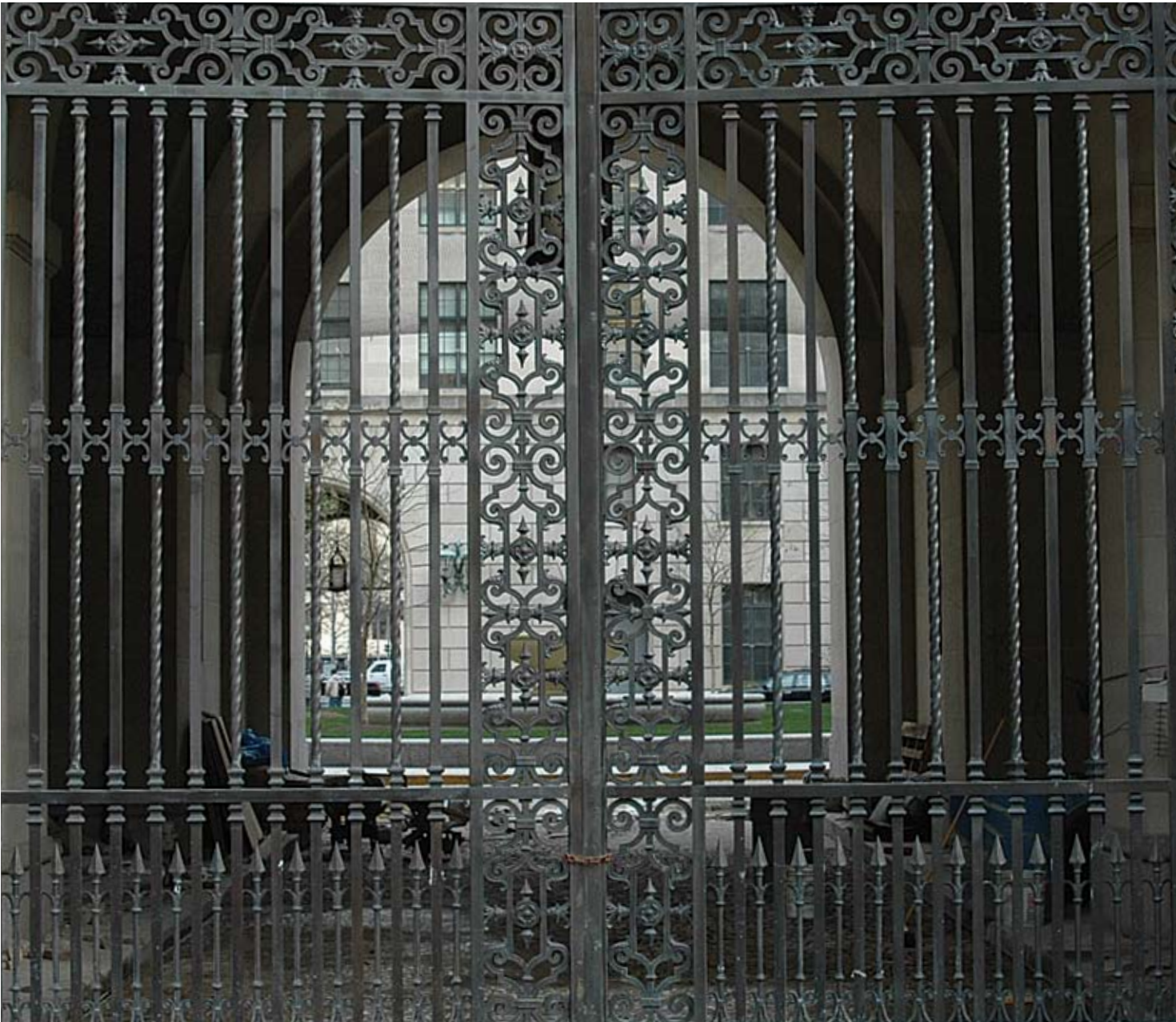


Guarding Privacy in the Federal Government: A Holistic Approach*



*connectedthinking

Interviews

Eight in-depth interviews with privacy experts were conducted in conjunction with this paper. In particular, we would like to thank the following “on the record” interviewees:

Emily Andrew
Acting Chief Privacy Officer
U.S. Postal Service

Maya Bernstein
Senior Advisor, Privacy Policy
U.S. Department of Health and Human Services

Ruth Hill Bro
Partner
Baker & McKenzie

Linda Koontz
Director of Information Management Issues
Government Accountability Office

Ari Schwartz
Deputy Director
Center for Democracy and Technology

Barbra Symonds
Director of Privacy and Information Protection
Internal Revenue Service

Hugo Teufel, III
Chief Privacy Officer
U.S. Department of Homeland Security

Steve Yonkers
Privacy Officer
U.S. Department of Homeland Security/US-VISIT

The Federal Government has records on virtually everyone.

