NASCIO Representing Chief Information Officers of the States

Research Brief

October 2006

NASCIO Staff Contact: Mary Gay Whitmer, mwhitmer@AMRms.com or (859) 514-9209.

Keeping Citizen Trust: What Can A State CIO Do To Protect Privacy?

Privacy--A Defining Issue:

Privacy is a defining issue of the day for both the public and private sectors. Citizens are now aware of data breaches, identity theft and the risks that can result from personal information finding its way into ill-intended hands. Even state legislatures have taken notice of privacy's importance in recent years. From 2004 to the present, thirty-eight state legislatures have enacted data breach notification laws mandating, to varying extents, notification requirements for citizens whose personal information has been compromised by a security breach. In spite of legislative measures taken on this issue, data breaches have been frequent in the private, public and university sectors. The figures and the potential financial consequences can be startling:

- Approximately **324 data breaches** have been reported since February 2005.
- Over **93 million records** with personal information may have been compromised.[1]
- A recent, high-profile data breach involving a data reseller **cost an estimated $6 million** ($2 million of the total cost expended was used to notify those with compromised information).[2]
- The Congressional Budget Office (CBO) estimated that one recent **federal data breach notification bill would likely cost state, local and tribal governments in excess of the $64 million** unfunded mandate threshold in one of the first five years after implementation. CBO also estimated that these costs would be likely to grow over time.[3]

In addition to potentially substantial financial consequences, a privacy compromise can quickly create public relations concerns. For example, these headlines were in the mainstream press:

- ***"Thieves Steal Personal Data of 26.5M Vets"***[4]
- ***"Source: Theft of Vets' Data Kept Secret for 19 Days"***[5]
- ***"Vets Rip VA and Data Breach Report"***[6]

---

[1] "A Chronology of Data Breaches Reported Since the ChoicePoint Incident," Privacy Rights Clearinghouse, updated October 2, 2006, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.
[2] "Be Afraid of the Catastrophic Data Breach," Searchsecurity.com, December 1, 2005, <http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1147324,00.html>.
[3] Congressional Budget Office Cost Estimate, S.1789 Personal Data Privacy and Security Act of 2005, April 19, 2006, <http://www.cbo.gov/ftpdocs/71xx/doc7161/s1789.pdf>.
[4] "Thieves Steal Personal Data of 26.5 M Vets," Hope Yen, abcnews.com, May 22, 2006, <http://abcnews.go.com/Politics/wireStory?id=1991902>.
[5] "Source: Theft of Vets' Data Kept Secret for 19 Days," Terry Frieden, John King, and Marsha Walton, cnn.com, May 23, 2006. <http://www.cnn.com/2006/US/05/23/vets.data/index.html>.

Those headlines refer to a recent, high-profile data breach in which an employee with the U.S. Veterans Administration (VA) took home a laptop computer in violation of the VA's IT security policy. The laptop contained the personal information of over 26.5 million veterans and was stolen from the employee's home. While the laptop was later recovered and the personal information was determined not to have been compromised, the damage had already occurred. Unflattering headlines had been written. Jobs had been lost. Citizen trust in a federal agency's ability to keep personal information private had been diminished at best and, at worst, irreparably harmed.

While this data breach involved a federal agency, the compromise of citizens' personal information could easily occur at the state or local level. For example, consider these *possible* headlines:

- "***Thieves Steal Personal Data of 5 Million Citizens of [insert state name here]***"
- "***Citizens Rip [insert state name here] and Data Breach Report***"

Or what about the following possible headline?

- "***Citizens Rip State CIO for Data Breach Report***"

The possibility is real, but the risks can be greatly minimized through the use of the appropriate privacy policies and practices, business process improvements, and implementation of security measures.

The Evolving Nature of the Privacy Discussion:

Privacy has always been an important issue that has even been recognized and protected by the U.S. Supreme Court.[7] However, the nature of the privacy discussion is evolving and has become increasingly complex. It has not been that long since privacy protections were provided, at least to an extent, by public records being discretely tucked away within locked file cabinets of government agencies. Now, though, the privacy discussion is driven by an environment of increased information sharing across traditional agency and governmental boundaries and the ease with which information can be collected, compiled, manipulated, used and transmitted. Rapidly evolving technologies have and will only continue to facilitate this, while the legal framework for privacy, as well as the generally accepted business practices to guard against privacy compromises, have failed to keep pace. The rise of homeland security efforts at all levels of government has also played a significant role. Moreover, privacy has become an important facet of many of the high-priority issues of the day, including:

- Homeland security
- Emergency management
- Disaster recovery and business continuity after natural disasters, such as Hurricane Katrina, or homeland security-related events

---

[6] "Vets Rip VA & Data Breach Report," K.C. Jones, July 14, 2006, <http://www.techweb.com/showArticle.jhtml?articleID=190400470&cid=RSSfeed_TechWeb>.

