Data privacy and cybersecurity laws have been rapidly developing in the United States this year, especially in California, New York, Nevada and Massachusetts. While there are ongoing efforts to pass a federal privacy law, these states are continuing to lead the way.

In the wake of Europe’s General Data Protection Regulation (GDPR), US legislators and regulators have passed—or are looking to pass—privacy standards with enhanced disclosure and rights obligations, as well as stepped-up cybersecurity requirements and breach reporting timelines. The definition of personal information also continues to expand beyond traditional US notions of personally identifiable information.

Many of these laws have extraterritorial reach, and compliance with one set of rules is no guarantee of compliance with another. Businesses that have a nexus to the US, or that collect and use personal information that can be associated to US residents, should consider paying particular attention to the applicability of US data privacy and cybersecurity laws to their business practices.

Federal regulators like the SEC and FTC are also continuing to emphasize the importance of privacy and cybersecurity through new regulations and enforcement actions, particularly when it comes to senior officer accountability, written cybersecurity plans and vendor due diligence.

**State legislative developments this year (2019)**

**California**

The California Consumer Privacy Act of 2018 (CCPA) goes into effect on January 1, 2020—and it applies well beyond California’s borders.

While the law shares many features with Europe’s GDPR, including enhanced disclosure obligations and enhanced individual rights, there are significant differences. California also armed its new law with the prospect of steep fines for noncompliance and a private right of action. Companies doing business with California residents, even those located outside California, will want to start planning to comply with the impending law, even if they are already compliant with other US privacy laws and the GDPR.

Those businesses that are already GDPR compliant have a leg up on CCPA compliance, but important differences between the GDPR and the CCPA exist that companies may need to accommodate. For example, to comply with the CCPA, businesses have to disclose their verification procedures in their privacy policies and have to implement two-step procedures prior to deleting a consumer’s information.

This year the California legislature substantially amended the CCPA, and the California Attorney General (AG) published its draft implementing regulations. Although the CCPA now contains new exemptions, as well as one-year deferrals for employees and contractors, these exemptions and deferrals are more limited than many people think.

On January 1, 2020, consumers can start making requests under the CCPA and plaintiffs can start bringing lawsuits under the CCPA’s private right of action for any data breaches.

For more on the CCPA, please visit our CCPA hub at [www.californiaconsumerprivacy.com](http://www.californiaconsumerprivacy.com). Our CCPA hub contains a series of articles, including one detailing the draft regulations and the recent amendments, as well as our series of webcasts on the CCPA.

**New York**

In July 2019, New York’s Governor signed the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) into law to enhance breach notification requirements and to require businesses to adopt reasonable safeguards to protect New York residents’ personal information (effective from March 1, 2020). The SHIELD Act applies to companies that hold private information of New York residents, whether or not those companies do business in New York.

The SHIELD Act, like the CCPA, expands the definition of personal information. For New York, personal information now includes biometric information; account, credit or debit card numbers, if circumstances exist where such numbers could be used to access an individual’s financial account; a user name or e-mail address, in combination with information that would permit access to the account and any unsecured protected health information as defined under the Health Insurance Portability and Accountability Act (HIPAA). The SHIELD Act also obliges businesses to put in place a reasonable data security program, including allocating responsibility to a designated employee.
to oversee cybersecurity operations, appropriately vetting third-party providers and providing training to employees on data security issues.

Regarding data security protections, the SHIELD Act requires one or more employees to coordinate the company’s security program that, among other things, must 1) identify reasonably foreseeable internal and external risks; 2) assess the sufficiency of safeguards in place to control the identified risks, and 3) adjust the security program in light of business changes or circumstances.

The SHIELD Act is in addition to the New York State Department of Financial Services’ (DFS) groundbreaking Cybersecurity Regulation, which took effect in March 2017. The Cybersecurity Regulation requires insurance companies, insurance agents and brokers, banks and other financial services providers regulated by the DFS, regardless of whether they are domiciled in New York, to conduct risk assessments of their Information Technology (IT) systems and maintain a cybersecurity program based on that assessment. It also imposes a number of standards and requirements for governance and operation of the IT systems.

**Alabama and Mississippi**

Alabama and Mississippi recently joined Michigan, Ohio and South Carolina as the most recent states to adopt the NAIC Data Security Model Law (Model 668). Model 668 is based on DFS’ Cybersecurity Regulation and it creates requirements for both data breach notification and written information security plans. Model 668 also creates special requirements relating to third-party service providers.

Alabama’s law adopting Model 668 was passed on May 1, 2019 and will partially go into effect a year later on May 1, 2020 (the third-party service provider requirements will go into effect in 2021). It has a wide reach, as it applies to any person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association or other business entity that acquires or uses sensitive personally identifying information of Alabama residents and third party recipients. Mississippi’s law adopting Model 668 was passed on April 3, 2019 and went into effect on July 1, 2019. It applies to any person who conducts business in Mississippi and who, in the ordinary course of the person’s business functions, owns, licenses or maintains personal information of any Mississippi resident.

**Washington**

On May 7, 2019, Washington passed new legislation updating its existing cybersecurity law to expand the definition of personal information and reduce the breach notification requirement from 45 days to 30 days. The law continues to apply to any person conducting business in Washington who owns or licenses computerized data that includes personal information (but does not apply to information subject to HIPAA, the Health Information Technology for Economic and Clinical Health Act, or the Gramm-Leach-Bliley Act).

Washington’s new requirements become effective on March 1, 2020.

