-border incidents. In responding to this challenge, companies are likely to want to ensure not only that they have sufficient capability to understand the laws in these various jurisdictions, but also that they can effectively manage competing legal interests across jurisdictions. For example, in the United States, companies responding to an incident will often issue a broad litigation hold to avoid deletion of data that is likely to be relevant to anticipated litigation. However, this can sometimes come into tension with privacy laws in other jurisdictions that direct the deletion of data that is no longer required for business purposes. In addition, regulatory and public expectations for prompt notifications and transparency and views on appropriate levels of inquiry may vary across borders. Such variation makes it likely that companies will face challenges in balancing the need to communicate with regulators and other stakeholders with other legal risks, including potential litigation in the United States.

Strategic Law Enforcement Engagement. Because cross-border cyber incidents often involve criminal activity in multiple jurisdictions, companies will likely find themselves balancing the risks and benefits of engaging with one or more law enforcement agencies as part of their incident response processes. Engaging with law enforcement in a cross-border incident can be a prudent step. Law enforcement agencies can provide threat intelligence, coordinate with foreign counterparts to compel third-party disclosures, or take steps, such as seizing servers used by malicious actors, that may mitigate harm or deter the threat actor from taking further damaging actions. However, law enforcement engagement also can come with trade-offs, including the potential loss of control and confidentiality over specific

aspects of an incident response process. Analyzing these potential costs and benefits can be particularly complex in the context of a cross-border incident that can implicate the interests of law enforcement agencies in multiple countries. For example, a company may have to decide which law enforcement agency or agencies it should engage with, how this decision will impact engagement with regulators in those countries, and how it will support any ongoing engagement with foreign law enforcement.

Preserving Privilege. Many countries recognize some form of attorney-client privilege, but the protection varies in its application and scope even where it is recognized. For example, some countries do not provide in-house counsel work product and communications the same level of protection often afforded to those of outside counsel, and privilege can be lost if information is communicated to wider groups of recipients within a client. Understanding these jurisdictional distinctions is likely to be important as companies respond to cross-border incidents and manage subsequent regulatory inquiries or civil discovery. Moreover, companies facing such incidents in 2019 are likely to benefit from following standard best practices for protecting privilege where it applies, including by employing appropriate markings on all documents and keeping communications to "need to know" audiences within the business.

Extraterritorial Application of Data Privacy and Security Laws. Various data privacy and security laws extend to businesses based well beyond a country's borders. For example, the GDPR applies to data processing activities relating to the offering of goods or services to data subjects situated in the EU and monitoring of the behavior of such data subjects, even if the business is not formally established in the EU. Companies facing cross-border incidents in 2019, consequently, will want to evaluate the full range of legal regimes to which they may be subject and which supervisory authorities they will be required to coordinate with.

Continued Regulatory Pressure on Cybersecurity and Data Privacy

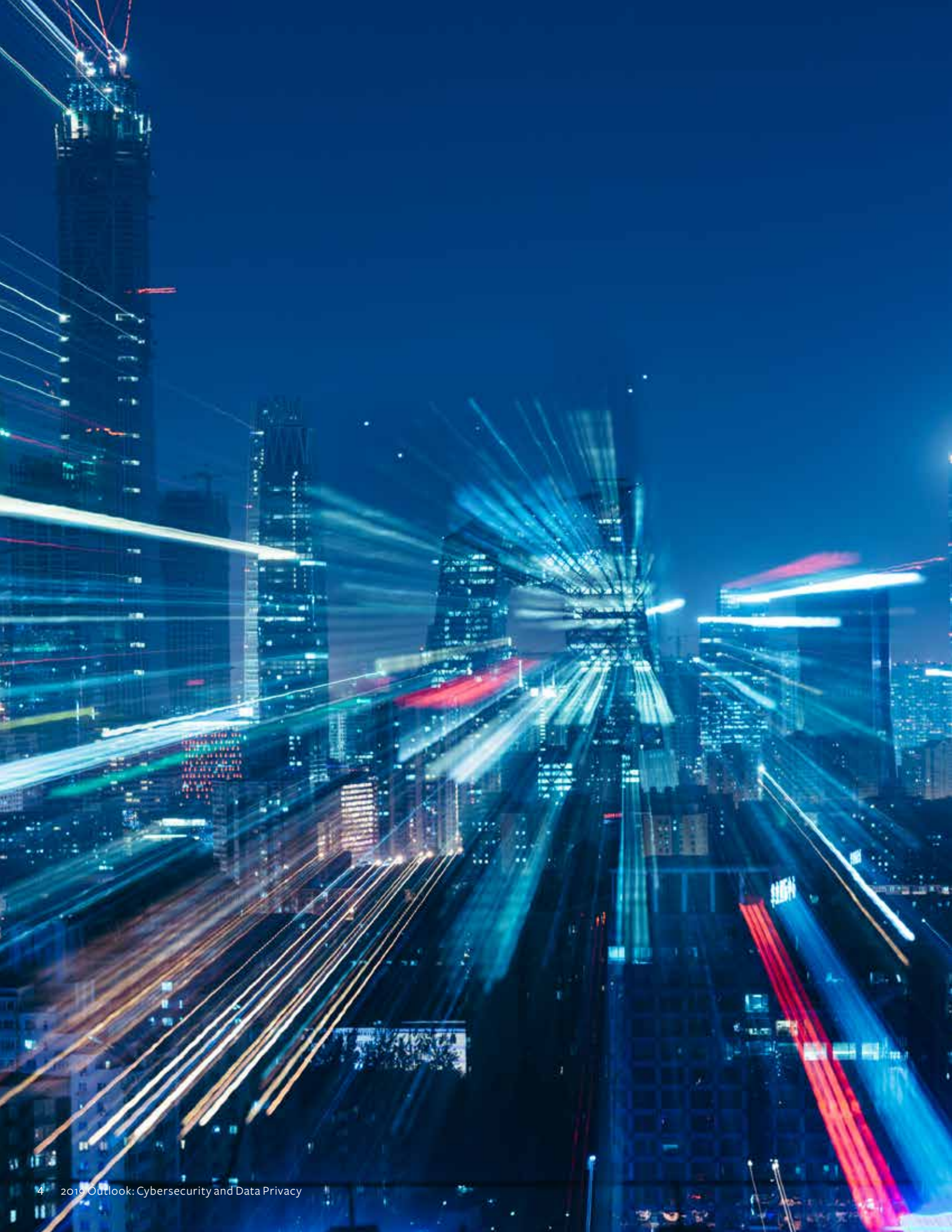
Regulatory scrutiny of cybersecurity and data privacy practices continued to grow across industries in 2018. We expect regulators to continue this trend in 2019 through use of the full range of regulatory tools, including new or updated guidance, investigations and enforcement actions, engagement with industry and other stakeholders, supervisory examinations and public education. This trend will likely be seen across numerous economic sectors. We focus below on five areas—financial services, public company disclosures, medical devices, connected vehicles, and consumer data security and privacy—that are likely to see regulatory activity in the coming year, both with respect to traditional enterprise technology and the expanding world of connected products.