[7] Griswold v. Connecticut, wikipedia.com, October, 02, 2006, <http://en.wikipedia.org/wiki/Griswold_v._Connecticut>. In this decision, the U.S. Supreme Court held that a "right to privacy" exists, even though it is not explicitly stated in the U.S. Constitution or Bill of Rights.

- Electronic health records
- Driver's license reform through REAL ID Act implementation
- IT consolidation and shared services initiatives

In the context of this evolving privacy discussion, many states are still in the process of determining how best to address privacy across the state enterprise, and the state CIO's involvement varies greatly from state-to-state. Regardless of where responsibility for privacy may reside in a given state, the one constant among all states is the need for the many privacy stakeholders to understand privacy's importance and how citizen privacy can be protected. ***This brief provides state CIOs with a common frame of reference for the importance of citizens' information privacy and some initial ways for states to implement and manage privacy protections.***

I. Common Starting Points for a Privacy Discussion

What Privacy Is and Is Not:

Privacy and security are closely linked but are not interchangeable concepts.

Privacy, in the context of this brief, refers to the decisions that are made about when and how states should collect, store, use, disseminate and dispose of citizens' personal information and how policies based upon those decisions should be implemented. For example, when should it be acceptable for an agency to collect a citizen's Social Security Number? Can that agency then share that citizen's name and Social Security Number with other state agencies? Or even share it with third parties, such as data resellers? These questions involve citizen privacy with respect to personal information and create the need for states to address how citizens' personal information is handled in a holistic fashion.[8]

Privacy is a personal construct that accrues to individuals, not to the information itself. In other words, a *person* may have the right to have certain personal information kept private by the state. That right does not accrue to the information itself. An individual's right to information privacy is a separate concept from the confidentiality rights that may apply to a corporation regarding its intellectual property or other business-related information which, if wrongfully disclosed or misappropriated, could result in economic harm.

While there is not a universal definition for the types of information that are considered "private" and should be subject to heightened protections, certain types of information are more likely to be protected by privacy laws, regulations, and/or policies. For example, there are legal

[8] The broader concept of privacy as it relates to personal freedom from government intrusion is protected by the U.S. Supreme Court in the landmark case, Griswold v. Connecticut. Although neither the U.S. Constitution nor the Bill of Rights contain a specific right to privacy, the Court struck down a Connecticut state law that criminalized the use of contraceptives on the basis that the Bill of Rights contains "a penumbra" or zone protecting privacy that is necessary to give the Bill of Rights' specific guarantees "life and substance." *However, this brief addresses privacy only as it applies to the government's use of citizens' personal information.* For more information about Griswold, please see: <http://en.wikipedia.org/wiki/Griswold_v._Connecticut>.

protections in place regarding a government entity's collection of Social Security Numbers and criminal penalties that can result from wrongful access to financial account information. Medical information is also subject to federal and state regulation and is considered among the most sensitive types of information.[9]

Security is a related concept. It is *how* information is protected--the measures that an organization takes, including virus protection, firewalls, roles-based access to sensitive information, and intrusion detection systems, to ensure that personal information is not accessed or used in a manner that is contrary to its privacy policies.

Although privacy and security are separate concepts, the relationship between the two is best expressed by the statement that "one cannot have privacy without security." The privacy policy dictates *how a state will collect and use citizens' personal information*. The security policy dictates *how a state will protect that information* from misuse by those internally as well as externally.

II. The Public Sector Environment

The evolving discussion regarding how to protect citizen privacy has been the result of a convergence of factors that originate from both inside and outside of state government. ***One of the major factors unique to government is the inherent openness that is expected of government at all levels. This has created the challenge of balancing that expectation of openness and transparency with the need to protect the privacy of personal or sensitive citizen information.*** The recent surge of major media coverage has also pushed privacy to the forefront of citizens' minds. As the events of the next several years unfold, including those that are related to technology, politics, and homeland security, other factors will likely be added to the list of current privacy drivers below:

Internal Factors:

Environmental Complexities:

- The **complexity of state government** with many agencies and branches that collect and hold a wide variety of citizens' and state employees' information
- Legal mandates **requiring the retention of certain types of information**, such as that related to workers' compensation claims, for many decades
- A **patchwork of state laws** governing privacy on a sector-specific basis, such as medical privacy and Social Security Number protection laws
- The **increasing need for the cross-referencing of information across agencies** and even levels of government, such as checking the names of lottery winners against lists of individuals who are overdue on child support payments

[9] For more information about the types of personal information that are legally protected, please see NASCIO's "Information Privacy: A Spotlight on Key Issues," February 2004, <http://www.nascio.org/publications/InformationPrivacy2004.pdf>.