Introduction

Pressure for the Federal Government to protect the personal data and privacy of the American public is stronger than ever. The likelihood of privacy breaches occurring has increased with the enhanced portability of data on laptops, flash drives, cell phones, and other mobile devices. Missteps in information security now have severe ramifications, including damage to public trust and the high cost of an often lengthy recovery period. Stringent privacy protection regulations continue to evolve, requiring that government agencies implement agile, robust privacy programs that not only ensure immediate compliance, but also anticipate the challenges ahead. As a result, senior executives at federal agencies are now wrestling with how to design and effectively implement comprehensive, strategic privacy programs.

PricewaterhouseCoopers' Federal practice, along with the Economist Intelligence Unit (EIU), recently examined the Federal Government's progress in implementing privacy programs. Four common themes emerged from eight interviews with Federal Government officials and privacy experts:

- Privacy protection should be one of the primary goals of an agency and must be integrated into all aspects of the organization. Robust privacy practices should be viewed as mission facilitators rather than organizational roadblocks.
- Three of the key components of a comprehensive privacy program include: an assessment of existing data flows and protections; the implementation of policies, procedures and controls linked to regulations; and the use of clearly-defined, relevant metrics to monitor program success.
- Mapping data throughout its lifecycle is crucial. Agencies should know what Personally Identifiable Information (PII) is being collected, how it is being used, and who is using it. Storage, access, and deletion of data must be taken into account, and the risks involved in all steps of the lifecycle must be identified and mitigated.
- A culture of protecting personal data is imperative. For such a culture to flourish, it must have strong support from the top, along with buy-in from management at all levels of the organization; a dedicated, independent Chief Privacy Officer (CPO); cooperation across IT, legal, and day-to-day operational support; and agency-wide privacy training and education.

Developing such a comprehensive privacy program and fostering a supportive culture requires that government agencies take a holistic view of the issues and challenges facing them, rather than employing a checklist approach to meeting regulatory requirements “It’s not just about doing the ‘paper exercise’ of a privacy impact assessment,” says Julie Nethery, Privacy Lead for PricewaterhouseCoopers’ Federal practice. “Privacy is a strategic capability for meeting the mission of federal agencies.” (See sidebar: *Privacy as a strategic enabler*). Strong privacy programs go well beyond keeping agencies out of the papers and the courtrooms. They are key to building and maintaining public trust. And they protect the most fundamental principles and liberties on which the government itself was founded.

Privacy as a strategic enabler—PwC

Government agencies must take a strategic, holistic approach to designing effective privacy programs by developing a privacy framework that offers consistent operating guidance throughout the agency. Collaboration across the agency is key in designing a realistic, implementable privacy framework and a successful, consistent privacy program.

According to PricewaterhouseCoopers’ Nethery, privacy should be periodically assessed against the privacy framework at the department level as well as at the various offices, bureaus, directorates, etc., to ensure the privacy program is functioning as intended. Initial assessments may include questions such as:

- How is the privacy function organized?
- What practices are in place?
- How effective is the training program, compliance laws, OMB mandates, and how often are privacy practices audited?

Once an initial assessment has been completed, a road map will help steer the agency in the right direction for meeting privacy requirements. A privacy road map might, for example, move from creating a privacy roles and responsibilities matrix to designing

and delivering a training program to developing a robust privacy compliance program.

At a more tactical level, privacy should be an explicit part of systems and programs development at inception. “As we learned when security became increasingly important, it is more difficult, and often more costly, to implement requirements after a system has been built or a program established. It is important to address privacy requirements from the beginning,” says Nethery. “Privacy efforts may meet resistance, due to potentially increasing the cost and reducing the speed of systems development. While these concerns are legitimate, the need to comply with regulations and protect the organization from privacy breaches with measures appropriate to the data the agency holds is arguably more important.”

Key Takeaways:

- Agencies should develop the privacy framework as a management tool;
- Periodic assessments are important in evaluating the success of the privacy program; and
- It is more costly to build privacy in as an afterthought.

Failure to execute effective privacy protection measures can be expensive. Fines may be levied, expensive remunerations made, funding lost, and reputations damaged.

Government: A Higher Standard of Protection

The Federal Government is uniquely motivated to protect the privacy of citizens and legal permanent residents. Key drivers include:

- The ethical obligation to protect large amounts of the American public's personal information;
- The significant cost of mistakes; and
- The need to adhere to federal regulations.

