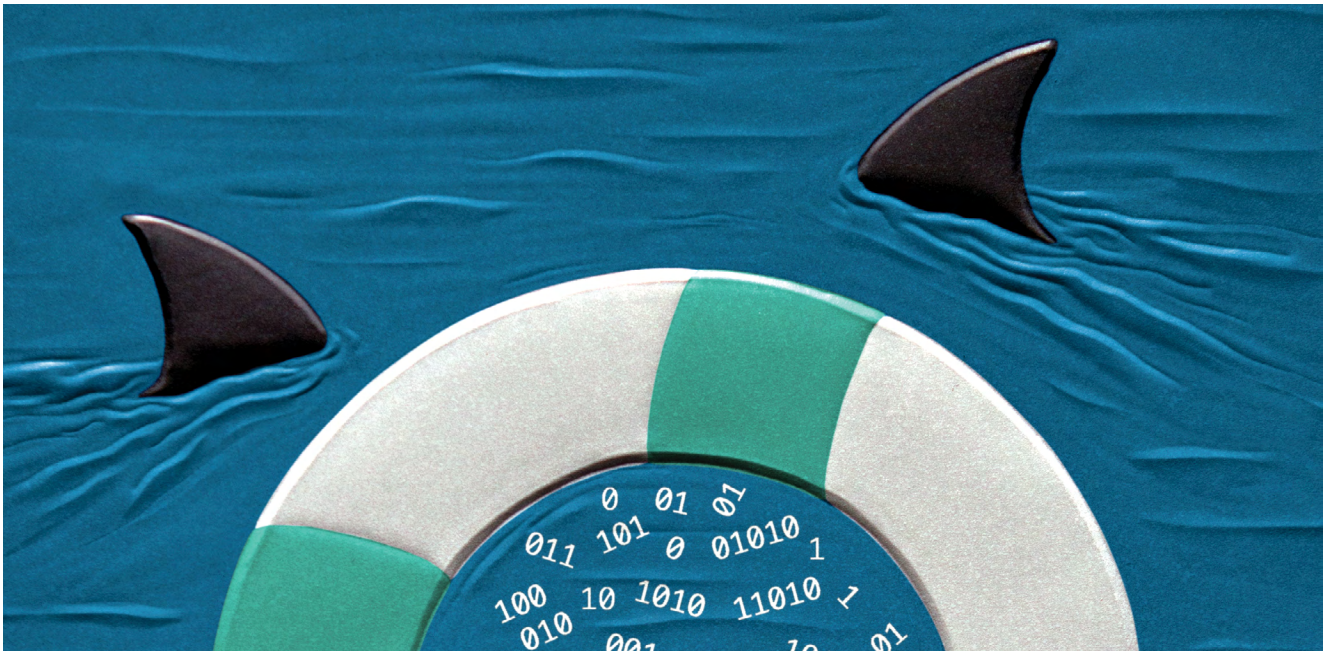

PERSPECTIVE

The Brave New Frontier of Public Sector Privacy

BY KATHERINE BARRETT AND RICHARD GREENE

Cybersecurity efforts have been the main way state and local governments have tried to secure data from the prying eyes of potential malefactors. But breaches are inevitable—the bad guys frequently seem to be at least a little step ahead of the good guys in that domain. As a result, privacy is the key for entities that are interested in taking a prophylactic approach toward securing confidential records.

It's no surprise then that a recent study by the National Association of State Chief Information Officers (NASCIO) reported that: "In the last decade there has been immense growth in the state chief privacy officer (CPO) role. As demand increases for online services and states capture more personally identifiable information from citizens, more states are emphasizing the importance of privacy."

The speed with which that title is gaining currency, at least at the state level, is impressive, with 21 states reporting that they had a chief privacy officer role in May 2022, up from 12 in 2019, according to NASCIO.

At the local level, the chief privacy officer position is somewhat less widespread, but that doesn't mean cities and counties aren't carefully focusing on privacy issues as well—often through staffers within their chief information officer's shop. "I think the issue of privacy has burst onto the scene nationally," said Katy Ruckle, chief privacy officer for the State of Washington.

With faith in government at a historic low, there's probably been no better time to reassure people that governments are being careful with the reams of data they collect from them. "Privacy can help build better trust with the public," said Daren Arnold, chief privacy officer for the State of Ohio. "I think people have this feeling that they have to turn over information to whatever government agency requests it, but they have no say as to how it's going to be used. But if there are proper rules around that information and if it's used for the purpose for which it's provided, that will build trust."