NASCIO • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com •
W :: www.nascio.org

People:

- The increasingly **tech-savvy nature of state employees** who know how to use and misuse state IT resources
- The **presence of contractors** who may use or work with state IT resources and have access to citizens' personal information

Technology:

- The prevalence of **personal technological devices in the state workplace**, such as PDAs and iPods, that possess large storage capabilities
- The **more mobile workforce** with state-issued laptops, PDAs and other wireless devices that can be easily lost or misplaced and may contain sensitive information
- The **evolving nature of state websites** and balancing the desire to make information available electronically with the need to ensure that certain personally identifiable information is not placed on the web or available without appropriate safeguards

External Factors:

Environmental Complexities:

- The exploding **growth of digital information** within both the public and private sectors
- **States' need for cross-boundary information sharing**, including with local governments (examples exist in the justice, homeland security, data fusion center and health IT contexts)
- **Increased interest in health information exchanges** at all levels of government and with the private sector
- The challenge of **protecting more types of individuals' contact information**, including information concerning home phone, address, email, wireless devices, cell phones, and instant messaging applications
- The interest of **commercial data resellers** in continuing to purchase states' databases of personally identifiable information
- Sector-specific **federal privacy regulations**, including those in the medical and financial areas, that may directly apply to state entities or could influence state privacy protections

People:

- The **gradual erosion of citizen trust in government** as data breaches occur with increased frequency
- Growing **citizen demands for governmental accountability and transparency** with respect to many types of information, such as information on criminal activity, sex offenders, delinquent taxpayers, voters in elections, campaign contributions, disciplinary actions against professional license holders (including doctors and lawyers), and the quality of health care
- The increasing **demand for more and enhanced online citizen services** that may require the collection of citizens' personal information and the implementation of enterprise identity management solutions
- The importance of conducting **background and credit checks using private sector resources** in relation to applicants for state employment

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com •
W :: www.nascio.org

Technology:

- The **ever-mutating state IT threat environment** in which viruses, worms, botnets and hackers present the risk of exposing citizens' personal information as well as sensitive government information
- The use of **online geographic information systems (GIS) through which citizens can access spatial information**, such as an aerial view of an individual's house
- The **adoption of emerging technologies**, including Radio-Frequency Identification (RFID) and other emerging wireless state technologies

III. The Current State of Privacy

State Privacy at Present:

With states functioning in an environment of expanding information sharing efforts across traditional governmental boundaries, all too prevalent data breaches, and heightened levels of citizen distrust, [10] ***the criticality of developing an organized way to address privacy issues across the state enterprise has also increased.*** To understand when and how state CIOs may encounter privacy issues, an important first step is to examine how privacy issues come into play within the current state environment.

The Decentralized Nature of State Government: Comprised of many agencies, branches, and quasi-governmental entities, states hold mounds of sensitive, personal information in disparate places across the enterprise. The same information relating to an individual, such as a Social Security Number, may be collected, used and stored by multiple state agencies. With data stored in a distributed fashion across the state, protecting that data in all of the places in which it exists can be a monumental task. In addition, agency policies and business practices with respect to that information may vary greatly, increasing the risk that a privacy compromise could occur, even if most agencies have adequate privacy protections in place.

Greater Opportunities for Information Sharing: Within many contexts, such as justice and health care, there are expanding opportunities for information sharing across agencies, among levels of government and with the private sector. Many of these information sharing initiatives stem from the need to detect fraud, enforce tax and child support payments, prevent medical mistakes, and even avert terrorist attacks and other serious crimes.

A Complex Legal Framework: Adding more complexity is a legal framework that addresses privacy on a sector-specific basis. There are both state and federal laws that address the privacy

[10] "Privacy Trust Survey of the United States Government: An Executive Summary," the Ponemon Institute and The CIO Institute of Carnegie Mellon University, January 31, 2004, <http://cioi.web.cmu.edu/research/2004PrivacyTrustSurvey>.

of certain types of information—health information, financial information, and other types of sensitive, personal information. However, since privacy has been addressed in a somewhat organic fashion, there may be conflicting statutes across state agencies. Some agencies may collect personal information that other agencies are legally prohibited from collecting. The same may be true regarding the resale or secondary use of information. For example, one state agency may be able to share or sell information, while another, such as a state motor vehicle department, may be restricted from sharing or reselling the information unless it is for certain, specified purposes. The secondary use or resale of citizen information is especially important in the government context, because citizens frequently must provide personal information in order to receive a government entitlement or service. However, citizens may be unaware that this information can be shared with other agencies or even resold to a private sector data reseller.

The State CIO and Implementation of Privacy Requirements:

It is within this complex environment that state CIOs may encounter issues related to the effective management and implementation of privacy protections involving technology and the handling of electronic data. Hence, state CIOs need to understand how their enterprise view can contribute to addressing privacy-related issues. For example, state CIO insights might include:

- How the variety of technologies and business process improvements across the state can be used to properly implement and manage privacy protections
- How privacy should be "baked-into" new IT systems by identifying and addressing privacy issues at the beginning life cycle stages
- How security measures can help ensure private citizen information remains that way

The state CIO also can share expertise regarding how initiatives such as IT consolidation, shared services, enterprise architecture, security, enterprise identity management, and even REAL ID Act implementation, present unique issues and challenges. These must be considered in the implementation of security controls and other measures that ultimately serve to protect the privacy of citizens' personal information.