FINANCIAL SERVICES

Financial services regulators have long taken a leading role with respect to cybersecurity and data privacy. 2018 was no exception as a broad range of state and federal agencies engaged with industry on these important topics. This trend is set to continue into 2019.

Financial institutions and other public companies will benefit from carefully monitoring proposed regulatory changes both to take available opportunities to weigh in and shape regulatory policy and to enable effective compliance. Below we highlight regulatory topics for financial services companies and institutions to watch in 2019.

NAIC Model Data Security Law Implementation. In May 2018, South Carolina became the first state to adopt the model data security law that was developed in 2017 by the National Association of Insurance Commissioners ("NAIC"). In December 2018, Ohio and Michigan became the second and third states to adopt the NAIC model law. If adopted by a state, the NAIC model law will build on existing data privacy and consumer breach notification obligations by requiring insurance licensees to comply with detailed requirements regarding maintenance of an information security program and notification of cybersecurity events. We expect that more states will adopt the NAIC model law in 2019, with versions already introduced in the Rhode Island and Nevada legislatures.



NASAA Model Information Security Rule Proposal. In September 2018, the North American Securities Administrators Association ("NASAA") proposed a model rule for information security and privacy requirements for state-registered investment advisers ("state-RIAs"). We expect the proposal will be finalized in 2019, but it remains to be seen how rapidly it will be adopted by states, and it is unclear how the proposal will interact with existing cybersecurity requirements, such as Colorado's and Vermont's cybersecurity regulations for broker-dealers and state-RIAs providing services in those states or Massachusetts's generally applicable cybersecurity regulation.

New York Cybersecurity Regulation Implementation. The cybersecurity regulation ("NY Regs") adopted by the New York State Department of Financial Services will turn two years old in February 2019, and the final requirement in its phased implementation schedule will become effective in March 2019. This final requirement relates to the relationship between financial institutions that are authorized to engage in business in New York ("Covered Entities") and third-party service providers ("TSPs"), and will require Covered Entities to pass on certain cybersecurity obligations to TSPs by requiring Covered Entities to develop written policies and procedures designed to ensure the security of systems and data accessible to, or held by, TSPs. Additionally, each Covered Entity will be required to address with their TSPs, through due diligence or contractual protections, (i) the use of access controls and multifactor authentication, (ii) encryption of nonpublic information in transit and at rest, (iii) prompt notification to the Covered Entity of certain cybersecurity events and (iv) representations and warranties from the TSPs concerning their cybersecurity policies and procedures.

SEC Red Flags Rule Enforcement. In September 2018, the US Securities and Exchange Commission ("SEC") brought its first enforcement action against a registered broker-dealer/investment adviser under the Identity Theft Red Flags Rule ("Regulation S-ID"). While this is the SEC's first enforcement action alleging violations of Regulation S-ID, it is part of a growing trend of initiatives by the SEC and the Financial Industry Regulatory Authority that focus on cybersecurity in their examinations of registered securities entities.

NFA Breach Notification Requirement. In January 2019, the National Futures Association ("NFA") revised the information security requirements for its members, which consist largely of regulated participants in the commodity derivatives markets. The revisions become effective on April 1, 2019, and require members to notify the NFA of a breach, similar to the regulator notifications required under the NY Regs.

