



URL : <https://www.itbusinessedge.com/articles/should-the-u.s.-have-a-federal-data-privacy-law.html>

Print Article

Should the U.S. Have a Federal Data Privacy Law?

If the entire European Union can come together to enact serious data privacy regulations for its citizens, why can't the United States Congress do the same? Right now, U.S. data privacy laws are scattershot among individual states, covering different things and, like the state-based data breach notification laws, only add more confusion. Having a national law would provide the same protections to everyone.

On the other hand, **GDPR has only been live for a few months, so we don't know what the long-term implications will be**. Or maybe we should wait to see how well the state privacy acts function before we take on a federal mandate.

I asked security and privacy professionals for their opinions: First, do we need a data privacy law at the federal level and second, if we do, what do you think should be in that law?

Almost everyone agreed that yes, a law passed by Congress is necessary.

"After numerous large-scale breaches and the well-publicized misuse of consumer data, we are well past the time for comprehensive data privacy protections for all U.S. citizens," Michael Magrath, director, Global Regulations & Standards, OneSpan, said, adding that the data privacy law should apply to online and offline data.

Callum Corr, data analytics specialist from ZL Technologies, agreed that we need to do this, but he's concerned about who would take the lead in writing that bill. "Big tech giants have been pushing politicians and commissioners alike to allow them to come together and write a policy that is going to be favorable to the largest companies in the industry," he said. In fact, a number of big tech firms **plan to introduce a data privacy framework** to the Senate.

"If we allow the tech leaders to write the law that is supposed to regulate them, then it defeats the purpose," Corr added. "The regulation needs to be consistent and therefore, it has to be federal." State laws are set up to fail because they all have boundaries attached, and the flow of data today has no boundaries. A federal law would address that.

There Is Something Started

There is one pending bill, S.2289, which was introduced to the Senate in January, Pravin Kothari, CEO of CipherCloud, pointed out. This bill calls for the creation of an Office of Cybersecurity within the Federal Trade Commission (OCS-FTC, which would create, issue, and distribute regulations that require covered business entities (predominantly credit bureaus) to provide a complete overview of the technical and organizational security measures they have in place.

But, while this is a start, we need to proceed with caution. "The legislative environment is uncoordinated and generally ineffective. Look at HIPAA and PCI, which have been in place for long periods of time, but have not stopped health care organizations or financial institutions from becoming victims - regardless of the requirements and penalties," said Kothari.

Empower Individuals and Their Right to Data Privacy

So we need the federal law, but what should it cover? The federal law should ideally empower individuals, said Rishi Bhargava, co-founder at Demisto. That includes following rights:

- The right to know what data is being collected by a data controller/processor
- The right to deny the collection of that data
- The right to ask for removal of that data at any time
- The right to be informed about any major breach that compromises their data

We Need Accountability

Despite the industry-based federal privacy laws enacted now, Ali Golshan, CTO and co-founder at StackRox, explained, we lack overall accountability for times when consumer data is lost or mishandled. However, he added, before we can have accountability, we need to figure out how to make the current compliances work with a broader privacy act. And any privacy law will need to include transparency of data management across organizations of all sizes.

Privacy Needs Protection

You can't think about data privacy without considering data protection. Any U.S. federal data privacy legislation should include a requirement, not a recommendation, that multifactor authentication must be used to access systems containing personal information, Magrath suggested, and should leverage the NIST's Digital Identity Guidelines v1.1 and future revisions.

Learn from GDPR

A lot of organizations have already taken steps to **be in compliance with GDPR**. Also, as states begin to enact their own laws, businesses will need to add more data privacy layers. We don't need to build a U.S. law from scratch, said Nathan Wenzler, chief security strategist at AsTech.

"We could start with GDPR as a framework, since it's already affecting U.S. companies who collect and use personal data for EU residents, and work to modify and improve upon it for our own purposes," Wenzler explained. "The intent of GDPR satisfies many pieces of a user-centric data privacy and protection effort."

GDPR is hardly perfect, of course, but a federal data privacy law similar to GDPR would provide users some amount of recourse to control how, where and in what manner their personal data is used, which in and of itself would be a huge step forward in our data privacy efforts.

Overall, what we want from a federal data privacy law is something that will help businesses keep consumer data secure and private as they work across state and international borders, TrustArc Chief Data Governance Officer Hilary Wandall said, adding, "A U.S. national standard that applies across industry sectors will provide a stronger position and voice for U.S. business and policy interests in the international privacy regulatory dialogue."

Sue Marquette Poremba has been writing about network security since 2008. In addition to her coverage of security issues for IT Business Edge, her security articles have been published at various sites such as Forbes, Midsize Insider and Tom's Guide. You can reach Sue via Twitter: [@sueporemba](https://twitter.com/sueporemba)

Print Article