Key Privacy Considerations for the State CIO:

As privacy concerns continue to arise, some key issues that a state CIO may need to examine are as follows:

- **Risk Management:** Privacy is a risk management issue regarding how best to minimize the risk of personal information being exposed to the public or to those without proper authorization.
- **Privacy is Part of the Information Management Life Cycle:** Privacy considerations are infused throughout the data management life cycle from the time it is collected to the time of its ultimate disposal. For example, before electronic equipment is disposed of or sold, there should be adequate measures in place to ensure that any personal or classified information that may have been stored on that equipment is properly sanitized and is not retrievable.
- **Privacy Involves Both Legal and Business Decisions:** Some questions revolving around privacy are legal in nature. These include questions such as: What must a state do to protect

privacy? What is a state prohibited from doing? What are the areas in which a state may use its discretion about how to protect privacy? Other decisions, though, are business decisions—how can an agency integrate business process improvements that will better protect citizens' personal information?

- **The Many Forms of Personal Information:** Privacy involves not only information that is in electronic form, but also information that may be in a paper-based form locked within government file cabinets or storage facilities. Since citizens' personal information may ultimately be kept in multiple forms, from paper to electronic, rules that are consistent across media types are helpful.
- **Implicit Privacy-Related Responsibilities?** Some CIOs may already have some implicit responsibility for privacy through their involvement in IT security, consolidation, enterprise architecture or business process improvement initiatives.

IV. Privacy at Risk--What a State CIO Can Do

State CIOs will likely encounter privacy issues in relation to state IT systems and electronic information. These issues may arise within the implementation of a new IT system, a new statewide initiative, such as REAL ID Act implementation, or in connection with the state CIO's IT security responsibilities. Below are some areas in which the state CIO may discover the existence of IT-related privacy issues. Within those areas, this brief identifies instances in which the CIO may need to consider the implementation of privacy protections in order to foster citizen trust.

In exploring the suggestions below, CIOs should take into account the unique facets of their states, including existing governance structures and their state's IT and political environment.

Governance:

- **Get a Seat at the Table:** For issues involving the storage, transmission, sharing or disposal of personal information, the state CIO can provide important technical and policy expertise and should have a seat at the table when such issues are involved. This is particularly true with respect to electronic information that may be highly sensitive, such as medical information or information that must be retained for many years. The state CIO also may find it helpful to develop a relationship with the state Chief Privacy Officer (in the rare case that a state has one), the state Attorney General or agency information owners. In addition, a state CIO may seek to involve state enterprise architecture and security staff members where they have the appropriate expertise to be of assistance. Another option may be for the state CIO to create a privacy subcommittee or working group under the state CIO Council.

Enterprise Architecture-Related Efforts:

- **Incorporate Privacy into Enterprise Architecture (EA):** State CIOs generally lead a state's EA efforts and should consider the placement of a privacy domain within the state's architecture and include representation from a variety of agencies on the privacy domain team. EA can be an effective tool in helping to understand a state's legal and

policy parameters with respect to privacy and how to design privacy requirements into IT systems, as well as accommodations for future changes in what information is considered private. In addition, the variety of perspectives from agencies participating on the domain team can be invaluable. For state CIOs who may not have the flexibility to incorporate a formal privacy domain into their state's EA program, the consideration of privacy issues can help a state determine and/or solidify where responsibility for privacy implementation regarding electronic information may reside.

- **Security Standards:** Security standards provide an avenue through which a state CIO can contribute to ensuring that citizens' private information remains that way. For example, if personal information will be submitted by citizens via the state's portal, then the implementation of security measures, such as Secure Sockets Layer (SSL), are necessary to prevent unauthorized individuals from accessing or intercepting that information. A similar example is the implementation of standards for the encryption of personal or sensitive information that is stored on or transmitted by portable wireless devices, such as PDAs or laptops.
- **Embark on a Data Classification Effort:** Data classification efforts can serve as a valuable starting point in determining which categories of information held by the state are sensitive and therefore subject to potential risks that include data breaches and other privacy compromises. Once sensitive categories of information are identified, such as Social Security Numbers, credit card numbers, financial information and medical information, the state CIO may consult on the appropriate types of security measures that can be applied to ensure the privacy of that information.

Arkansas' Data Classification Effort: As the Arkansas Office of Information Technology (OIT) began to create standards, it became apparent that not all information held by state agencies should be protected in the same manner. This made the classification of agencies' data imperative. In 2003, OIT looked to other states and the federal government for examples. Arkansas' grid is organized according to both data sensitivity and system criticality. As Arkansas agencies complete the grid, they must consider external privacy mandates, since the grid does not define what information is "private." Agencies also must consider their systems in terms of the criticality of the government services they support. The most critical government services are considered to be public safety and public health services. It is important to note that other security standards directly relate to the classification of data and IT systems. For example, back-ups of "sensitive," "very sensitive" or "extremely sensitive" data must be housed off-site at a secure location.

