NASCIO

Perspectives on Privacy

A Survey and Snapshot of the Growing State Chief Privacy Officer Role

Perspectives on Privacy:

A Survey and Snapshot of the Growing State Chief Privacy Officer Role

Compared to a private company or even any other level of government, the need to focus on privacy at the state level is significant. The amount of personal information citizens provide to their state outweighs anything a citizen provides to any one company. States create people's identities with birth certificates and end legal identities with death certificates. They create drivers' licenses and hold personal information related to health, education, criminal records, victim records, financial information, and family status. While states have always held this kind of information, the explosion of electronic personally identifiable information in the last several years has meant that organizations and governments have had to hire staff to deal with the privacy implications.

In addition, states must operate under the umbrella of federal privacy regulations. While officials in one agency may understand compliance around the Health Insurance Portability and Accountability Act (HIPAA), officials in another agency may be dealing with compliance related to the Family Educational Rights and Privacy Act (FERPA). The policy environment around privacy in state governments is complex, especially in a decentralized information sharing environment. An enterprise-level privacy official can help bridge the gaps and provide guidance.

While the general population has been aware of security issues over the last 20 years due to increasing private use of technology, more citizens are becoming aware of and concerned about their privacy rights being infringed upon. Incidents in the news like Facebook sharing user data with Cambridge Analytica continue to cause concern. This concern from citizens along with the increase of electronic information, and an increasingly complex regulatory and information-sharing environment, has meant that state governments are reacting and focusing on privacy by hiring an enterprise privacy official or Chief Privacy Officer.

Words

From the wise: Pro tips from State CPOs

We asked state CPOs to share other tips or advice they may have for states considering creating the role or for new CPOs. The following are some helpful quotes from our interviews.

Benefits of a CPO

"Since I've been in state government, security has always recognized that there are the business functions over here and security functions over there and nobody in the middle to bridge it. If you don't have a CPO to lead how you bridge that gap you have the businesses looking to security for their privacy needs and they interpret their privacy needs as something that security can do—monitoring systems, software applications, etc."

"We've had three executive meetings and three people have turned to me and said, 'we are so glad you are here, we knew we had holes, and we couldn't find a path to patch those holes'—really that patch was a human, a CPO."

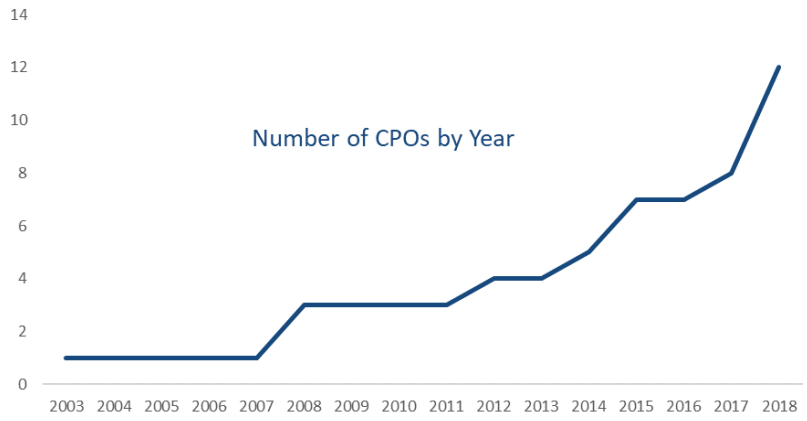
"If we miss the mark with respect to individual privacy and we lose the trust of our partners, it all stops. Because of that and our desire to continue this work, privacy is of utmost importance of us."

Enterprise Privacy Role Gaining Focus in States

In the private sector, the CPO role is relatively common for an organization or business of any size that collects personal information. The International Association of Privacy Professionals (IAPP) recognizes Jennifer Barret Glasgow, who was named CPO of Acxiom in the early 1990s as the nation's first CPO.[1] The CPO role in the private sector really started gaining momentum in the early 2000s with many large corporations filling the role.[2]

In the federal government, agencies have had a designated Senior Agency Official for Privacy (SAOP) since 2005, but they did not have to be called a CPO, which was a political compromise at the time. In 2016 the Office of Management and Budget released further guidance elevating the role, requiring that each SAOP be a deputy assistant secretary or the equivalent level.[3]

A decade and a half later, that time seems to have come for state governments. The first state Chief Privacy Officer was named in 2003 in West Virginia. Since then the role has slowly, but steadily grown in states.

