SPONSORED CONTENT

Understanding the New Privacy Landscape

In May, Kansas Attorney General Derek Schmidt sent a letter to the governor and the state legislature urging them to create a new legal framework to guide the use of contact-tracing data intended to reduce the spread of COVID-19.

Schmidt said new software tools that use cellphone location data to alert individuals when they come in contact with someone who has tested positive for the coronavirus are "certain to present challenging legal issues not addressed by current Kansas law."

Schmidt isn't the only one raising concerns. The urgent public health requirement to track and limit exposure to the highly contagious virus has sparked growing worries that aggressive surveillance techniques threaten privacy protections for patient medical records.

"All of this is occurring without even a basic statutory architecture to guide development and deployment of the practice and management of the sensitive personal information collected," Schmidt wrote to Kansas Gov. Laura Kelly and legislative leaders.[1]

COVID-driven tensions turn up the heat on an issue that's been simmering for several years. Massive technology-enabled growth in the collection and monetization of personal data has sparked pushback in the form of legislation intended to give citizens more control over how organizations collect, use and protect information about them.

State lawmakers across the nation introduced hundreds of privacy bills just last year. One of the most prominent pieces of 2019 privacy legislation — the California Consumer Privacy Act (CCPA) — took effect in January, marking the first of potentially many state-level attempts to emulate the European Union's groundbreaking General Data Protection Regulation (GDPR), which gave EU residents more control over how organizations use their personal information.

New Privacy Expectations

All of this points to a sea change in how state and local government agencies must manage and protect data. The societal shift toward reasserting privacy as a fundamental right is driving heightened citizen expectations for government agencies to be responsible stewards of personal information. It's also reshaping the regulatory environment for public and private sector organizations.

"Government organizations are going to have to demonstrate the ability to discover and identify protected data — and map how that data is used," says Deb Snyder, former chief information security officer for New York State who is now a senior fellow with the Center for Digital Government (CDG). "Agencies need these capabilities to instill citizen confidence and demonstrate compliance with new regulations. It's essential for them to know what data they have, where it resides, who accesses it and what business processes it supports."

That's easier said than done. Governments have spent the past 30 years creating a patchwork of interconnected systems that share data to support transactions and business processes. Unfortunately, the touchpoints and data flows between these systems often are poorly mapped, making it difficult to understand how and where data is used. And demonstrating compliance with multiple regulatory requirements across this uncertain terrain is even harder still.

"It creates insane complexity," says Snyder. "You need the ability to map all of that and then apply a set of controls to it. You also need to demonstrate and confirm continuous compliance by monitoring those systems and policy settings in real time."

Results from CDG's annual Digital Cities and Digital Counties surveys indicate CIOs are feeling the impact of these data management issues. Data governance ranked among the top 10 technology priorities for city and county respondents in 2019.

In addition, chief privacy officers (CPOs) — charged with managing risk, creating privacy policies and ensuring compliance with multiplying privacy laws — are becoming more common in state and local governments. Thirty-six percent of cities and 45 percent of counties have at least one full-time position dedicated to enterprise privacy responsibilities, according to the 2019 surveys. And at least 13 states have created a CPO or similar position, according to a 2019 *Government Technology* report.

Smart Tools for Compliance

Fortunately, technology tools available to help governments address privacy challenges are growing smarter and more sophisticated. For instance, data discovery tools can help agencies understand where sensitive data is stored and how it is used by various systems. In addition, intelligent risk management solutions use artificial intelligence and machine learning to continuously monitor compliance with security and privacy requirements across complex IT environments.

Importantly, these and other data management technologies also can extend to data used by cloud service providers and third-party contractors.

"I think organizations are going to have to get serious about service providers and hold them to the same compliance requirements," says Snyder, "which can span from reviewing contracts and updating procurement procedures to automated reviews of systems that are beyond the immediate reach of the organization."

Ultimately, these tools help agencies get a better handle on what data is most critical to business processes and/or most sensitive from a regulatory perspective, so they can apply the right level of protection.

"If you don't know those basics, it's hard to properly focus your resources on bringing things into compliance or to a better state," she says. "You're just basically shooting in the dark."

Snyder adds that agencies should limit the amount of citizen data they gather and maintain. "Try to collect only as much data as you need to perform a specific function, and routinely purge data you no longer use," she says. "The more you keep, the greater your possible risk and exposure."

Get Started

As citizen expectations continue to rise and the regulatory landscape grows more complex, agencies must commit to strengthening their privacy programs. Classifying data, mapping information flows, and implementing smart compliance and risk management tools will all be part of this effort.

"The message really is just get started," says Snyder. "Being able to protect privacy and prove compliance isn't optional."

GROWING ATTENTION ON PRIVACY

45% of counties have a full-time position dedicated to enterprise privacy responsibilities.

36% of cities have a full-time position dedicated to enterprise privacy responsibilities.

13 states have appointed a chief privacy officer or similar position.

Data governance ranked **#6** in the top 10 technology priorities for city and county CIOs.

SOURCE: 2019 DIGITAL CITIES AND COUNTIES SURVEYS AND GOVTECH.COM

[1] https://www.govtech.com/policy/Kansas-AG-Calls-for-Contact-Tracing-Limits-Privacy-Protections.html