For more information about Arkansas' data classification policy, guidelines and grid, please see the following webpage and click on "Data and System Security Classification": http://www.techarch.state.ar.us/indexes/standards.htm.

- **Standing Guard--Network Monitoring and Perimeter Defense:** Monitoring systems with inbound content filtering can help to manage spam and phishing attacks that could otherwise compromise personal information or the security of a state's

network. The monitoring of Internet activity can also be used to block state employees from visiting inappropriate websites. Depending upon whether a state CIO has operational IT security responsibilities, the CIO could have authority with respect to network monitoring and perimeter defense measures.

Policy:

- **The Policy Piece:** Understanding privacy policies and their potential impact is critical, especially in the designing of IT systems. Therefore, the CIO should be at the table to advise on implementation, management, and financial impact issues, when privacy policy is being debated.
- **Use of the Fair Information Principles:** When state CIOs encounter privacy issues, the use of the Fair Information Principles (FIPs) can be of assistance. Identified by the Federal Trade Commission in a 1998 report regarding online privacy, the FIPs form the basis of many U.S. and international privacy laws. The principles are as follows and can be used to guide the analysis of privacy issues:
    - **Notice/Awareness:** Providing a citizen with notice of the collection and intended uses of his or her personal information
    - **Choice/Consent:** Providing a citizen with a choice or means of consenting to the collection and use of his or her personal information
    - **Access/Participation:** Permitting a citizen access to his or her personal information and a means of correcting inaccurate or incomplete information
    - **Integrity/Security:** Providing appropriate measures to secure citizens' personal information that has been collected
    - **Enforcement/Redress:** Enforcing privacy policies that are in place and providing citizens with a means of redress in instances of non-compliance

  The FIPs are meant to serve as guideposts and their application will vary with the circumstances. For example, it may not be appropriate in a justice setting to provide a person accused of a crime with notice or consent regarding the collection of his or her personal information. The Federal Enterprise Architecture Security and Privacy Profile, v.2.0, contains a "Privacy Control Family," which is similar to the FIPs but is geared to government privacy protection. For more information, please see this newly updated profile at: http://www.whitehouse.gov/omb/egov/documents/FEA_SPP_Ver2.pdf.
- **State Website Privacy Policies:** Almost all state website portals include a link to a privacy statement from the portal's homepage. However, such privacy statements are not effective unless all agencies that have webpages on the state portal adhere to those statements. Through his or her involvement in state portal issues, the state CIO may be able to play a role in ensuring that state agencies comply with portal privacy statements. It is also important for those privacy statements to clearly delineate the types of personal information that may be collected, used, and stored, and list a primary point of contact for citizens with questions or concerns. For links to state website privacy policies, please see NASCIO's "State Profiles" webpage at: http://www.nascio.org/aboutNascio/profiles/. *Each state profile includes a link to the state's website privacy policy as well as its homepage.*

NASCIO • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com •
W :: www.nascio.org

- **Acceptable Email and Internet Use Policies:** A CIO may have authority with respect to a state's policy regarding employee and contractor use of state email and the Internet. Acceptable use policies should clearly prohibit employees and contractors from emailing personal information with exceptions for certain instances where there exists a business need for such and appropriate security measures are in place. Adequate employee and contractor education can make a difference in reducing the amount of personal information that is transmitted via unsecured email or the Internet.
- **Records Retention and Archiving Policies:** Today's reality of email, electronic communications and "born digital" content in state government has increased the risk of inappropriate retention of records and the converse of that--deletion of electronic records that should be kept for legal or business reasons. Records form the basis of a state's information intelligence and are increasingly only available electronically. However, if records are kept past their specified retention period, there is a risk that those records, and the personal information within them, could fall into the wrong hands. If a state CIO encounters this issue, the CIO may consider suggesting a systematic approach to managing records retention issues. This may include the creation or clarification of guidance for agencies on the retention and archiving of electronic records containing personal information. Note that this may exist in connection with some states' freedom of information laws.
- **Too Much Information--Policies Regarding Citizens' Submission of Personal Information:** In making an initial inquiry with a state agency through email or a live-help chat application, a citizen may submit personal information, such as a Social Security Number or other sensitive information, when it is not necessary. Acceptable use policies should cover such scenarios and include processes through which state employees can discourage citizens from submitting that type of personal information, unless it is required or requested. This may be a more prevalent occurrence for benefits or retirement system agencies. You can find more information about the privacy implications of live-help chat applications in Appendix C of NASCIO's Research Brief entitled "TLK2UL8R: The Privacy Implications of Instant and Text Messaging in the States," at: http://www.nascio.org/nascioCommittees/privacy/#publications.
- **Data Breach Notification:** A significant number of states have enacted data breach notification laws requiring that notice be sent to individuals whose personal information may have been compromised so that they can take steps to monitor their credit reports for any suspicious activity. Such policies can be a way of helping citizens minimize the damage to their credit and finances that could result from a data breach. In the event of a breach at the state level, the CIO may be a participant on the response and crisis management team. Thus, for states with a data breach notification law, the CIO may find it helpful to understand what types of privacy compromises trigger data breach notification requirements and what state obligations flow from those requirements. For states without such a law, the CIO may consider what notification steps may be appropriate if a privacy compromise occurs.
- **Blog Away?** Blogging has become a popular means of self-expression. However, acceptable use policies that apply to state employees are necessary so that state employees know where the line is between appropriate and inappropriate blogging. A state CIO may consider including guidance for blogging in state IT requirements or acceptable use policies.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com •
W :: www.nascio.org

