# Cisco Calls for US Federal Privacy Legislation—Leveling the Privacy Playing Field

Mark Chandler, Executive Vice President, General Counsel
February 7, 2019

Irony alert: Even as every day we become more dependent on the internet and its wealth of information to simplify our lives, we ask ourselves more and more: can we trust the way our own personal information is handled?

Much of the current public debate about data privacy has been directed to the consumer market. But enterprise-facing companies who do not monetize customer data through advertising, like Cisco, must work to ensure that our customers – and our customers' customers – can trust the way data will be handled. This is especially crucial as more and more devices are connected to the Internet, and the peromise of the "Internet of Things" becomes real.

The legal environment governing use and access to personal information must provide protections and assurances to our customers. These legal protections will augment and reinforce steps we are taking internally to build and maintain trust, like development of our Customer Data Protection Program. The fact is, however, the current legal framework for data privacy in the US is not adequate. That's why Cisco's Chairman and CEO, Chuck Robbins has now issued a call for "comprehensive US federal data protection legislation anchored to core principles of transparency, fairness, and accountability because the right to privacy is a fundamental right."

Our goals for US legislation are three-fold:

- Ensure interoperability between different privacy protection regimes
- Avoid further fracturing of legal obligations for data privacy through a uniform federal law that aligns with the emerging global consensus
- Reassure customers that enforcement of privacy rights will be robust without costly and unnecessary litigation.

## Ensure interoperability between national and regional privacy protection regimes

The US has strong data privacy laws that impose strict industry-based requirements for handling, storage and use of specific categories of sensitive personal information by healthcare providers, financial institutions, and others. In addition to robust enforcement of those sectoral laws by regulators, the Federal Trade Commission also actively uses its authorities to challenge unfair and deceptive acts and practices impacting data privacy across the US economy. And yet, the absence of a general federal privacy law—covering data use, handling, and storage—is undoubtedly hurting the competitveness of US-based multinational companies doing business abroad.

For example, the US is considered to have adequate legal protections allowing American companies to handle EU personal data by virtue of an

agreement, called EU-US Privacy Shield. This agreement establishes a process whereby individual companies can adopt additional obligations equivalent to requirements under EU law. This arrangement combines company contractual promises with existing US legal protections to effectively ensure compliance with EU law. However, it is a solution that is needlessly complex—it requires repeated explanation to customers and it does not scale well globally.

The American system for data protection should be one that can easily interoperate with major regional and national data protection regimes, such as the EU, Japan, and Brazil without the need for separate agreements. While we need not adopt the GDPR in the US word for word., w e should shift toward a model that clearly communicates how data are protected and how those protections are enforced—without the need for individual organizations to subsequently adopt adjunct measures demonstrating their qualifications for handling personal data from outside the US. This should not be an overly complicated task given that the GDPR itself was built from a foundation of privacy principles that originate from those long documented in the US. To continue along the current path will only lead to unnecessary friction for US-based companies seeking to do business in the global market.

Avoid further fracturing of legal obligations for data privacy through a uniform federal law

California has now already passed a data privacy law slated to take effect in 2020. If the pattern that followed California's adoption of data breach notification legislation in 2002 holds true, we may see each of the 50 states pass their own versions of a data privacy law. Not only might the rules differ by state, but the enforcement mechanisms could also lead to confusion and unnecessary expense without any appreciable benefit to consumers.

There is significant risk that these various state laws may impose disparate or even conflicting requirements on companies doing business within the US. They would also make it harder for small companies to compete across state lines—much less in the global economy. Accordingly, we recommend that Congress occupy the field and preempt the possibility of inconsistent state requirements for data privacy.

Provide Robust Enforcement Mechanisms Without Unnecessary Litigation

Any federal privacy law must also include a robust enforcement mechanism. The Federal Trade Commission should be authorized to develop common-sense, flexible regulations informed by both a public consultation process and their own learnings from enforcement actions. Clarity around what the law requires will make both compliance and enforcement easier.

Becauase the FTC is a relatively small agency with limited resources, we believe State Attorneys General should be empowered to enforce the federal law—subject to the FTC having a right of first refusal. However, we believe that the duplicative litigation likely to result from extending a private right of

action would not be justified by any reasonably expected incremental benefits to privacy enforcement.

In the coming weeks and months, we plan to engage in the conversation around the development of federal privacy legislation in the US—and in similar conversations around national data privacy laws globally. We will point out what we think has worked well through the adoption of the GDPR, APEC Cross Border Privacy Rules, and other data protection regimes. We will also be candid about where changes are needed or more work needs to be done. Our goal is to help strike the right balance between free flows across national and regional boundaries necessary for innovation and the transparency, fairness, and accountability necessary for customers to feel confident in a digital society.

The world demands that data networks be built from the the ground up to meet users' data privacy expectations, and Cisco's own "Privacy by Design" principles are built to meet those expectations whether data are processed on business premises, in users' devices or in the cloud. To build trust and to be "trustworthy" in a world where we offer data-powered services is a different challenge than we've faced before. While many things about our business are changing along the way, we will never compromise the core values that have made and will keep Cisco the most trusted supplier of technology products and solutions. That is our North Star. The current lack of a US federal privacy law is making it harder for us to tell that story. That's why we believe the US needs to adopt smart, effective, robust privacy laws that will reassure customers that their data is protected in a globally connected world.