**Nevada**

As of October 1, 2019, Nevada requires certain businesses operating in Nevada to provide consumers with the right to opt-out of the sale of data. Unlike the CCPA (which applies to both online and offline business operations), the Nevada law only applies to operators of Internet websites and online services. Operators that collect and maintain personal information from consumers that reside in Nevada, and engage in activity that creates a nexus with Nevada, must have measures in place to ensure that any covered information that has been collected or will be collected is not sold if an individual exercises his or her opt-out right.

**Massachusetts**

On April 11, 2019, Massachusetts’ new breach notification law went into effect. The law requires businesses that suffer data breaches involving social security numbers to provide, free of charge, credit monitoring services for a minimum of 18 months to affected consumers. If the business that is breached is a credit monitoring agency itself, this requirement is extended to 42 months. In addition, the law requires post-breach notifications filed with the Massachusetts Attorney General to provide information about the company’s security program and identify its parent and affiliated companies.

Massachusetts’ new law applies to any person that owns, licenses, maintains or stores data that includes personal information about a Massachusetts resident.

**Maine**

On June 6, 2019, Maine passed legislation to prevent broadband Internet service providers (ISPs) from using, disclosing, selling or permitting access to consumer personal information without consumer consent. The law requires broadband Internet service providers to provide a clear and conspicuous notice of the provider’s obligations and the consumer’s rights. The law also requires broadband providers to take reasonable steps to protect customer personal information that takes into account the nature and scope of the provider’s activities, among other factors.

Any ISPs providing services in Maine should ensure that procedures are in place to obtain express and affirmative customer consent to use, disclose, sell or access customer personal information and provide a means for the customer to revoke such consent at any time.

**Texas**

On June 14, 2019, the state of Texas passed a law creating an attorney general notification requirement if 250 Texans are affected by a data breach. The notification must include a detailed description of the breach; what information was compromised; how many residents were affected; measures taken to mitigate the breach; and whether law enforcement has been notified. The law also requires that individuals be notified within 60 days of having their personal information compromised. The new breach notification requirements go into effect on January 1, 2020.

On the data privacy side, the law creates a Texas Privacy Protection Advisory Council, whose purpose is to study data privacy laws and make recommendations to the legislature by September 1, 2020.

**Maryland**

On April 30, 2019, Maryland updated its existing data privacy legislation to expand the required actions a business must
take after becoming aware of a data security breach. The amendments, which took effect on October 1, 2019, include:

- An express authorization to use the information subject to the breach for providing notification to national information security organizations created for information sharing purposes, in addition to the existing purposes of notification and data protection; and
- A prohibition on a business maintaining or possessing computerized data from charging a fee for providing the owner or licensee of that data the information required to comply with notification requirements.

Federal efforts

Federal legislative efforts have so far not resulted in any comprehensive federal privacy law, which means that companies will be forced to continue to navigate a myriad of privacy laws at the state level (in addition to foreign privacy laws).

The US Congress saw over 20 bills establishing federal personal data protections introduced between January 2019 and November 2019, none of which have been adopted. Most recently, on November 18, 2019, Bill S.2889 — the National Security and Personal Data Protection Act of 2019 — was introduced in an effort to safeguard data of US citizens and residents from foreign governments that pose risks to national security by imposing data security requirements and strengthening review of foreign investments, and for other purposes. On November 5, 2019, Bill H.R. 4978 — the Online Privacy Act of 2019 — was introduced to provide for individual rights relating to privacy of personal information, establish privacy and security requirements for covered entities relating to personal information, and to establish an agency to be known as the United States Digital Privacy Agency to enforce such rights and requirements, and for other purposes. It remains to be seen whether either of these latest bills will gain traction.

Given the complexities of the issues surrounding data privacy and the wider ramifications on national commerce and international affairs, the prospects of a passage of comprehensive federal privacy legislation in the foreseeable future remain low. Nevertheless, there has been a spate of federal enforcement actions this year against companies for data privacy violations, demonstrating that regulators will not be shy to disrupt business practices and will likely continue to rely heavily on monetary penalties to disincentivize privacy violations. Many of these enforcement actions have been brought by the Federal Trade Commission (FTC), under its authority to stop companies from engaging in unreasonable data security practices, or from making misleading statements or omissions about data security. The enforcement actions placed particular emphasis on senior officer accountability, written cybersecurity plans and vendor due diligence.

Conclusion

Data privacy and cybersecurity remains top of mind for legislators and enforcement agencies in the US—as it must for businesses and senior executives, even those headquartered abroad.

Ultimately, businesses need to review existing privacy policies to ensure that data is adequately protected and consumers are afforded the rights provided by the new state laws and regulations. In addition, businesses must properly represent their data practices in a transparent manner and hold senior officials accountable for data handling practices.

Businesses should keep a close eye on the developing US laws and regulations covering data privacy and security, particularly as those laws continue to evolve rapidly at the state level.

For more information, please contact:

Michael Bahar  
Partner, Washington DC  
T: +1 202 383 0882  
michaelbahar@eversheds-sutherland.com

Sarah Paul  
Partner, New York  
T: +1 212 301 6587  
sarahpaul@eversheds-sutherland.com

Paula Barrett  
Partner, United Kingdom  
T: +44 207 919 4634  
paulabarrett@eversheds-sutherland.com

Mary Jane Wilson-Bilik  
Partner, Washington DC  
T: +1 202 383 0660  
mjwilson-bilik@eversheds-sutherland.com

Arkansas

On April 5, 2019, Arkansas updated its data privacy laws to join a growing number of states to:

- Include “biometric data” under the definition of “personal information”;
- Keep a record of any determination of the likelihood of harm following a data breach; and
- Notify the attorney general within 45 days after a determination has been made that there is a reasonable likelihood of harm following a breach of the security system affecting more than 1,000 individuals.