US Treasury Department Critical Infrastructure Initiative. In July 2018, the US Department of the Treasury released a report "identifying improvements to the regulatory landscape that will better support nonbank financial institutions, embrace financial technology, and foster innovation." The Treasury Department used the report to announce that it will lead "a multiyear program with the financial services industry to identify, properly protect, and remediate vulnerabilities" with respect to critical infrastructure. We expect further details on this critical infrastructure initiative to be released in 2019.

PUBLIC COMPANY DISCLOSURES

In February 2018, the SEC highlighted cybersecurity concerns for public companies by formalizing guidance that reiterates that companies should consider the materiality of cybersecurity risks and incidents when preparing required disclosures. In addition, the revised guidance addresses the importance of policies and procedures related to cybersecurity by encouraging companies "to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure." Going forward, public companies across industries are likely to continue to face challenging questions regarding potential disclosure obligations under this guidance. Moreover, because cybersecurity risks and incidents may qualify as material nonpublic information, companies will want to pay attention to the SEC's guidance on evaluating and monitoring trading activities to avoid potential insider trading exposure. In several high-profile data breaches, senior company officials have faced intense scrutiny for trading activity that appeared to be based on insider information, and the SEC appears poised to continue this trend in 2019.

MEDICAL DEVICES

The US Food and Drug Administration ("FDA") continues to prioritize cybersecurity of medical devices and made significant headway on promised cybersecurity activities in 2018. We expect that trend to continue into 2019 as FDA continues to push these initiatives into action. Although FDA typically does not update guidance on a periodic basis, in October 2018, FDA issued draft guidance that, once final, will supersede the October 2014 final guidance on the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Public meetings to solicit comments on the draft guidance are scheduled for January 2019, and FDA will likely move quickly on finalizing the guidance after the comment period closes in March. Most notably, the new draft guidance focuses on how manufacturers can address the risks to patient safety created by connected devices. FDA also made efforts to facilitate increased information sharing across the federal government in the coming years by signing a Memorandum of Understanding with the Department of Homeland Security to further increase cooperation between the agencies, and by creating two new Information Sharing and Analysis Organizations. Finally, in 2019, health care delivery organizations have a new tool to respond to cybersecurity incidents in the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook, sponsored by FDA.

CONNECTED VEHICLES

The Department of Transportation ("DOT") and the National Highway Traffic Safety Administration ("NHTSA") have prioritized cybersecurity in recent years, including through ongoing engagement with industry stakeholders and the issuance of *Cybersecurity Best Practices for Modern Vehicles* in October 2016. In the past year, DOT continued to highlight cybersecurity and data privacy as key topics for companies to address as they build automated driving systems. Its guidance document, *Preparing for the Future of Transportation: Automated Vehicles 3.0* ("AV 3.0"), issued in October 2018, built upon DOT's last major statement addressing automated vehicles: *Automated Driving Systems 2.0: A Vision for Safety* ("A Vision for Safety"), released in September 2017. A Vision for Safety identified twelve "priority safety design elements" that manufacturers were encouraged to consider in designing highly automated vehicles, including vehicle cybersecurity. AV 3.0 reaffirms this focus on cybersecurity and specifically supported the "Voluntary Safety Self-Assessment" approach announced in the 2017 policy. The new guidance noted that public-private coordination and information sharing are essential to managing cybersecurity risk and highlighted the value of engaging with the Department of Homeland Security and other public-private information sharing organizations. The continued emphasis on cybersecurity was also reflected in a September 2018 speech by the Deputy Administrator of NHTSA, who stated that "collective safety risk management through information sharing is vital" and highlighted the importance of maintaining consumer trust that the automotive industry "is committed to working together to anticipate and mitigate cyber risks." Automotive industry participants will therefore want to continue focusing on cybersecurity and data privacy as they design, build and support increasingly connected vehicles in 2019.

CONSUMER DATA SECURITY AND PRIVACY

Enforcement activity by the Federal Trade Commission ("FTC") has been a constant feature of the consumer data security and privacy landscape over the past decade—with the commission bringing more than 60 actions alleging that companies engaged in unfair or deceptive practices that failed to adequately protect consumers' personal data. The FTC can be expected to remain focused on data security and privacy in 2019. In December 2018, the FTC held a two-day public hearing devoted to data security, at which the Director of the Bureau of Consumer Protection stated that "data security will continue to be an important priority for the FTC and that the FTC will not be retreating from its role as the nation's primary data security law enforcement agency." The FTC plans to schedule a similar public hearing on consumer privacy—"the first comprehensive re-examination of the FTC's approach to consumer privacy since 2012."

Enforcement actions are likely to remain a key tool for the FTC in 2019 as it sets consumer data security and privacy policy, including for connected devices. Many such enforcement actions may end in consent orders, but litigation also may continue to test the FTC's authority and the theories it pursues in enforcement actions. In June 2018, the US Court of Appeals for the Eleventh Circuit vacated the FTC's cease-and-desist order against LabMD, concluding that it imposed an "indeterminable standard of reasonableness" and was not specific enough in what it prohibited and what it required. 2019 may see additional challenges to the FTC's authority to bring—and ability to win—such actions, including in the FTC's litigation against a router manufacturer over allegations of inadequate security that is scheduled for trial in June.