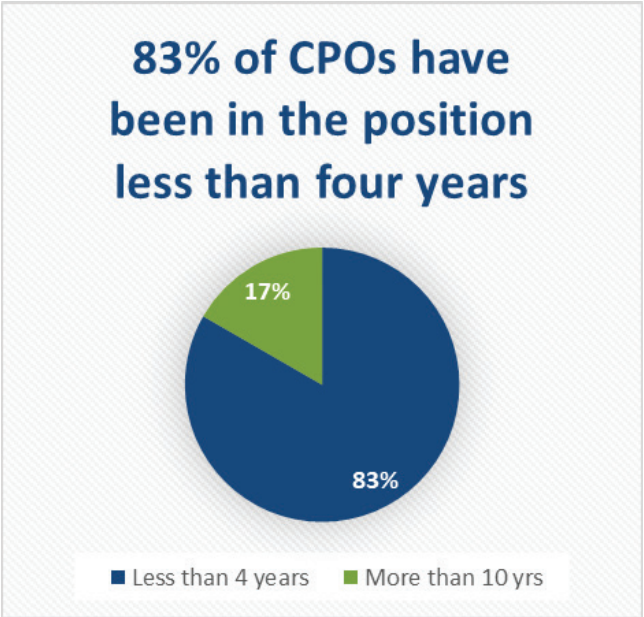


Chief Privacy Officers: A Growing Role

At the beginning of 2019, NASCIO interviewed twelve state chief privacy officers (CPOs). Of the twelve, four had been in the position for less than a year, two for less than two years and four for less than four years. The other two had held the role for over ten years. Eight of these CPOs were the first to hold the role for their state. We set out to learn why the role is gaining popularity among states, how states are structuring the role and what backgrounds state CPOs bring with them when they start the position. We also asked them for words of wisdom for states who may be thinking about creating the role.

"How do we maintain privacy while sharing data to improve outcomes? My general posture is to find a way to "yes." If a requester brings a valuable use case, how can we enable that effort from a legal perspective to advance that business case while ensuring compliance not only with the legal requirements, but (this is an important point) with citizen expectations, because you don't get to choose if you interact with us, so we better be the best stewards of your information as a data subject as we can be, and we're serious about that."

"Our state recognizes that privacy and security are key to maintaining the public's trust in state systems. Because of the data protection policies and the training required of all executive branch employees, there is pervasive awareness of the duty state employees have to protect confidential personal information, not just from unauthorized disclosure but also from improper access and use."



A CPO by Any Other Name….

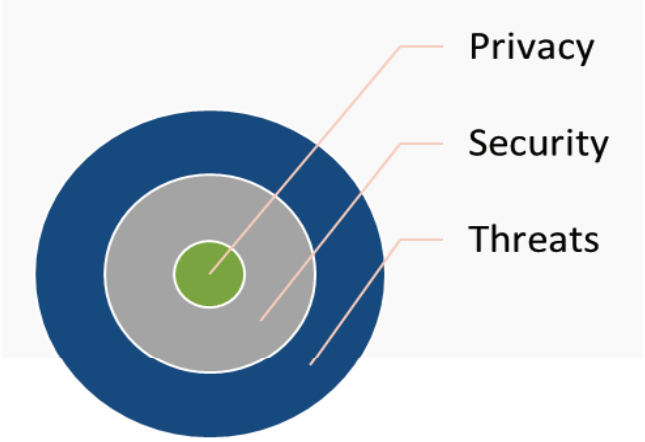
It's safe to say that most states have someone working on privacy issues even if it's not their full-time job or not at the enterprise level. Most departments of health and human services or personnel have been dealing with privacy issues longer than other agencies. However, about a dozen states have moved toward hiring an enterprise chief privacy officer or someone who holds those duties.

While most state CPOs have the title of Chief Privacy Officer (seven), others may have alternative titles such as Chief Compliance Officer, Privacy Program Manager, Compliance and Privacy Officer, Enterprise Data Privacy Officer or may have dual titles and dual roles such as Director for Enterprise Privacy, Chief Operating Officer for Information Technology or General Counsel in addition to the CPO title and role. For the purposes of this publication, we will refer to all state privacy officials as CPOs.

In a 2014 IAPP survey of Fortune 100 chief privacy officers, 59% held the "Chief Privacy Officer" title, so the variation of titles in the states is not unique to the public sector or state government.[4]

Privacy vs. Security

Privacy is a constitutional right to control access to your information. Security is the physical or technical process/procedure to protect that right from intentional or unintentional threats to that privacy.