Business Processes and Practices:

- **Bake Privacy into New IT Systems and Technologies:** For some IT projects within a state CIO's purview, privacy regulations or laws may require privacy to be "baked into" new IT systems. To be truly effective, privacy must be considered at the very inception of a project, throughout the design process, and all the way through to implementation. In this way, privacy can be part of the fabric of an IT system and not simply an add-on at the end.
- **Where is Your IT Equipment? Asset Management and Tracking:** Knowing where state IT equipment is and whether it could potentially contain citizens' information is a starting point for protecting citizens' private information. From there, a state will be better able to track those IT assets throughout their respective lifetimes.
- **Disposal of IT Assets:** With the disposal or salvage of IT assets containing citizens' personal information, a state will likely have to take more extensive measures to ensure that all of the personal information has been sanitized and cannot be retrieved once an IT asset is out of state reach. This may include such assets as CDs, magnetic tapes, thumb drives, and cell phones—all of which could hold personal or other sensitive information. IT security standards may specify the minimum steps to ensuring proper IT asset sanitization.
- **A Word about Wireless Devices:** With the increasingly mobile state workforce, state employees or even contractors may use wireless devices and could store personal information on them or receive or transmit such information via those devices. Business processes that account for potential privacy implications associated with those devices can be of assistance in protecting private information while allowing employees to be more mobile. State employees may also introduce their own personal wireless devices, such as iPods, cameraphones, and thumb drives into the state workplace. These devices could be used in an unauthorized fashion to extract potentially sensitive information from the state workplace. For more information about the privacy implications of portable wireless devices and security measures that can be used to protect sensitive information that may be stored on or transmitted via those devices, please see NASCIO's "The Year of Working Dangerously: The Privacy Implications of Wireless in the State Workplace—Parts I and II," at: http://www.nascio.org/nascioCommittees/privacy/#publications.
- **Compliance, Enforcement and Audit:** Enforcing compliance with enterprise IT standards and adding an audit function regarding those standards are ways of ensuring that agencies take privacy protection seriously and implement those measures in a competent fashion.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com •
W :: www.nascio.org

Privacy and Portfolio Management in North Carolina: As of October 1, 2006, North Carolina state agencies are required to comply with a state law that deals with personally identifiable information (PII) and data breach notification (N.C.G.S. 75-65). The State Information Security Office has an initiative to identify ways to help agencies meet needs created by this new law. The state has taken an enterprise approach to the life cycle of IT systems, which are tracked from inception (project proposal) to retirement through the Portfolio Management System (PPM). Since the implementation of the PPM approach, the state has incorporated information security in the project review process. As part of the information security review risk assessment, agencies with proposed new IT systems are asked to identify any legal and regulatory requirements pertaining to confidential or PII data. For systems containing confidential information or PII, the security architecture must be appropriately more robust. For existing IT systems, the PPM system has recently been upgraded to store data fields relating to confidential or PII information. Once this information is entered by the agency, the state has the added capability to determine which systems have confidential or PII data fields. This information is useful throughout the system's life cycle in risk management and cyber incident response. For example, if a state agency IT system has a cyber incident, a quick look at those fields in the PPM system would determine if PII reporting requirements apply, thus helping the agency to respond appropriately.

- **State IT Consolidation:** All manner of IT consolidation efforts have emerged in the past several years in many states. A recent, national NASCIO survey assessment of the states regarding IT consolidation revealed a strong trend towards consolidation in the states. Nearly 75 percent of the 34 survey respondents who had consolidation efforts responded that the CIO was the initiating party for the consolidation effort.[11] The consolidation of IT systems and resources could bring together sources of information, especially where data warehouses are created or expanded. In such cases, CIOs may encounter privacy issues and may need to analyze and understand the privacy controls that are required in addition to the appropriate IT security controls.
- **New State Initiatives and Privacy Implementation:** As the state technology leader, a state CIO may be involved in a wide-range of projects from driver's license reform with REAL ID Act implementation to homeland security or emergency management efforts to IT consolidation and enterprise identity management initiatives. As a result, the CIO may be able to point out particular challenges in implementing privacy protections that may be associated with these projects and initiatives.
- **The Privacy-Procurement Connection:** A sound practice is to ensure that the procurement process incorporates compliance with security and privacy requirements. If a state CIO has review authority over agency IT procurements, then, by ensuring that adequate security measures are in place, the state CIO also will be helping to ensure the protection of any sensitive information that may be involved.