Expanding Cybersecurity and Data Privacy Litigation

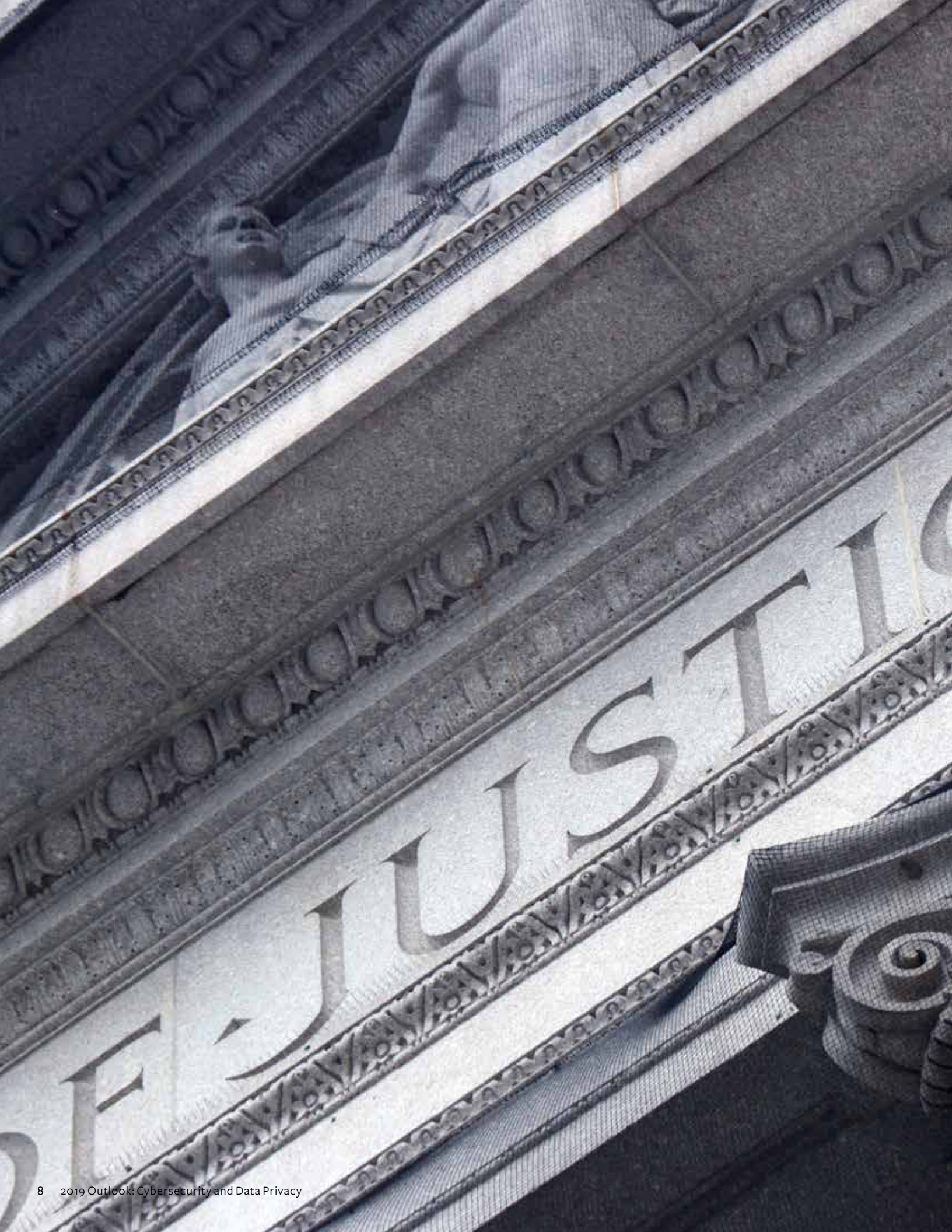
Cybersecurity and data privacy litigation continues to grow, both in the potential liability exposure it presents to companies and the types of litigation and theories advanced by plaintiffs. Countless putative privacy and cybersecurity class actions were filed in 2018, asserting claims based on federal privacy statutes, state biometrics laws and common law theories, among many other bases. Lawsuits also addressed the security and privacy implications of connected products, artificial intelligence, and other evolving technologies, and continued to expand beyond consumer class actions. Meanwhile, courts continued to wrestle with high-stakes issues for privacy and security litigation, including the proper application of the Supreme Court's decision in *Spokeo, Inc. v. Robins* in this context (a question that the Supreme Court itself recently raised in a pending case) and the risk of future injury sufficient for standing in data breach cases.