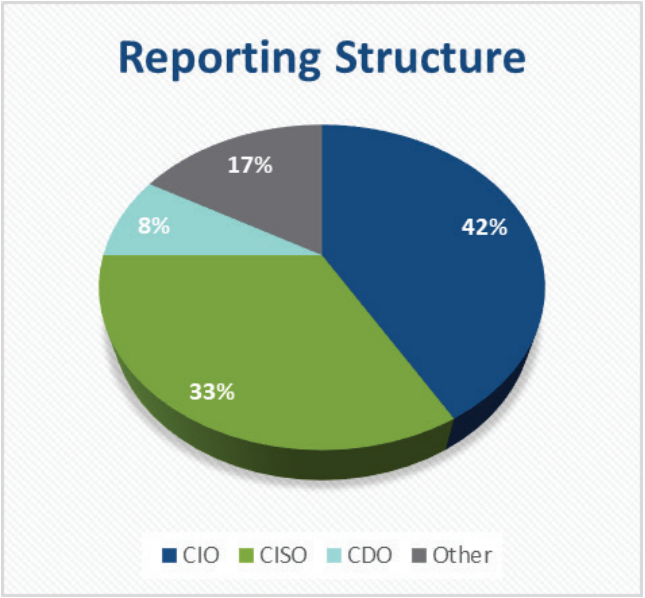


Authority and Reporting Structure

We asked the state CPOs about their authority—executive branch, judicial branch, legislative branch or only their own agency. All but two CPOs said that they have authority over the executive branch agencies—though some agencies may not choose to participate in initiatives, and some other agencies or departments outside of the executive branch agencies may receive input from the CPOs office. Two said that they only had authority over their own agencies however they did have advisory or coordination duties over other executive branch agencies. Most also said that they serve in a consultation/advisory/policy role with the judicial and legislative branches.

The structure of the role varied slightly in each state. Four state CPOs directly report to the State Chief Information Officer (CIO) and they are housed within the information technology department and another reports to a director who reports to the CIO. Four CPOs report to a state Chief Information Security Officer (CISO) though one actually reports to a manager who reports to the CISO. One CPO in a differently structured state reports to the state Chief Data Officer. Another reports to a Chief of the Technology Division which puts the CPO at the same level as the CIO and CISO. The CPO in a different state reports to the director of the board of Risk and Insurance Management.

For the private sector it's less common to report to a CIO. Again, in the 2014 IAPP survey, privacy leaders for Fortune 100 companies were most likely to be housed in the legal department (63%) and report to the general counsel (41%). Only seven percent (7%) were in the information technology department and only three percent (3%) reported to a CIO.



Statutory Authority (or Not)

Despite the strong focus on privacy that states have demonstrated by hiring a Chief Privacy Officer, only three states we spoke with out of twelve have established the role under statute. The remaining CPO positions are either under an executive order or part of other policies such as a cybersecurity policy or a privacy policy or part of an initiative from a governor or other official.

Budget (or Not)

While defined budgets are often the mark of a state's commitment to and support of a program, only one state currently has a defined budget for privacy—a line within the information security budget. Two other CPOs are currently working on their first privacy budgets and expect them to be included in the FY2020 budgets. The other nine have no defined budgets for their privacy initiatives.

Degrees and Certification

Law degrees are common among privacy professionals and this holds true in state government as well. Of the twelve CPOs we talked with seven (58%) have law degrees. In addition, eight (67%) CPOs have or are working toward at least one CIPP (Certified Information Privacy Professionals) certification from the IAPP. Some had other or additional degrees such as a Ph.D., a master's in public health, or a master's in education, which they felt had served them well in their roles. All had experience in privacy.

These numbers are similar to the private sector privacy leaders. According to the IAPP survey, 62% of respondents had a JD and 76% held CIPP/US certification.

Prior Experience

Unsurprisingly all CPOs we talked with came into the role with significant prior experience. Some had private sector experience, some had public sector experience, and some had both. Four had experience with health privacy issues. Other experiences included the US Department of Defense, private law practice, database development, software development, project management, cybersecurity, state government regulatory law, holding privacy roles at agencies, and running privacy programs for private companies or other levels of government.

As one CPO stated, "It's a very multifaceted job and there's no one thing that can prepare you. It seems people with diverse careers who have done multiple things are probably well suited for (the necessary) multi-tasking."

Advice

CPO Success: Advice from current leaders

"I believe a CPO should look at why agencies are using the data they have in the ways that they do. Look for opportunities to replace regulated data with other information which would satisfy their requirements. For example, don't use SSA information when other means might be available. Regulated data should only be used when absolutely necessary."

