SheppardMullin

Navigating U.S. Data Privacy: A Guide for French Companies

Based on Presentation for the French American Chamber of Commerce
SF-LA | November 5, 2025

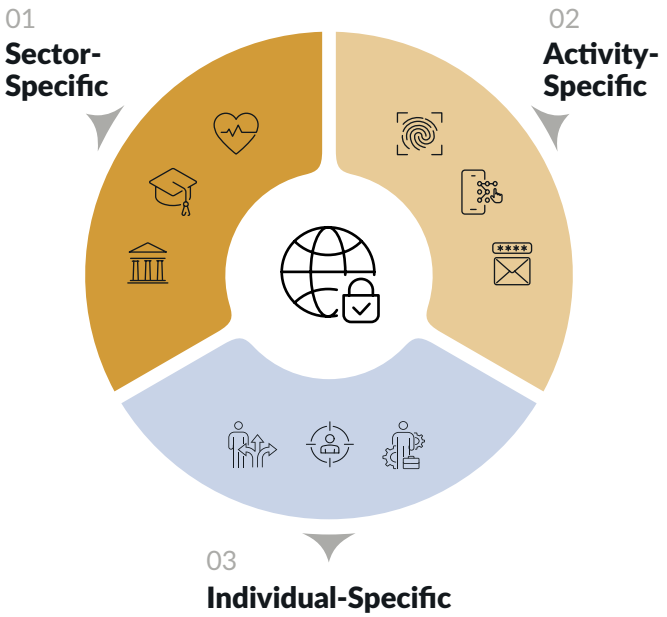
For French companies that do business in the United States, understanding the complex privacy and cybersecurity environment is key to managing risk. This is even more important as we face rapid changes and developments under the new federal administration.

Unlike a single privacy law approach found in European countries, the U.S. takes a sectoral and activity specific approach, with narrow laws found at the federal, state, and even local level. This creates a unique landscape that requires careful attention.

It is important to keep in mind the current legal landscape, as well as risks to specific industries and to specific activities. Fortunately, there are several practical steps you can take to manage those risks.

The U.S. Data Privacy Law Patchwork

For companies familiar with Europe's legal landscape, the American approach to data privacy can be surprising. The United States does not have a single, comprehensive federal law for data privacy. Instead, it takes a "patchwork" approach. Both where you find the laws – at the federal, state, and even local levels – and the type of laws that exist. Substantively, U.S. privacy laws fall into three categories.



In the first category are privacy laws directed to specific sectors. For example, health care, financial services, or education. The laws in these areas include the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach-Bliley Act, and more. In the second category are privacy laws that govern when entities engage in a specific activity. These include laws that govern sending text messages (Telephone Consumer Protection Act), collecting biometric information (Illinois's Biometric Information Privacy Act), or protecting -or failing to protect- personal information (data security and data breach notification laws). The final and third category are privacy laws that are designed to protect specific types of individuals, like children (Children's Online Privacy Protection Act) or employees. While the resulting obligations are like those in "one law" systems, in the U.S., the requirements are spread across hundreds of different laws.

While there is a growing number of states in the United States with "comprehensive" privacy laws modeled off of non-U.S. laws like the General Data Protection Regulation (GDPR), they are not as comprehensive as one might think. They by necessity coexist with the existing patchwork of laws, and as such do not cover things like data breach notification, sending digital marketing communications, and more. French companies should keep this broad patchwork in mind. While the requirements in the U.S. under this patchwork may be similar to those that exist under GDPR, they are spread across multiple different laws, at multiple levels.

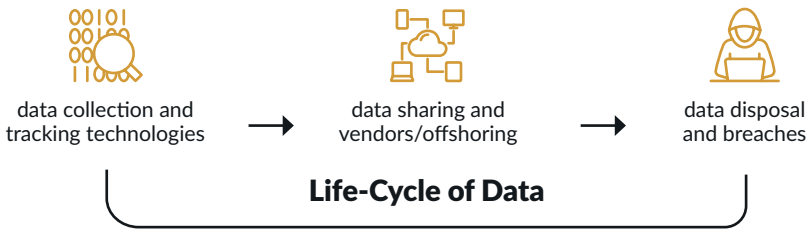
Sector-Specific Risks in the U.S. Market

There have been some specific areas of focus in the past several years for both federal and state regulators. These include kids' use of social media, as well as collection and use of healthcare data. Other areas of concern include digital tracking (cookies, tracking tools), as well as collection and use of biometric information.

Enforcement can come from federal or state regulators, as well as private litigation from plaintiffs claiming they have been harmed by companies' activities. In the healthcare space, while enforcement might occur, for example, under the federal law, HIPAA, there are also state-level laws, like Washington's My Health, My Data Act. In terms of private rights of action, there are privacy laws (primarily at a state level), that give individuals rights to sue. This includes the California Invasion of Privacy Act (CIPA), which has been used to bring web tracking suits.