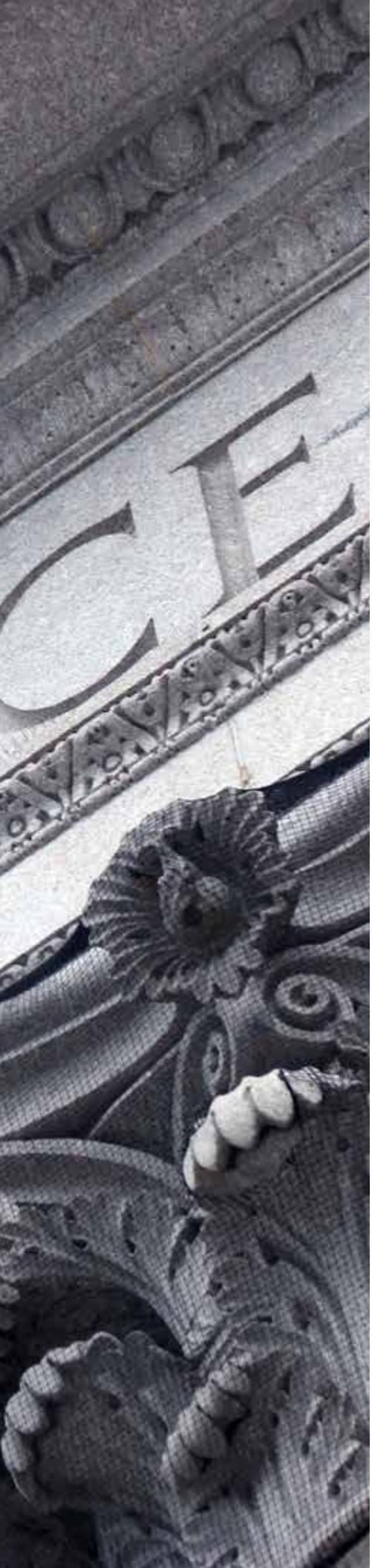
Cybersecurity and data privacy litigation is poised to expand once more in 2019 as more disruptive technologies are adopted across the economy and expectations for cybersecurity and data privacy continue to evolve.

The creation of a limited private right of action under the California Consumer Privacy Act, which we discuss in more detail below, likewise suggests that this litigation will only grow over time. Companies consequently should expect litigation risk to be a key factor in determining their respective approaches to cybersecurity and data privacy in 2019 and beyond.

DATA BREACH CLASS ACTIONS

Data breach class actions remain a persistent risk for companies that hold US customers' personally identifiable information. Although litigation does not necessarily follow after every data breach, many putative class complaints continue to be filed shortly after data breaches hit the news. Following a major data breach, dozens of consumer class actions may be filed, further raising the stakes of litigation. Moreover, with close attention paid by the press and security researchers to companies' responses to incidents and plaintiffs' attorneys watching for potential missteps or failures to remediate compromised systems, litigation risks can arise well after the original compromise. Companies should therefore continue to have the management of litigation risk front of mind in responding to consumer data breaches in 2019.





It remains to be seen whether 2019 will be the year that the Supreme Court clarifies what precise risk of future harm is necessary to establish Article III standing in data breach class actions. The US Circuit Courts of Appeals are currently split on this important question, with the Third Circuit, Sixth Circuit, Seventh Circuit and DC Circuit having found the alleged risk of future harm after a data breach sufficient to establish standing, and the First Circuit, Second Circuit, Fourth Circuit and Eighth Circuit having reached contrary conclusions. This past year, the Ninth Circuit joined the former group of Courts of Appeals in its *Zappos.com* decision. Relying on its prior decision in *Krottner v. Starbucks Corp.* (the precedential value of which had been questioned after the Supreme Court's decision in *Clapper v. Amnesty International USA*), the Ninth Circuit concluded that the plaintiffs' allegations of an increased risk of identity theft were sufficient to establish Article III standing. The Zappos.com petition for certiorari is pending before the Supreme Court as of the date of this publication.

INTERNET OF THINGS LITIGATION

Connected devices continue to become more deeply integrated into our daily lives and our economy. Connected cars, medical devices, toys, home appliances, consumer electronics, and more are bringing new services and capabilities to consumers. Connectivity likewise is being brought to commercial, manufacturing, agricultural, and critical infrastructure applications, from farming equipment to the factory floor and beyond. This connectivity creates exciting opportunities for companies and offers great benefits to the customers they serve.

However, these opportunities also bring new litigation risk. As anticipated, litigation relating to connected devices—often referred to as the "Internet of Things"—continued to grow in 2018. Consumers alleged that certain devices lacked adequate security and, thus, were overpriced or exposed them to a risk of future harm from cyber attacks. Other putative class actions alleged that connected devices collected or used personal data improperly, thus violating consumers' privacy rights. Ongoing litigation over automotive researchers' 2015 discovery of alleged security vulnerabilities in a connected vehicle reveals the high stakes of such litigation. In an ultimately unsuccessful petition for certiorari after class certification in that case, the defendants explained the massive potential liability at stake, describing the case as involving "three statewide classes containing more than 220,000 consumers claiming $440 million in damages." Such figures, even if only claimed at this stage, highlight the high stakes of cybersecurity and data privacy litigation regarding the Internet of Things. Indeed, this risk will only increase in the event of future cybersecurity attacks on connected devices that result in personal injury or other physical consequences.

SHAREHOLDER AND DERIVATIVE CYBER LITIGATION

Consumer class actions following cyber incidents have increasingly been accompanied by securities class actions or derivative litigation. In September 2018, for example, Yahoo! entered into an $80 million settlement of claims that the company misled investors about large-scale data breaches it suffered. Litigation also continued in 2018 in the securities class action that was filed against Equifax after it suffered high-profile data breaches. Derivative actions have also continued. Final approval was given to a $29 million settlement of the Yahoo!

data breach derivative litigation in January 2019, for example. Likewise, the fast-food company, Wendy's, settled a data breach derivative action in May 2018, with an award of almost $1 million in attorneys' fees and an agreement to take various remedial measures. Considered in combination with the reporting disclosure guidance issued by the SEC and increasing regulatory pressure on boards to perform effective cybersecurity oversight, these securities class actions and derivative actions further highlight the importance of cybersecurity and data privacy for a company's most senior leadership in 2019.