"You must sell the importance and need for the position within the state, in terms of business drivers and the relationship of trust and service obligations to our customers and citizens. Risk management, compliance, and the increasing growth of and demand for data are driving factors in creating the position."

A Day in the Life…

The day to day work of the state CPO depends on the maturity of the program and the authority of the CPO in any given state. It will be unique to how the role is defined and structured and organizationally located. Some of the newer CPOs are working on developing a privacy program from the ground up or working to implement a new privacy program. Some are working on implementation or focusing on learning more about the business processes of the various agencies they serve. Many of them spend a great deal of time assessing how far along agencies are in their privacy training.

Several of the CPOs we spoke with mentioned the importance of learning about the business of the agencies, so they can understand their privacy needs and better serve them. One state CPO illustrated the complexity of privacy issues at various agencies by explaining that during their assessment they were surprised to learn about the significant amount of personally identifiable information held by the state department of agriculture. While they once thought of the agriculture department as being all about cows and land, they soon realized that the agency administers welfare benefits and runs community supported agriculture programs.

Many CPOs mentioned that they administer or conduct privacy trainings for agency employees. They also may work with a privacy point person at various agencies to delegate some of the responsibilities of the privacy program and training. Many will also develop tools and resources for privacy management such as compliance guides, agreement templates and assessments tools.

Of course, despite their efforts at training and striving to bring agencies into a proactive mindset around privacy, any CPO will spend time responding and reacting to privacy incidents and answering the privacy, legal and compliance questions that arise from agencies.

Most CPOs also mentioned that they serve as a subject matter or policy expert on privacy issues for the governor, legislature and judiciary. They may give input on legislation or policy proposals because of their expertise on privacy law and privacy issues.

At least one CPO works on public education and outreach as part of their position. They visit places such as senior centers and community colleges to talk with the public about privacy. They also have a dedicated website for the public, sharing tips and tools for people who are interested in learning more about privacy in specific areas such as email and passwords.

Other duties include creating privacy impact assessments, contract reviews, negotiating with vendors, reviewing data sharing agreements, developing information security policies, and dealing with privacy issues surrounding data sharing.

> "What are we doing to build a pipeline? There's a lot of talk about building a pipeline for security, but what are states doing to build chief privacy officers. It's limited when you can't fund enough people to start building that pipeline. What are the initiatives that you as a CPO are doing to start generating a pipeline?"

"Your goal is to build a privacy management program—you don't want to just provide privacy services. Give people the tools to use the privacy program so you aren't always responding to problems."

"Find and demonstrate tangible business value and outcomes to constituents. Define and share relevant metrics. Communicate (communicate, communicate) with various audiences through a variety of mechanisms and channels to be effective. Different users have different motivations and information needs."

Motivation

Each state has a slightly different motivation for hiring a Chief Privacy Officer. For some it may be a reaction to a data breach and subsequently mandated by law. For one it was simply the enactment of and challenges associated with HIPAA. For others it may be because they understand the value in the vast amount of data held by a state—they want to use it as an asset and improve outcomes for citizens--and understand privacy is an important part of that. As states have moved toward transparency and providing open data, they also have understood the importance of ensuring that open data does not mean sacrificing citizen privacy.

Other states have recognized that having a privacy point person was an important part of taking information security seriously and a good compliment to a Chief Information Security Officer. One CPO suggested to a former colleague, who happened to be the incoming governor of their state, that the state was lacking in privacy. That advice led to a job offer as the state's first ever CPO. If often just takes one person with a focus on privacy to change the direction of a state's privacy posture.

Privacy Culture: Proactive or Reactive?

We asked CPOs if they felt that their state had a proactive or reactive culture when it comes to privacy. Those with more developed privacy programs thought it was proactive. They mentioned that top-down support from the governor or agency head was key in getting the support needed to have a proactive privacy program.

Those with programs just starting out tended to classify the program as reactive. One CPO said that agencies evolve from reactive to proactive only after there is a privacy incident: once they realize there is a problem, and there is someone to talk to about it, and there were steps they could have taken to prevent it, then it becomes a priority. As one CPO stated, "It's difficult to get into an agency and say, 'you should be doing this,' until they call me and say, 'we lost a laptop, what do we do?'"

Maturity of the Privacy Program

Because most of the CPOs we talked with were the first to hold the role, most of them also had a hand in (or continue to work on) developing the program (or implementing it if it was previously established in law). Three of the CPOs are working on creating their privacy programs from the ground up. When they took the positions, this was one of their first tasks.

