REGULATION

What You Need to Know About California's New Data Privacy Law

by Dipayan Ghosh

July 11, 2018

pm images/Getty Images

Late last month, California passed a sweeping consumer privacy law that might force significant changes on companies that deal in personal data — and especially those operating in the digital space. The law's passage comes on the heels of a few days of intense negotiation among privacy advocates, technology startups, network providers, Silicon Valley internet companies, and others. Those discussions have resulted in what many are describing as a landmark policy constituting the most stringent data protection regime in the United States.

Much of the political impetus behind the law's passage came from some major privacy scandals that have come to light in recent months, including the Cambridge Analytica incident involving Facebook user data. This and other news drove public support for a privacy ballot initiative that would have instituted an even stricter data protection regime on companies that deal in consumer data if the state's residents voted to pass it in November. But after intense negotiation, especially from leading internet companies and internet service providers, the backers of the ballot initiative agreed to drop the initiative and instead support the passage of the law.

The new law — the California Consumer Privacy Act, A.B. 375 — affords California residents an array of new rights, starting with the right to be informed about what kinds of personal data companies have collected and why it was collected. Among other novel protections, the law stipulates that consumers have the right to request the deletion of personal information, opt out of the sale of personal information, and access the personal information in a "readily useable format" that enables its transfer to third parties without hindrance.

The law notably establishes a broad definition of "personal information," drawing in categories of data including a consumer's personal identifiers, geolocation, biometric data, internet browsing history, psychometric data, and inferences a company might make about the consumer. The protections over this data are to be enforced by the state's attorney general, though consumers will maintain a private right of action should companies fail to maintain reasonable security practices, resulting in unauthorized access to the personal data. (The data breach protection applies to a set of personal data that is narrower than that protected in the more general privacy protections.)

Perhaps the primary issue that firms are contending with is that the law's requirements could threaten established business models throughout the digital sector. For instance, companies that generate revenue from targeted advertising over internet platforms — such as Facebook, Twitter, and Google — must, as the law is currently written, allow California residents to delete their data or bring it with them to alternative service providers. This restriction could extend to internet service providers such as AT&T and Verizon, which collect broadband activity data (web browsing data) and could attempt to use it to generate behavioral profiles to enable digital advertising. These measures might significantly cut into the profits these firms currently enjoy, or force adjustments to

their revenue-growth strategies. They could also further impact any businesses that advertise on digital platforms, as the service they are purchasing — highly targeted advertising — might become less precise as a result of the new protections afforded to individual consumers.

Some firms stand to lose even more. Data brokers such as Acxiom, Epsilon, Experian, and Oracle, for example, generate profits by collecting quantities of data on individual consumers and selling it to third parties — be they ad networks, marketers, retailers, or any other type of interested business. These are precisely the kinds of practices that are directly threatened by the consumer's rights to deletion and to opt out of sale of data.

While the law, which is set to come into effect at the start of 2020, technically applies only to California residents, it will most likely have much broader implications. Most major companies that deal in consumer data, from retailers to cellular network providers to internet companies, have some Californian customers. That will leave those companies with two main options: either reform their global data protection and data rights infrastructures to comply with California's law, or institute a patchwork data regime in which Californians are treated one way and everyone else another. That last option can be more expensive for companies, and could disgruntle non-Californian customers should they be given fewer data privacy options by the service provider. Indeed, similar questions about Americans' data rights arose during Mark Zuckerberg's congressional testimony in regard to Facebook's compliance with new European regulations.

Critically, the legislature has left open the door to amendments to the new law. We can also expect the state attorney general to work with public stakeholders to develop more specific compliance guidance for the industry over the months ahead. In the time before the law is enforced, we are likely to see more debate among industry leaders, consumer advocates, and everyone in between — all of whom will wish to affect the law and its enforcement to their own benefit.

Dipayan Ghosh is a Fellow at New America and the Harvard Kennedy School. He was a technology and economic policy advisor in the Obama White House, and formerly served as an advisor on privacy and public policy issues at Facebook. Follow him on Twitter @ghoshd7.

This article is about REGULATION

⊕ Follow This Topic

Related Topics:

Technology | Security & Privacy | Technology | Advertising, Marketing & Public Relations