Increasing Adoption of Comprehensive Data Privacy Regimes

The implementation of the GDPR drove substantial compliance work for many companies in the past few years.

2019 is likely to see both continued focus on the GDPR as well as similar attention paid to a wave of new, GDPR-like laws that continue to complicate the data privacy landscape.

Several jurisdictions, including countries such as Brazil and states such as California, have already followed suit and passed or proposed legislation inspired by the GDPR. Managing and responding to these emerging regimes will be a key focus of private sector data privacy work in 2019.

GDPR. The GDPR came into effect in May 2018 and continues to demand significant focus by companies seeking to remain in compliance with its obligations. This regulation represented a sea change in the way privacy is regulated for individuals in the EU. Some of the key changes include:

- Direct applicability of the GDPR in the same form in all EU Member States (with some powers of derogation granted at the national level in specific areas, such as employment law);
- Expanded extraterritorial scope that captures non-EU businesses;
- Significantly higher fines of up to the higher of 4% of an enterprise's worldwide turnover or €20 million per infringement;
- New data breach notification obligations that require notice to the relevant EU supervisory authority without undue delay and where feasible within 72 hours after becoming aware of a data breach;
- New data privacy governance requirements, including the appointment of a data protection officer and the use of data protection impact assessments for higher risk processing;
- Requirement to implement "privacy by design";
- Expanded individual privacy rights, including the "right to be forgotten", the "right to data portability" and the right not to be subjected to automated data profiling; and
- New direct obligations for both data controllers and data processors.

Member State supervisory authorities have already brought a number of enforcement actions since the GDPR went into effect. The UK's Information Commissioner's Office ("ICO"), for example, brought an enforcement action against a Canadian company for violating Articles 5, 6 and 14 of the GDPR, which also concurrently demonstrates the GDPR's extraterritorial reach. Moreover, high-profile GDPR actions and, in some cases, significant financial penalties, have been levied against other major companies, some of which are based outside of Europe. In addition, supervisory authorities have reported that the number of complaints filed by data subjects and the number of notifications of personal data breaches have increased substantially, in some cases increasing by as much as 10 times that of pre-GDPR times. Accordingly, the number of enforcement actions is likely to increase substantially in 2019.

We also expect to see more and expanded guidance from regulatory bodies on GDPR compliance issues in 2019. Various supervisory authorities, including the European Data Protection Board ("EDPB"), have already released guidance on the GDPR. These guidance documents build upon that which has already been released by the Article 29 Working Party. Notably, the EDPB has released guidelines on the territorial scope of the GDPR and on the derogations of Article 49.

CCPA. If 2018 saw the final push to prepare for GDPR compliance, then 2019 will likely see a similar effort by relevant companies to develop compliance mechanisms for the new California Consumer Privacy Act ("CCPA"). Set to take effect in 2020, (with the law becoming operative on January 1, 2020 and

enforcement actions delayed until July 1, 2020), this law is the most sweeping general privacy statute in the United States. It protects an expansive set of consumer information and applies to companies across economic sectors. The law also constitutes a departure from prior US privacy regulation in its provision of new protections and rights to consumers with regard to their personal information. In some respects, the CCPA bears resemblance to the GDPR, and, accordingly, a company may be able to leverage capabilities developed in response to the GDPR in its CCPA compliance efforts, particularly regarding disclosure requirements and subject access rights. However, these legal frameworks are not identical, and in 2019 companies will need to determine what new or modified mechanisms CCPA will require. Further complicating this task, many expect the CCPA to be amended before it takes effect in 2020, although the nature of any such amendments remains unclear, and several significant provisions of the CCPA are subject to implementing regulations to be issued by the California Attorney General on an uncertain timeline. Only the Attorney General can enforce the CCPA, with one notable exception: the CCPA grants consumers a private right of action for the unlawful exfiltration or disclosure of limited categories of personal information.

Brazilian General Data Protection Law. Another law inspired by the GDPR is Brazil's new General Data Protection Law (Lei Geral de Proteção de Dados, or "LGPD"). The LGPD was signed into law in August 2018 and amended in December 2018 by an executive order. Among the changes made by the executive order are that the LGPD will become effective in August 2020, six months after the initially scheduled date of February 2020. The LGPD is very similar to the GDPR, such as in terms of material scope, definitions, principles, security requirements and data breach notification requirements. The law also has extraterritorial applicability, similar to the GDPR. There are, however, some differences. For example, the LGPD contains some additional, more specific bases for processing that are not covered by the GDPR, such as for the protection of health in a procedure carried out by health professionals and the protection of credit. The potential fines are also lower than those under the GDPR—violations can result in fines of up to the higher of 2% of the company's gross revenue in Brazil the previous year or R$50 million. Still, companies subject to the LGPD will likely undertake substantial compliance work in 2019.

Other Jurisdictions. Other jurisdictions also are considering data protection laws that are similar to the GDPR. In the United States, for example, legislators in certain other states, such as New Mexico, have proposed laws similar to the CCPA. In addition, other countries, such as India, are considering laws inspired by the GDPR. Discussion and debate around the prospect of expanded and new legal regimes for data privacy with global applicability and consequences will likely be prominent in 2019.