One CPO helped the governor's office draft executive orders for the privacy program, and then they worked to implement the program once the executive orders were established. Another came into a state with a privacy and security program based on NIST (National Institute of Standards and Technology) standards. Their job was to help agencies meet the goals that had already been set by law.

Some of the other CPOs have helped develop and implement currently established privacy programs in the last few years.

Advancing the Role of the Chief Privacy Officer: Advice from State CPOs

We asked state CPOs for their advice to state leaders who may be interested in creating or elevating the CPO role. We wanted to know what they thought worked and didn't work best in their states, and what the ideal CPO role, reporting structure and authority would look like. Three main themes emerged: the CPO should sit where they have an enterprise view, they need a budget and enforcement authority, and they need a point of contact in every agency.

1. Give the CPO an Enterprise View and Authority

While CPOs differed on where exactly the position should be organizationally located within the executive branch, the consensus was that the role needs to have authority and placement over the state government enterprise to be most effective. Those who advocated housing the position in the information technology (IT) department, stressed that it works only if IT is already consolidated or plays a centralized role. If the CPO's office is under a different agency, the agency should be a shared services agency similar to IT.

Others argued that it makes more sense for the CPO role to be in the compliance/legal environment, or wherever a cyber insurance policy is administered for ease of coordination. There were concerns that privacy leaders deal with many issues outside of information technology, so it can unintentionally limit the scope of the privacy program to be under IT.

Still some CPOs went as far as to say the role should be cabinet-level reporting to the governor or part of the governance team. One also suggested the CPO could be the head of a privacy commission which could be a very strong position for a CPO in state government.

2. Enforcement Authority and Budget

Another common theme was that the CPO would be most effective if the state passed legislation clearly defining the scope of the role while creating enforcement authority and a budget. Most CPOs found that it is difficult to get all agencies to take advantage of their offered services without enforcement authority. Many CPOs are only able to make themselves available when agencies come to them with concerns or questions or offer trainings to those who are willing to attend. Having the ability to push out policies to agencies results in consistency among the executive branch agencies on how they collect data and why it is collected.

Those without a budget often must ask their agency head for funding for each project they want to undertake. Along with a clearly defined budget, some CPOs also expressed the need to staff the CPO's office while building a pipeline of privacy professionals at the state-level.

3. A Privacy Officer in Every Agency

Many CPOs expressed the benefit of having a privacy officer or a designated privacy contact in each agency that would either report to or coordinate with the CPO. This would help the CPO better understand the business process for each agency. It also allows the CPO to be able to train someone at each agency which would result in consistency and the ability to mature the privacy program at the same rate at each agency. Of course, this must be part of the privacy budget as well. As one CPO stated, "I think it's very difficult when other agencies aren't already funded to do this type of thing, because human services (and similar agencies) will always come first, and budgets are tight."

The CPOs who had this set-up in their states found it extremely useful and beneficial. One CPO stated that one of the most valuable functions of their job was coordinating the different agencies. "There are agencies that have really good procedures developed, and we are able to share that with the other agencies which leverages the work that has already been done in that area," explained the CPO.

Endnotes

1. Jennifer Barret Glasgow IAPP Profile: https://iapp.org/about/person/0011a00000DlPjEAAV/
2. CNET: IBM Appoints Chief Privacy Officer: https://www.cnet.com/news/ibm-appoints-chief-privacy-officer/
3. Federal News Network: OMB Turns up the Juice for Federal Privacy Officials: https://federalnewsnetwork.com/reporters-notebook-jason-miller/2016/09/omb-turns-juice-federal-privacy-officials/
4. Benchmarking Privacy Management and Investments of the Fortune 1000: Report on Findings from 2014 Research. IAPP: https://iapp.org/media/pdf/resource_center/2014_Benchmarking_Report.pdf

Principle Author and NASCIO Staff Contact: Amy Hille Glasscock, Senior Policy Analyst, aglasscock@nascio.org

Contributor: Doug Robinson, Executive Director, NASCIO

Special thanks to the twelve state privacy leaders who volunteered their ti me to speak with NASCIO for this project.

NASCIO
Representing Chief Information Officers of the States

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and information technology (IT) executives and managers from the states, territories and District of Columbia. NASCIO's mission is to foster government excellence through quality business practices, information management and technology policy. NASCIO provides state CIOs and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information and promote the adoption of IT best practices and innovations. From national conferences to peer networking, research and publications, briefings and government affairs, NASCIO is the premier network and resource for state CIOs. For more information, visit www.NASCIO.org.