



June 21st

[David Weldon](#)

## **NY bill proposes sweeping changes on how consumer data is managed**

New York's State Senate is considering a bill that would impose sweeping new requirements for organizations that collect and process consumer data, including a fiduciary-like duty to protect such data.

To learn more about the proposed regulations, Information Management spoke with Kon Leong, chief executive officer at ZL Technologies on what we can expect.

***Information Management: Please give us an overview of the recent New York Privacy Act?***

Kon Leong: The New York Privacy Act is simply the latest flavor of the week in U.S. state privacy regulations, restricting how organizations can process personal data and putting in place processes by which data subjects may request access to, correction or deletion of their personal data.

While these new regulations are a good sign, privacy remains in its infancy the U.S., and this is most evident in how we approach privacy debates. Even though there is a lively conversation around the policies behind privacy, there is radio silence about the finer implications and technological requirements needed to meet these privacy regulations.

***IM: How does the New York Privacy Act differ from California's Consumer Privacy Act?***

Leong: The New York Privacy Act has many similarities to CCPA and other recent privacy regulations. At their core they intend to give control of data back to the consumer by giving them a voice in how their data is used.

However, while the language is similar, the devil is in the details. The New York Privacy Act for example allows for individual lawsuits between data subjects and the offending organization, rather than indirectly through an enforcement agency.

There are other important differences, for example how personal data is classified, and it's the differences rather than the similarities that carry steep implication for businesses. The differing policies creates a checkerboard of privacy regulations that organizations must navigate in order to operate across state lines.

Companies are now finding that in complying with these regulations, even the most basic functions become extraordinarily complex. For example, finding users' data across all the various silos across the enterprise has frustrated many companies under GDPR as the siloed state of today's IT architecture makes it extremely difficult.

Now envision a business that has to meet multiple privacy regulations from different states that all have unique privacy regulations. The reality is that data management in most organizations is simply years away from being able to handle all this data, particularly from different privacy policies across states.

***IM: Will the New York Privacy Act be the better regulation to influence a federal US data privacy law over GDPR? How will the New York Privacy Act impact organizations, both nationally and globally?***

Leong: As new regulations continue to appear, the federal government will at some point be compelled to pass a national regulation similar to GDPR. However, as organizations slowly update their technology to comply, a new host of consequences will arise.

The most important consequence will be the paradoxical truth that absolute privacy actually entails absolute intrusion. Consider this takeaway from [JD Supra](#) on the NYPA: "The bill, in its current form, will require businesses to track and correlate nearly every data point that can be mapped to a known consumer, including inferences drawn by the business based on those data points."

In essence, an iron grip over data is necessary to compliance. When technology does advance to the point where total information governance becomes possible, we should be extremely afraid. In short, the technology that would enable companies to have an iron grip over users' data would be easily exploitable under the wrong hands.

A thought experiment to illustrate this point: If we were to send the technology required to meet the regulations back to WW2 Germany, would there have ever been a resistance? Perfect surveillance, perfect intrusion, and perfect control over every single individual's data.

The only way to manage such technology is with diligent oversight. And when in our history has sustained oversight been successful?