Focus on Data Privacy and Cybersecurity Policy

Policymakers at the state and federal level are poised to focus intensely on data privacy and cybersecurity issues in 2019. Debates over data privacy are likely to consider the respective roles of state and federal governments in regulating this important issue. Cybersecurity policy, meanwhile, is likely to have a particular focus on addressing and responding to threats posed by foreign actors. Policy decisions in both areas are likely to have significant consequences for the private sector, so businesses may benefit substantially from monitoring and engaging in these important policy debates.

DATA PRIVACY

The respective roles of state and federal governments in data privacy policy will be a key issue in 2019.

As discussed above, the California Consumer Privacy Act creates new rights for consumers regarding the transparency, collection, usage, sharing, deletion and sale of personal information. Lawmakers in other states already are pursuing similar legislation, dramatically increasing the chances that companies doing business in the United States will soon have to manage a patchwork of comprehensive privacy regimes across individual states.

Many corporations and industry associations will likely mobilize to push for a single federal data breach notification standard as part of such a law, as reflected in a number of recent private sector recommendations on the topic. Businesses will benefit from monitoring developments in this space as proposed legislation could have significant financial and operational consequences. For example, one

bill proposed at the end of 2018 would have imposed duties of care, loyalty and confidentiality on online service providers that are engaged in interstate commerce over the Internet and collect identifying data about end users. While the timeframe for passing privacy legislation into law may stretch into the coming years and success is never certain, stakeholder commitment to the effort is real, and we expect that it will take up a good deal of legislators' attention in the coming year.

Congress also is likely to focus oversight activities on data privacy in 2019. Data privacy was covered in a number of prominent oversight hearings in 2018 that largely reacted to high-profile events and centered mostly on social media companies. Congressional oversight is expected to increase significantly in 2019, especially with Democratic leadership of the House of Representatives. For example, the incoming leadership of the House Energy and Commerce Committee has indicated that privacy oversight will be high on its agenda in 2019. We expect that this oversight will relate to companies' use of consumer information and on the choices and knowledge consumers have about the use of their data. We also anticipate that oversight hearings will focus on the issues receiving the most public attention, which include data breaches, the security of user data and the use of sensitive personal information (such as biometric and geolocation data).

The Trump administration also is likely to focus on data privacy policy in 2019. In November 2018, the National Telecommunications and Information Administration received public comments from over 200 organizations as it sought to develop the administration's approach to consumer privacy. In addition, the National Institute of Standards and Technology has begun its own process to develop a privacy framework based on its highly successful cybersecurity framework. Both of these processes should be active throughout 2019.

Finally, even as companies carefully track data privacy developments in the United States at the state and federal level, the issue continues to take on global salience as well. In June, the G20 summit meeting in Japan will focus on global data governance. Speaking at the World Economic Forum in January, Japanese Prime Minister Shinzo Abe argued for updating World Trade Organization rules to account for and facilitate the free and secure flow of data globally. His comments were echoed by other world leaders. Although these were initial discussions, and no single proposal or policy solution has appeared to gain prominence, multinational businesses would do well to follow the evolution of global perspectives on these topics and weigh opportunities to engage in the ongoing debate.

CYBERSECURITY

The challenges posed by cybercrime and cyber-espionage are likely be central to US cybersecurity policy in 2019, both domestically and in its foreign relations. Private sector entities may have opportunities to work with the federal government in addressing such pressing issues, and potentially stand to benefit from monitoring evolving developments in this area.

Trade Secret Theft. Companies should expect the current Administration to remain focused on the threat to American economic prosperity and national security posed by economic espionage in 2019. In 2015, China and the United States publicly committed to not engage in the cyber-enabled theft of intellectual property for commercial gain. Recent statements from senior administration officials and high-profile indictments brought by the Department of Justice indicate the view of some leading government officials that China has failed to adhere to that commitment. For example, the Department of Justice indicted two Chinese nationals associated with the Chinese Ministry of State Security of numerous hacking offensives associated with a global campaign to steal sensitive business information. Congress is also likely to consider legislative responses to trade secret theft and economic espionage. These actions suggest that 2019 is likely to see further disputes with China over cyber theft of trade secrets. Companies—especially those in industries that have previously been targeted by espionage campaigns—are likely to benefit from tracking developments in this space.

DHS Reorganization. On November 16, 2018, President Trump signed the Cybersecurity and Infrastructure Security Agency Act of 2018, thereby effectuating a significant reorganization of cybersecurity capabilities at DHS. This legislation established the Cybersecurity and Infrastructure Security Agency ("CISA") as the entity within DHS that is "responsible for protecting the Nation's critical infrastructure from

physical and cyber threats." In this role, CISA manages significant public-private cybersecurity engagement and information sharing, including through the National Cybersecurity and Communications Integration Center. 2019 will likely see opportunities for companies to continue building relationships with DHS on cybersecurity issues, including through initiatives championed under its new organization.