[11] "NASCIO's Survey on IT Consolidation and Shared Services in the States: A National Assessment," NASCIO, May 2006, <http://www.nascio.org/publications/ITConsolidationMay2006.pdf>.

From the Legal Side:

- **Be Aware of Privacy Laws and Regulations:** The U.S. takes a sector-specific approach to privacy regulation with laws in sectors such as health care and financial services. Federal privacy laws such HIPAA (the Health Insurance Portability and Accountability Act) may apply to state agencies that handle health-related information. If a state agency conducts certain types of activities with the federal government, such as data matching programs, then federal privacy laws may govern those activities as well. States also have unique legal frameworks for privacy. In recent years, many states have enacted data breach notification, anti-spyware, anti-phishing and other laws in pursuit of citizen privacy protection.[12] Understanding privacy laws and regulations can help CIOs identify where privacy issues might arise and what steps should be taken in pursuit of those legal requirements.
- **Contract Negotiations with Data Resellers:** The state CIO's involvement in negotiating conditions of use with data resellers can ensure that the appropriate privacy protections are in place with respect to citizens' personal information once it is in the hands of data resellers and their downstream customers. State CIOs should work with their legal counsel to ensure that information provided to data resellers is subject to the appropriate disclosure requirements and protections.

Security and Data Protection and Handling:

- **The Connection Between IT Security Measures and Privacy:** Since privacy cannot be accomplished without adequate security measures, state CIOs should consider whether current IT security standards and practices are adequate to protect the privacy of citizens' information. For example, increasing numbers of state employees use wireless portable devices, like PDAs. The state CIO may consider heightened security measures, such as encryption for data both at rest and in transmission, if a state employee handles sensitive information on such a device. By encrypting sensitive information, the potential consequences incurred if a PDA is lost or stolen can be greatly minimized.
- **Access Controls to Physical Facilities and IT Systems:** Access controls can be a valuable tool in preventing those without authorization from accessing personal information. For example, employee access cards for facilities that house important state IT infrastructure, such as data centers, can prevent unauthorized individuals from ever entering the premise where they then could try to compromise state IT assets. Access controls for individual computers can also assist in keeping those without proper authorization from accessing systems containing sensitive information, such as medical information.
- **Block it Out--Data Redaction:** State CIOs may encourage the use of data redaction software or tools to automatically redact or obscure personal information that could be included in documents that are available to the public via freedom of information laws.

[12] For more information about privacy legislation in individual states, please see the National Conference of States Legislatures (NCSL) privacy webpage at: <http://www.ncsl.org/programs/lis/cip/priv/privacy.htm>.

NASCIO • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com •
W :: www.nascio.org

- **Encourage Data Purging and Protect Archives:** States may routinely collect and retain more personal information than is necessary. For personal information in electronic form that is not required to be kept in accordance with record retention laws, state CIOs may consider encouraging agencies to delete or purge such information. In other instances, state agencies may retain personal information for a certain amount of time and then either take it offline or store the information in another medium such as magnetic tapes or CDs. In those instances, measures may be needed to help protect that information from compromise, including protections for the information once it is in offsite storage.
- **Beware of the Printed Word:** Personal or sensitive information also can be stored in many forms—not just electronic. The same negative implications, including identity theft, can result from the compromise of information that is held in paper form. Thus, an approach to privacy that covers all media in which personal information may be held could reduce potential privacy risks, regardless of the form in which private information is held. For example, state IT departments may print out live production databases. In this case, any personal information included in those print-outs should be shredded to avoid "dumpster divers" from retrieving and misusing that information. Another alternative is to use test data that does not contain individuals' personal information.
- **Don't Forget Data Warehouses:** Data classification efforts are an important step in protecting significant amounts of personal information from multiple agencies that are stored in data warehouses. Implementing proper data protection and security controls also are essential for protecting sensitive information in data warehouses.