Naturally, finance offices need to be abundantly careful about maintaining privacy of the data they receive directly through one means or another, from tax returns to bids for procurements to internal records

of the finance offices themselves, such as the social security numbers of employees.

And that's just the beginning. Because finance offices are often sharing data with other agencies, they carry the heavy burden of helping to ensure that information isn't revealed to prying eyes. "They need to have safeguards, to make sure that information isn't leaked out," explained Amy Glasscock, program director for innovation and emerging issues for NASCIO.

"Finance professionals are handling large amounts of financial information for individuals," Ruckle said, "and I've seen cases where large spreadsheets full of private information have been generated and sent to the wrong email address, with the potential that it will go out to large numbers of people."

Ginger Armbruster has been chief privacy officer for the City of Seattle, Washington, since 2017. Her job is particularly complicated because Seattle, like other cities, operates under the strictures of the state's open information laws. That means that if a city agency gathers information of any kind, it doesn't require a hacker to get to it—it's open to the eyes of anyone who requests it. "I have to make nearly anything that the city creates available to the public."

Armbruster provided a particularly powerful example. The Department of Transportation in Seattle wanted to make it easier and safer for children to walk to school—an estimable goal. As part of that effort, it issued a survey that included questions like, "How do you walk to school?" "What's your gender?" "How old are you?" "At what time do you travel?"

"So, we worked with the department of transportation, which was very open to our counsel, and said, you don't need to know the exact route any individual child travels or exactly when they're taking that walk. That's way too intrusive," Armbruster said. "They hadn't thought about how that information could be used in bad ways. They were just trying to protect the kids, not put them at risk.'"

Privacy shops need to concern themselves with two primary questions: Do we really need the data in the first place? and Who should have access to the data that's being collected?

Privacy shops need to concern themselves with two primary questions. The first is, "Do we really need the data in the first place?" With the capacity of technology to store endless troves of data, there's a distinct tendency toward getting every bit of information available from anyone interacting with a state or local government. But if personal identification data isn't necessary for the purpose for which it's being collected, then gathering it in the first place isn't wise.

Arnold provided another example. "In the finance space, you don't need people to put their social security numbers on their invoices. There's rarely a reason to put that on there."

The second big question is who should have access to the data that's being collected. Fewer eyes on privileged data mean it's less likely to leak out. As a result, states and local governments that are concerned with privacy are careful to make certain that data is shared only on a need-to-know basis. "Because privacy is a relatively new area of focus, people don't necessarily realize they shouldn't provide that broad access to data," said Cherie Givens, chief privacy officer for the State of North Carolina.

Efforts to maintain privacy have gotten trickier than ever because the pandemic led to many public-sector employees working from their homes. North Carolina state employees receive guidance on how to protect state data when working remotely, Givens said. "Personal information or personally identifiable information held by the state needs to be protected from unauthorized access by others, including people in your home. Your spouse or your children are not authorized to see state-held personally identifiable information."

What are the risks if someone's teenage child gets a glimpse of a spreadsheet? The answer becomes clear if you think like a chief privacy officer. "Think about the selfie generation," Givens said. "Someone could take a picture with a laptop in the background and post it on social media." If the laptop hasn't been locked, then the information on the screen could be seen by potential identity thieves or others who view this kind of social media post as if it were a pile of gold dumped in their lap.

Although privacy is clearly an important goal for a growing number of state and local governments, like other government efforts, one major challenge to progress is the lack of money necessary to do the work.

Consider the City of Oakland, California. The city's Privacy Advisory Commission has taken important steps to protect its citizens from the abuse of data gathered through technology like automatic license plate readers.

But Joe DeVries, deputy city administrator and chief privacy officer, said he'd like cities like Oakland do more, and he explains why that hasn't come to pass yet. "Like many cities, we're under-resourced. We struggle with huge swaths of poverty, and we have a large vulnerable population with a lot of needs. What I've observed in my work on privacy is that it's hard for people who are housing the insecure or victims of violent crime to think of privacy as a hot topic."

Katherine Barrett *and* ***Richard Greene*** *are principals of Barrett and Greene, Inc (greenebarrett.com). and are co-authors of the recently released* Making Government Work: The Promises and Pitfalls of Performance-Informed Management.