White House Cyber Strategy. The Trump administration released its first expansive National Cyber Strategy in September 2018. Building on the Administration's first executive order addressing cybersecurity, this document identified key goals and related actions to "ensure the American people continue to reap the benefits of a secure cyberspace that reflects our principles, protects our security, and promotes our prosperity." Many of the priority actions identified in this strategy have the potential to impact private sector entities and could be pursued by the government in 2019. For example, the strategy prioritizes "risk-reduction activities across seven key areas: national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation." Companies in these industries can expect increased cybersecurity engagement from government actors. Notably, the strategy eschewed a regulatory approach and, instead, called for "promot[ing] open, industry-driven standards . . . and risk-based approaches to address cybersecurity challenges." Companies and trade associations thus stand to benefit from remaining focused on government activity related to the National Cyber Strategy. However, there are potential risks associated with some of the administration's cybersecurity policies, including with respect to offensive cyber operations. In conjunction with the release of this national strategic position, the Administration altered the rules governing such military operations and authorized certain unspecified additional cyber activities against America's adversaries. Some commentators have raised concerns that such activities could lead to retaliation by foreign nation-states. The private sector will want to watch these developments carefully, especially as 85% of the nation's critical infrastructure—a primary target for cyber attack by malicious actors—is owned and operated by private entities.

EU Cyber Strategy. 2018 ended with a political agreement reached by EU institutions on the Cybersecurity Act (the "Act"). The Act paves the way for EU cybersecurity certification schemes for ICT products (i.e., hardware and software elements of network and information systems); services (i.e., services involved in transmitting, storing, retrieving, or processing information via network and information systems); and processes (i.e., sets of activities performed to design, develop, deliver and maintain ICT products and services). Another EU legislation that will have an impact on many companies' activities in 2019 is the Directive on Security of Network and Information Systems (the "NIS Directive"). The NIS Directive imposes specific security and notification requirements on operators of essential services (in sectors such as health, transport, financial market infrastructure and banking, water supply and distribution) and for digital services providers. Many national laws implementing the NIS Directive will enter into force in the coming year. Hence, affected companies will benefit from following these cybersecurity developments both at the EU and national levels.

Conclusion

Cybersecurity and data privacy are likely to stand among the most significant issues that multinational businesses must address in 2019. Cyber incidents continue to become more complex and severe, requiring companies to continue to refine their response capabilities, and legal frameworks, regulatory expectations, litigation risk, and policymaking continue to evolve, constantly adding complexity for companies. Businesses will benefit from continuing to refine their cyber risk management and data privacy compliance programs to address these evolving challenges in the coming year.

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, whether in Europe, Hong Kong, Brazil, or elsewhere around the globe. 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.

PUBLICATIONS:

2018 Cybersecurity and Data Privacy: Navigating a Constantly Changing Landscape

Cybersecurity and Data Privacy: Navigating a Constantly Changing Landscape highlights developments and priorities for businesses on a range of key topics, from the compliance challenges posed by new regimes such as the EU General Data Protection Regulation and the New York's financial services regulations, to growing expectations for due diligence in mergers and acquisitions, to evolving threats that demand thorough response playbooks.

To request a copy of this guide, please visit:
mayerbrown.com/Cybersecurity-and-Data-Privacy-Navigating-a-Constantly-Changing-Landscape-09-27-2018/

2017 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

2016 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

2015 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

CONTRIBUTORS

For more information about the topics raised in this 2019 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

Samantha C. Booth
+1 312 701 8327
sbooth@mayerbrown.com

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

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

Diletta De Cicco
+32 2 551 5945
ddecicco@mayerbrown.com

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

Charles-Albert Helleputte
+32 2 551 5982
chelleputte@mayerbrown.com

Sasha Keck
+1 202 263 3464
skeck@mayerbrown.com

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

Zaneta Kim
+1 650 331 2072
zkim@mayerbrown.com

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

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

Cristiane Manzueto
+55 21 2127 4235
cmanzueto@mayerbrown.com

Ian McDonald
+44 20 3130 3856
imcdonald@mayerbrown.com

Christopher M. Mikson
+1 202 263 3157
cmikson@mayerbrown.com

John Nadolenco
+1 213 229 5173
jnadolenco@mayerbrown.com

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

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

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

Benjamin Shoemaker
+1 202 263 3463
bshoemaker@mayerbrown.com

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

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

Emily K. Strunk
+1 202 263 3404
estrunk@mayerbrown.com

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

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

Jonathan Weinberg
+1 202 263 3442
jweinberg@mayerbrown.com

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

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

Lisa V. Zivkovic
+1 212 506 2482
lzivkovic@mayerbrown.com

Mayer Brown is a distinctively global law firm, uniquely positioned to advise the world's leading companies and financial institutions on their most complex deals and disputes. With extensive reach across four continents, we are the only integrated law firm in the world with approximately 200 lawyers in each of the world's three largest financial centers—New York, London and Hong Kong—the backbone of the global economy. We have deep experience in high-stakes litigation and complex transactions across industry sectors, including our signature strength, the global financial services industry. Our diverse teams of lawyers are recognized by our clients as strategic partners with deep commercial instincts and a commitment to creatively anticipating their needs and delivering excellence in everything we do. Our "one-firm" culture—seamless and integrated across all practices and regions—ensures that our clients receive the best of our knowledge and experience.

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

Americas | Asia | Europe | Middle East | www.mayerbrown.com

MAYER · BROWN