ARTICLES

Rising Tide of Privacy Regulation

By Rob Rosenzweig

Oct 29, 2018

Call it the GDPR effect.

Since May, when the European Union's General Data Protection Regulation (GDPR) – the most sweeping legislation in history for data privacy protection – went into effect, there's been a growing trend in the United States to shore up laws protecting consumer privacy rights. As an early adopter of everything from supermarket sushi to electric cars, it's no surprise that California is the first state to pass laws modeled after the EU's stringent privacy law. In the months since GDPR, California has passed two significant pieces of legislation:

- California Consumer Privacy Act of 2018 (CCPA)
- IoT Cybersecurity Improvement Act of 2017

Of the two laws, CCPA has the greatest potential impact on businesses. Structured in much the same way as GDPR, CCPA places restrictions on how companies collect, store and distribute data, and how they notify individuals of breaches. And much like GDPR, the stick is bigger than the carrot. There are significant penalties for non-compliance.

Briefly, the main tenets of CCPA include:

- *Right to Opt Out*. Consumers have the right to opt out of the sale of their personal information and businesses must publish their privacy policies on their home page.
- *Right to Access*. The law defines "personal information" and gives consumers the right to request which personal information a business has collected.
- *Right to Delete*. Consumers have the right to request the deletion of their personal information.
- *Right to Opt In*. For children under 16-years-old, businesses must have opt-in consent to sell their personal information. For children under 13-years-old, that opt-in consent must come from a parent or guardian.
- *Penalties for Non-Compliance*. Fines up to $750 per incident can be imposed; a data breach involving 10,000 customers could equate to a $7.5 million fine. Additionally, civil penalties can be up to $7,500 per intentional violation.

What does CCPA mean for you?

The world is increasingly smaller with the onset of a digital economy. A lot of businesses that thought they

wouldn't be regulated by GDPR are going to be impacted by CCPA. Similar to GDPR, which extends to any organization doing business with EU citizens, even if it's located outside of EU borders, CCPA applies to any businesses **operating** in California.

And although it's not as expansive as GDPR (for example, GDPR requires companies to appoint a Data Protection Officer in some cases), CCPA may have more impact in the U.S. because, for the first time, smaller businesses are now facing increased data privacy regulatory scrutiny.

Leading up to GDPR and during the implementation to become compliant, there was a general sense that regulators would only go after the Facebooks of the world, to make an example out of big data players. But with CCPA, it's more likely that small and mid-sized organizations will be impacted.

How the new regulation will really impact the data privacy and security ecosystem is yet to be determined. It will all come down to what kind of teeth CCPA will have when the law goes into effect in January 2020.

Regardless, it is clear that a more stringent data privacy regulatory landscape is here to stay. CCPA is the most restrictive non-industry specific regulatory framework in the U.S., but it won't be the last. California is traditionally first to adopt progressive legislation, but states like New York and Massachusetts are sure to follow suit.

Even if your company doesn't currently have transactions in California or with EU citizens, now is the time to start looking at your data privacy policies more closely. To get in touch with one of our cyber liability specialists, contact rrosenzweig@risk-strategies.com.

TAGS:
Cyber Liability