Media coverage

Learning from Europe but looking beyond for privacy law

By Jules Polonetsky, Opinion Contributor — 10/16/18 06:35 PM EDT
The views expressed by contributors are their own and not the view of The Hill

© Getty Images

Not a day seems to pass without reports of a new data breach or privacy miss-step by a company. It's no surprise that the White House, Congress, industry and civil society are increasingly in agreement about the need for comprehensive federal privacy legislation.

What should such a privacy law look like? This week the Senate Commerce Committee held a hearing seeking lessons from the recently adopted European General Data Protection Law, a detailed framework governing every aspect of collection and use of personal data. There is value in looking to the basic principles of the GDPR, but there are also areas where the GDPR principles can be refined to most effectively support the rights and freedoms U.S. legislators want to protect.

In a world of international data flows, national and global interoperability is critical. The GDPR seeks to have one set of privacy rules that are interpreted in a uniform way throughout the continent, as European Data Protection Board Chair Andrea Jelinek explained in her Senate testimony. Federal legislation that took some important lessons from GDPR would be a step towards trans-Atlantic interoperability.

The GDPR is technology neutral and covers every type of company and business model. At a time when data is collected across platforms—on the web, on mobile, with wearables, smart home devices, and phone and facial tracking — emulating the GDPR's comprehensive model with a law that sets one clear set of rules will be easier to enforce and easiest for consumers to understand.

Another central pillar of the GDPR is fairness, which means using data only as people would reasonably expect and not using it in ways that have unjustified adverse effects, a concept very similar to the current Federal Trade Commission statute authorizing legal action against deceptive or unfair practices.

But there are many aspects of the GDPR that are less suitable for U.S. legislation. The GDPR is comprehensive, written to regulate not only business, but also governments, political campaigns and not for profits. The laws regulating government collection and use of data in the United States do indeed need to be updated, but it seems unlikely that policymakers are ready to address those issues in this bill. And given the concerns about the political collection and use of data by Cambridge Analytica, a hard look at political campaign data uses is warranted, but may face First Amendment protections in the U.S.

When it comes to children's privacy, the U.S. children's privacy law, COPPA, requires parental consent for all collection of children's personal data, with very limited exceptions. The GDPR sets an age of 16, higher than 13 under COPPA, but only for the cases where consent is required and only for providing "information society services." In many cases, the legitimate interest and opt-out model is permitted for collecting kids data in Europe. COPPA

almost always requires parental consent and covers all online services, often with strict verification requirements.

The GDPR also poses some challenges for AI and machine learning, since it specifies that personal data must be collected only for a specified purpose, must be deleted or minimized when not needed for that purpose. While there are promising efforts to minimize data collection for machine learning by conducting processes locally on user devices instead of sending data back to a company, for many such uses of data today, large and representative data sets are required to power new models, to ensure accuracy and to avoid bias. A U.S. framework would be wise to ensure that uses of data for machine learning are supported, when conducted responsibly.

U.S. law should also provide more flexibility for research than the GDPR, which mandates that researchers provide more specificity about their plans and in many cases requires continual permissions from individuals for future uses. Researchers often do not know what type of insights a study will reveal, and rely on data sets that have been collected by third parties from participants they cannot contact.

Any legislation should also consider the increasingly sophisticated privacy tools that are emerging, including differential privacy to measure privacy risk, homomorphic encryption that can enable privacy safe data analysis, and many new privacy compliance tools that are helping companies better manage data. A law that will stand the test of time and successfully protect privacy rights while enabling valuable uses of data should include mechanisms to incentivize such technology measures.

So let's look to lessons from GDPR for a federal bill, but also to the best ideas that privacy experts in civil society and in industry can offer to develop a framework that prevents harms while supporting responsible uses of data.

Jules Polonetsky