Communications and Awareness:

- **Make Others Aware:** As the state technology leaders, state CIOs play an important part in educating their staff members as well as state agencies about all manner of technology issues. This is an avenue through which the CIO can point out the unique implementation issues and challenges associated with privacy protections.
- **Stay Apprised of Current Events:** Since many state CIOs have responsibility for IT security and hence must keep up with events transpiring in the field, it is also important for them to stay apprised of current events that impact privacy. Since security and privacy are closely linked, this is especially vital—what impacts privacy could very well impact security. In recent years, the compromise of sensitive personal and/or financial information through data breaches has been a high-profile issue. Many state legislatures have taken notice of this fact and have responded with data breach notification and information security laws. Several such bills are pending at the federal level and there remains a significant likelihood that legislation at the federal level would pre-empt similar state legislation.
- **Training and Awareness:** In cases where the state CIO plays a part in the development of training programs for state employees, adequate training on security measures can be a way of ensuring that state employees understand that security measures can protect citizens' private information. The theory that a chain is only as strong as its weakest link is exemplified in the state government context, since the vast majority of

employees use state IT assets on a daily basis. Hence, their understanding and compliance with IT security is paramount to maintaining the integrity of state IT systems and the information that resides within them.

V. In Summary--What CIOs Really Need to Know About Privacy

Privacy is a defining issue of the day. The discussion around privacy is evolving along with technology and the complexities of our fast-paced world. It is more important than ever to ensure that citizens' personal information, held by state government, is kept private. Citizen trust in government is a priceless commodity that is difficult to restore if betrayed, especially if a citizen has been victimized by identity theft and/or faced financial consequences as a result of a privacy compromise. However, protecting citizen privacy can be a particularly daunting challenge for the public sector, since it is faced with citizens' expectations of openness and transparency. After all, effective democracies are built on those principles. The rapid pace with which technology is evolving coupled with expanding information sharing efforts across all levels of government have also contributed to this challenge. Yet, the legal and regulatory framework for privacy as well as commonly accepted business practices to protect privacy have failed to keep pace with technology's evolution. This has resulted in countless data breaches and privacy compromises in both the public and private sectors. Surveys also indicate that citizen trust in government's ability to maintain the privacy of their personal information is relatively low.

Within this context, the state CIO likely deals with the implementation and management of privacy issues as they relate to a variety of projects and initiatives, including homeland security, emergency management, IT security, consolidation, electronic health records, and REAL ID Act implementation. Major areas in which a state CIO may encounter privacy issues include:

- Governance
- Enterprise architecture
- Policy
- Business processes and practices
- State and federal legal regulations
- Security and data protection and handling
- Communications with stakeholders and the raising of awareness.

In these areas, a state CIO may find it necessary to identify and address privacy issues. For example, in the context of governance or enterprise architecture, the state CIO may have the opportunity to create or participate in a privacy council or committee. This brief lists many ways in which the state CIO may address privacy issues that arise. Which avenues a state CIO pursues will depend on a state's unique environment. However, through the state CIOs' collective efforts, citizens' confidence in state government to protect their personal information can be maintained and even enhanced.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com •
W :: www.nascio.org

VI. Appendix--Additional Resources

NASCIO Privacy Committee Research Briefs:

The Research Briefs below, produced by the 2004 and 2005 Privacy Committee, are available along with other NASCIO Research Briefs at:
http://www.nascio.org/nascioCommittees/privacy/#publications.

"The Year of Working Dangerously: The Privacy Implications of Wireless in the State Workplace—Part I" (August 2005) [identifies the privacy implications of wireless technologies in the state workplace]

"The Year of Working Dangerously: The Privacy Implications of Wireless in the State Workplace—Part II" (September 2005) [provides privacy policy and security measures to help states address the potential privacy implications of wireless technologies]

"TLK2UL8R: The Privacy Implications of Instant and Text Messaging Technologies in State Government" (May 2005) [Note: TLK2UL8R is a text messaging abbreviation for "Talk to you later"]

"Welcome to the Jungle: The State Privacy Implications of Spam, Phishing and Spyware" (February 2005)

"Who Are You? I Really Wanna Know: E-Authentication and its Privacy Implications" (December 2004)

"Think Before You Dig: The Privacy Implications of Data Mining & Aggregation" (September 2004)

Other Privacy Resources:

"Protecting Privacy in Integrated Justice Systems," the National Governors Association (NGA), April 2006, http://www.nga.org/portal/site/nga.

National Conference of State Legislatures (NCSL), Privacy Resources Webpage, http://www.ncsl.org/programs/lis/cip/priv/privacy.htm.

National Association of Attorneys General (NAAG), Consumer Protection Webpage (scroll down to "Privacy"), http://www.naag.org/issues/issue-consumer.php.

National Electronic Commerce Coordinating Council (NECCC), Whitepapers, http://www.ec3.org/Pubs/PubWGPapersYr.htm.

Global Privacy and Information Quality Working Group, http://www.iir.com/global/GPIQWG.htm.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com •
W :: www.nascio.org

International Association of Privacy Professionals (IAPP), www.privacyassociation.org.

Federal Trade Commission (FTC), Privacy Initiatives, http://www.ftc.gov/privacy/index.html.

California Office of Privacy Protection, http://www.privacy.ca.gov/.

NAS**CIO** • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com •
W :: www.nascio.org