Mark Weatherford: The Future of Privacy in the U.S.

DAVID KIDD

Mark Weatherford has held executive-level cybersecurity positions in both the public and private sectors. He was first deputy undersecretary for cybersecurity at the U.S. Department of Homeland Security from 2011 to 2013. Prior to that, Weatherford was vice president and chief security officer for the North American Electric Reliability Corp., where he directed the organization's critical infrastructure and cybersecurity program for electric utilities across North America. He also served as chief information security officer for the states of California and Colorado. Perhaps most notably, Weatherford spearheaded some of the nation's first cybersecurity legislation aimed to protect citizens.

We recently spoke with Weatherford about the future of privacy legislation in the U.S. and the role emerging technologies might play in helping governments contend with growing privacy and regulatory complexity.

The European Union's GDPR and the California Consumer Privacy Act (CCPA) made big impacts in terms of privacy legislation, and several states currently have their own pending legislation. What do you see happening next? Is a federal law imminent?

The fact that it's on everyone's radar is a harbinger that other states will have some form of CCPA at some point. When we first started talking about GDPR, everyone poo-pooed it. Although there are parts of the law I don't agree with, GDPR made privacy better for the consumer. It raised the bar for how organizations use, collect, share and retain consumer information. The whole life cycle of data has become managed. A couple of years ago that wasn't the case. CCPA is the first step post-GDPR in the U.S. that's establishing the course for how we're going to protect consumer data.

I expect the federal government will take up a privacy law soon. There's so much personal information out there about every consumer now, and we have to protect it. And I think most security people would agree having a standard federal law or standard federal regulations would make protecting data much easier.

In the wake of this new and pending privacy legislation, how should state and local government leaders change their approach to data privacy?

First, it needs to be a priority. I think most legislators and most state leaders are aware of this issue, but prioritizing it in the stack of other things they're thinking about and worrying about is a challenge. Second, they need to prioritize it from the perspective of citizens. Despite the best intentions, most organizations are not going to spend money on security or privacy unless there's a compelling reason to do so. And that compelling reason is typically the threat of fines and legal damages.

What are some critical things state and local government leaders must understand about their data in order to protect it effectively?

Most organizations do not have a good handle on where their data is, who has access to it and how it's being moved around. Managing risk starts and ends with knowing what data you have and where it lives. Once you know that, you can start implementing controls to protect it. Creating policy is the next big step. Once you have policy in place, that will drive technology and architecture.

Can emerging technologies play a role in helping governments contend with growing privacy rules and regulatory complexity?

Yes, I'm working with several companies that are coming up with innovative ideas around this. One company has developed technology that can tell you where your sensitive data is exactly, which is not as simple as it sounds. There are also several companies that can tell you when people are doing unsafe things with your data, even people who have legitimate privileges and rights to access that data.

How do you see COVID-19 impacting privacy? Will the need for health surveillance blur privacy lines?

Like a lot of things in life, data can be used for good or evil. Our intentions are often good, but mistakes are made. Once we have data, it's difficult to ensure it's not going to end up in the hands of bad actors somewhere down the road. I completely understand the rationale for contact tracing around COVID, but we have to protect that data correctly. We need to proceed with caution.