The U.S. also has state-level unfair and deceptive trade practice laws that give individuals the ability to sue if they believe a company has engaged in a misrepresentation or has acted in a fundamentally unfair way. We see the former used for alleged privacy violations ("you said you would do X with my information, but you did Y"). And the latter, after data breaches ("it was fundamentally unfair not to better protect my information").

Companies that do business with the U.S. government also face a unique set of regulations. Different agencies have their own rules. The Department of Defense has a prominent certification program, but other agencies like the Department of Homeland Security have their own requirements. It is important to know which agency you are working with to understand the specific standards that apply. Your business may also be held to standards set by the National Institute of Standards and Technology, or NIST, which are seen as best practices in the industry.



Activity-Specific Risks to Your Business Operations

There are not only risks to entities in specific industries, certain activities in the US carry their own data privacy challenges. The way your company handles data, the partners you work with, and the technologies you use can all give rise to litigation or regulatory scrutiny. Managing these activity-specific risks is a key part of running a secure and successful business in the United States.

One area of focus for both regulators and class action attorneys has been use of tracking technologies on digital platforms. These tools run in the background of almost every digital platform, including websites and apps. They gather information about users, such as what page a person came from before visiting your site or where the user is located. They are, for example, what allows a website to remember what you left in your shopping cart and send you a reminder email. These tools implicate privacy laws insofar as the tracking tools gather and process personal information. Depending on the laws, there may be an obligation to provide users with notice and the ability to opt out (or opt in) to information being collected and used in this way.

Another risk area involves onboarding vendors who collect and/or process personal information on your behalf. Regulators have long taken the perspective that you could be held responsible for the data practices of your contractors and representatives. This concept is now being written into certain laws, including state "comprehensive" privacy laws. We are also seeing these concerns arise in the AI context. For example, a business uploading personal information into an AI model, which is used to train that model. There are expectations that the business will understand the extent to which the data is used for the vendors' purposes, or for those of third parties. Importantly, if this involves protected health information, there are patient consent issues to consider.

Finally, managing vendors who are located offshore presents another layer of risk. Some state laws prohibit sending certain types of health information outside the country. Even if a vendor is in the US, it is still critical to do your due diligence and ensure they can protect the data they handle for you.

Practical Strategies for Managing Risks

Now that we have examined the types of risk that can arise, what steps can companies take to navigate the ever-changing, risky, U.S. data privacy landscape? It is an understatement to say that it requires a proactive and adaptable approach. A flexible framework can help manage data privacy and cybersecurity risks while doing business in the United States. A flexible framework means going beyond reactive steps like insider threat training after a breach. Or, copying over standard –and not always feasible- recommendations from the literature ("put someone in charge of privacy" "conduct due diligence of every single vendor"). What does an adaptive program look like? What can companies do to go beyond the reactive and the routine? Here are five practical steps to consider.

First, take a principle-based approach to compliance. Instead of trying to memorize laws, categorize them into core principles. This will make it easier to slot in new obligations as the laws continue to change. Second, instead of guessing at your information collection and use practices, diversify the stakeholders who you involve in your diligence process. Similarly, when creating training programs, adapt them for the stakeholder group and focus training on key risks. Are you worried about malicious links, for example? If so, then use phishing email trainings. Third, remember the power of attorney-client privilege. When developing an approach, remember that the "draft" could end up being a smoking gun in potential litigation. Take steps to protect the work under doctrines of attorney client privilege (which often means more than just "copying the lawyer").

Fourth, borrow from organizational change research, and recognize the importance of psychological safety. When implementing compliance programs or adapting practices to address new laws, you are effectively implementing organizational change. When that happens, you want team members to feel safe identifying issues and mistakes. Relatedly, fifth, recognize the importance of small wins, and celebrate them. This step, too, comes from organizational change research. Change can be difficult, and recognizing your progress is an important step.

MANAGING PRIVACY RISKS

Five Practical Steps

Principles-Based Compliance
Instead of memorizing laws

Diversity Involved Stakeholders
Instead of guessing at information practices

Use the Power of Privilege
Instead of creating "smoking gun" assessments

Create Psychological Safety
Help team members raise issues

Celebrate Small Wins
Recognize your progress

Authors

Liisa Thomas
Privacy and Cybersecurity Team Leader and Office Managing Partner
+1.312.499.6335 | Chicago
+44.020.3178.7836 | London
lmthomas@sheppardmullin.com

Carolyn Metnick
Partner
+1.312.499.6315 | Chicago
cmetnick@sheppardmullin.com

Jonathan Meyer
National Security Team Leader and Partner
+1.202.747.1920 | Washington, DC
+1.212.653.8700 | New York
jmeyer@sheppardmullin.com