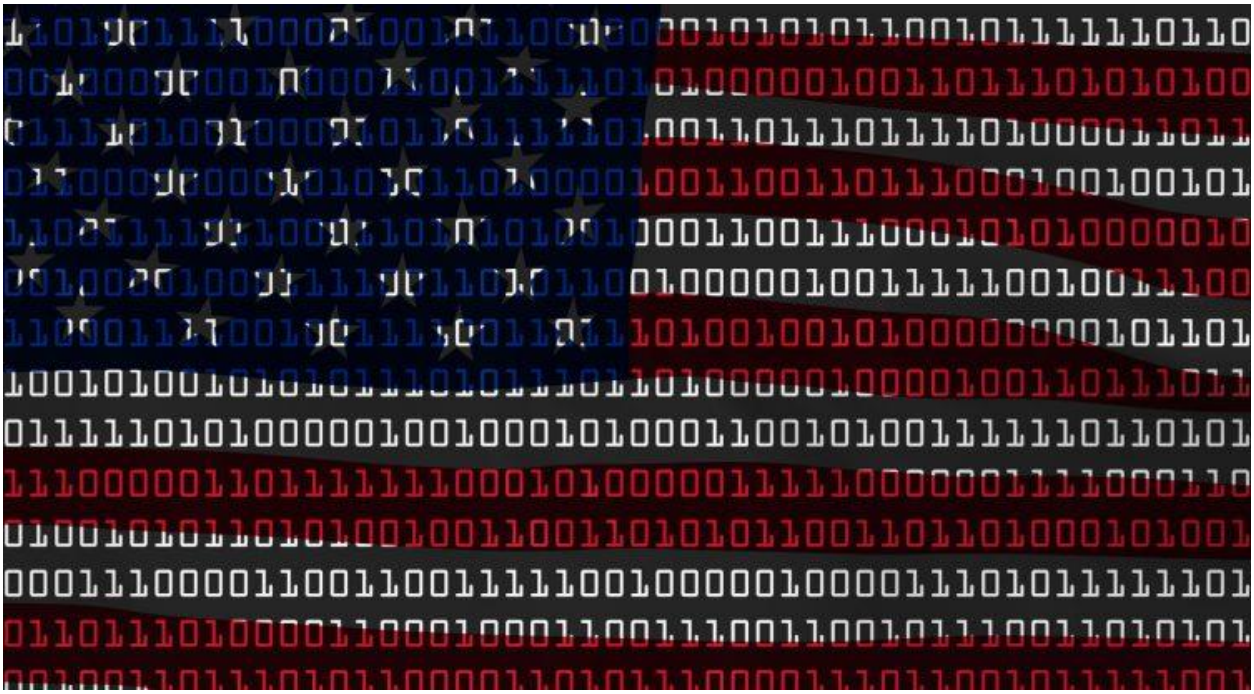
LAWYER MONTHLY

What's Next For US Data Privacy Legislation?

June 3, 2019

With the EU already beginning to look back on the implementation of GDPR, and looking ahead for new ways to protect data and privacy, legislation in the US still has a way to go.



But just how far behind is it? Here Lawyer Monthly speaks to Kon Leong, CEO of ZL Technologies, on the potential future of US data privacy legislation.

WILL THE CALIFORNIA CONSUMER PRIVACY ACT BE THE BETTER REGULATION TO INFLUENCE A FEDERAL US DATA PRIVACY LAW OVER GDPR?

It's difficult to foresee which of the privacy regulations will be most influential in the US at such an early stage. The US and global privacy landscapes are just now beginning to form and will undergo massive changes over the next decade. In addition to CCPA, various other states are creating their privacy regulations, creating a checkerboard of regulations that can be difficult for businesses to navigate. It's only a matter of time before we standardize privacy across the country to simplify it—although this will come with its own set of issues.

WHAT DO YOU THINK IS THE BEST FIRST STEP FOR DATA PRIVACY REGULATIONS IN THE US?

Creating legislation before understanding the technology required to fulfil it is putting the cart before the horse. Everyone is eager to discuss what privacy should be, but when it comes to the technology component of the conversation there is deafening silence. Very few understand what it takes to implement a system for privacy. Even the most remedial aspects such as finding and deleting someone's personal data become highly complex when you get to the enterprise level. The data management is not in place to support privacy and we're still quite a few years away. Lawmakers need to understand the technological challenges and then we might come back down to earth on what is currently possible.

WHAT SHOULD LAWMAKERS, BUSINESSES AND THE LARGER PUBLIC NEED TO CONSIDER IN THIS DATA PRIVACY DEBATE?

Hand in hand with the technology challenges of privacy are the *consequences* of true privacy. No one has really pieced out the implications of complying with this new wave of privacy regulation. Lawmakers, businesses, and the larger public need to consider what absolute privacy costs. When you see the process through to its logical conclusion there is a paradoxical truth: the most intrusive system is also the most private, and therefore absolute privacy entails absolute intrusion. Why? Because in order to protect personal information, an organization has to locate it, manage it and apply access privileges, which requires deep analysis and an iron grip on data. The CIA's surveillance is an example of a perfectly private and perfectly intrusive system. They have access to massive volumes of sensitive data, but within the CIA members can only see what they have access to. Complete understanding of their data, complete control.

WHAT HOLES AND GAPS HAVE ORGANIZATIONS OVERLOOKED, ESPECIALLY WHEN IT COMES TO IT BEST PRACTICES?

The world's IT architecture is largely silo-based. What this means is that data often lies in disparate repositories across an organization: for example, repositories for various data sources (email, file shares, SharePoint, structured data, etc.), and repositories for different governance functions (eDiscovery, records management, compliance, analytics). Issues arise when an organization must manage this data holistically, as data privacy regulations ask us to do. In essence, GDPR respects no silos. This will have to be reconciled in the coming years.

WHAT TYPES OF SOLUTIONS ARE AVAILABLE TO HELP BUSINESSES MEET DATA COMPLIANCE (GDPR AND REGULATORY) POLICIES?

While many compliance solutions exist, it's rare that they solve the underlying problem of holistic data management. Data management is fundamental to so many different functions, including privacy, yet very few solutions are able to do it well and to do it at scale. Consider the challenge of finding and deleting someone's data for a subject access request: the ability to search across all repositories to identify that subject's personal data and then determine whether it's eligible for deletion or if it's needed for other purposes such as legal, compliance, or records keeping. This requires repositories to be managed holistically and all governance functions to be running in complete synergy—these are core tenets of data management, but no one is talking about that. In the two decades I've been in this space, I've found that usually when everyone ignores a technology challenge it's because it's extremely difficult to solve. And that is just the type of challenge I've learned to embrace.