The privacy landscape for companies doing business in the US is rapidly changing. Alongside the California Privacy Rights Act (CPRA), which stipulates tighter data protection for millions of California residents by 2023, state-level privacy legislation is becoming a defined trend. States such as Nevada, Virginia, and Maine all recently passed comprehensive privacy laws. Other states, including Florida, Oklahoma, and Washington, are due to follow suit over the next year. As legislation advances, compliance with privacy legislation now needs to become a major corporate concern for every business.

Big tech is also formulating its response to how the future of consumer privacy might look. Facebook and Apple, two of the largest companies trading today, have differing opinions on how customers' privacy should be treated. As a result of the increasingly divergent approaches to privacy in both the private sector and state-level legislation, a uniform privacy landscape now looks unlikely to happen any time soon.

Fragmentation is nothing new. In the near to medium-term future, the prospect of an array of different privacy legislation presents a new set of challenges for compliance that will remind some of previous efforts. Anyone familiar with the history of data breach legislation in particular will recognize a familiar situation starting to take place. Even though states have been irregularly passing data breach notification legislation since 2002, efforts to create a unified federal law have repeatedly come up short. As a result, compliance requirements continue to vary from state to state.

However, while dealing with different compliance requirements around data breach notification is
inconvenient for businesses, the potential challenges created by a new wave of privacy legislation may be on another scale. Various state-level privacy laws, each with specific reporting and regulatory requirements, are an inherently daunting prospect for businesses.

Making sense of the privacy law mosaic
Although the prospect of a federal privacy law has been proposed as a solution, a nationwide privacy law may be more of a hindrance than a help for compliance officers.

Multiple proposals for a federal privacy law currently exist, and the timeline of any such law being enacted remains unclear. It is also important to note that one particular point of divergence among many proposals is whether such a law would supersede or sit alongside existing and future state-level legislation. This conjecture presents an increased likelihood that a federal law could complicate rather than simplify most businesses’ approaches to privacy.

While giving consumers the ability to opt out will undoubtedly be critical regardless of any federal privacy regulations, key details like which businesses will be affected are currently unknown. However, a common theme among all current and proposed state-level legislation is compelling organizations that leverage at least a certain amount of consumer information to provide their customers with the right to opt in or out of some level of data use. Laws such as the CPRA and the Virginia Consumer Data Protection Act (VCDPA) and upcoming bills such as the Washington Privacy Act share some stipulations that oblige businesses to give customers the ability to opt out.

Nevertheless, while they have much in common, these acts and others, such as Florida’s House Bill 863, differ considerably in areas such as defining what size businesses are affected and whether or not consumers have a private right of action. Looking at what happened to the preexisting California Consumer Privacy Act (CCPA), most acts are likely to change significantly before they become law.

Waiting is important, but being proactive is essential
So much is still unclear when it comes to how the privacy landscape is likely to change over the next several years. However, taking a reactive approach to privacy legislation is a poor strategy for any business to take. This is due both to the risks inherent in such an approach and the contrasting advantages that taking proactive action can give an organization. The problem with a reactive approach is highlighted by the vast majority of affected businesses remaining noncompliant with the CCPA in June 2020, six months after it came into effect.

Fortunately, thanks to the availability of the National Institute of Standards and Technology (NIST) Privacy Framework, a proactive approach to evolving privacy legislation is still possible. Using the evolving NIST privacy standards as a baseline for developing compliance efforts, businesses can effectively preempt present and future privacy legislation.

Ensure employee data protection and privacy
For any organization, a proactive approach to privacy should start with its own employees. Clearly defined under laws such as the CPRA and the General Data Protection Regulation, employee personal information security will soon be a legal responsibility for many businesses. As such, employee data protection is a critical first step in avoiding future fines for data exposure or misuse.

Additionally, as their own personal and professional activities leave a growing footprint of their personal information behind them online, employees are frequently the weakest link in any organization’s security posture. For threat actors whose aim is your customers’ data, overexposed employee information is a stepping-stone to a crippling data breach. According to research, most data breaches result from hackers using already accessible information to enter corporate networks.

As threat actors continue to leverage employee personal information, targeted phishing attacks remain a crucial driver of data breaches’ growing torrent. A core stipulation within every existing and proposed privacy law is placing legal responsibility on businesses to protect personal information from data exposure. While data breaches currently present a major reputational blow to any organization, tighter privacy laws could expose many organizations to significant fines. With legislation raising the stakes for data exposure and providing cybercriminals with additional leverage, employee personal information security is an important organizational asset.

Mitigating a vulnerable compliance risk factor
Protecting your organization from the risk posed by employee personal information means closing the privacy loop. One part of an effective approach to employee privacy is practical data governance and personal identity protection training.
Employees need to be empowered to see the real risks that easily accessible personal data presents to both themselves and their employers.

Another stalwart of employee privacy is giving individuals tools, such as privacy protection solutions, to protect themselves from the data brokers who find, collate, and sell their personal and professional information online. With most employees' professional email addresses easily found for sale online, investing in employee personal identity protection will pay dividends when it comes to increasing security.

Final thoughts
As the legal landscape surrounding privacy remains shrouded in uncertainty, organizations need to resist the urge to "wait and see" when it comes to compliance. Businesses can act now by accessing readily available frameworks alongside taking a proactive, employee-first approach to privacy.

By taking the opportunity to turn privacy into an organizational asset, proactive organizations can surf the changing wave of privacy rather than be swamped by it. As personal data becomes more valuable than oil in the world's commodity markets, your organization needs to recognize and protect employees' personal data as the valuable resources they are.

---

Endnotes

---

Takeaways
- State-level privacy legislation is a growing trend, and by 2023, tens of millions of Americans will be covered by comprehensive personal data protection.
- A side effect of different state-level legislation is an increasingly fragmented privacy landscape for businesses dealing with compliance issues within the United States.
- While a federal privacy law is anticipated, nuances in current proposals mean that such a law may further complicate the regulatory environment.
- In response to a compliance landscape that is likely to get more complicated, businesses need to be proactive when it comes to future compliance.
- Any proactive approach should start with employee privacy, a strategy that will also increase enterprise cybersecurity.