Unlike private sector companies such as credit agencies, advertisers and list brokers who have the luxury of touting privacy efforts as a competitive advantage, the Federal Government has records on virtually everyone and is expected to safeguard this information with the utmost care. The Internal Revenue Service (IRS) received 133 million tax returns from individuals in 2005. An estimated 96 percent of American workers (163 million people) are covered by Social Security benefits, while 63 million Americans potentially have some claim on services from the Department of Veterans Affairs (VA). The United States Postal Service

(USPS) processes change-of-address records for every person who moves. Other agencies collect information pertaining to political campaign contributions, border crossings, Medicare payments, as well as the personal information made available under expanded provisions of the USA PATRIOT Act. There is a record associated with every point at which the Federal Government touches the lives of its citizens, and even non-citizens (e.g. legal permanent residents and visitors) comprised of information about the individual and event.

The Federal Government's handling of PII draws particular scrutiny and therefore demands special vigilance. This is the case whether access to PII is business-driven—such as the Department of Homeland Security's (DHS) requests for increased data sharing—or the result of a breach due to unexpected behavior, such as IRS employees peeking at celebrity tax returns or computer theft at the VA.

Failure to execute effective privacy protection measures can be expensive. Fines may be levied,

expensive remunerations made, funding lost, and reputations damaged as the public learns the full extent of an information security or privacy breach. When a laptop and hard drive was stolen from the VA in May 2006, for example, the agency was estimated to have incurred a loss of \$160 million to cover free credit monitoring for affected veterans and another \$25 million to set up a call center and notify veterans of the possible breach. In addition, a coalition of veterans groups sought damages from the VA of \$1,000 for any of the 26.5 million veterans shown to be harmed by the breach.¹ The ultimate cost would have been drastically higher had the devices not been recovered or had there been any apparent misuse of the personal data stored on them.

Such security breaches and process failures often spur new, increasingly-stringent rules, adding to existing complex regulations and guidelines from Congress, the President, agencies such as the Office of Management and Budget (OMB), and States.

¹ Christopher Lee and Zachary Goldfarb, "Stolen VA Laptop and Hard Drive Recovered," The Washington Post, June 30, 2006.

A Unique Set of Challenges

Government agencies face unique privacy challenges, some analogous to, but many distinctly different from those confronted by private sector companies. The requirements to safeguard the privacy of personal data result in high levels of agency scrutiny and oversight. If an agency receives negative attention from Congress or a public citation for privacy violations, the triple threat of lengthy hearings, costly penalties, and a loss of federal funding looms large. “To achieve success, you need to think about privacy early, and you need to think about privacy often,” says Hugo Teufel III, CPO of DHS.

Paired with the damaging financial consequences of a privacy breach, the loss of public trust can be devastating. The American public entrusts the Federal Government with private information and expects strict safeguarding and controls. Accordingly, the Federal Government is expected to follow stringent guidelines in protecting the personal data it collects. “If the government doesn’t have privacy protections in place, the impact from an abuse is more extreme,” says Ari Schwartz, Deputy Director of the Center for Democracy and Technology (CDT), a non-profit public interest organization focused on civil liberties and privacy protections.

The Privacy Act of 1974 serves as the foundation for U.S. Government privacy protection policies. The original requirements of the Privacy Act continue to be expanded by laws from Congress and orders from the Executive Branch (e.g. guidance from OMB and the Privacy and Civil Liberties Oversight Board). This regulatory expansion includes the requirement for federal agencies to implement more thorough privacy programs by setting firm policies and procedures, tracking data flows of PII, implementing training programs, and designating CPOs. (See sidebar: *Privacy regulations: Facing the challenge of complex rules.*) Government agencies have little choice but to comply with this constantly changing patchwork of rules, often on short notice, and with limited and sometimes unbudgeted resources. And they are routinely monitored for compliance. For example, US-VISIT, a DHS border security program dealing with the entry and exit of visitors to the U.S., has received at least ten publicly-reported audits by DHS’s Office of Inspector General (OIG), the Government Accountability Office (GAO), and OMB since US-VISIT’s inception in January 2004.

Despite current privacy requirements, however, implementation has been uneven and few federal agencies have established cohesive privacy programs. Some have a program in name, but not in practice. Although OMB directed every agency to designate a Senior Agency Official to be responsible for privacy issues, often the Chief Information Officer (CIO) or someone in another role is simply assigned the additional title of CPO.² At a large agency, this can mean that privacy will not get the full attention it deserves.

Such complex regulatory demands require the Federal Government to take a measured approach to implementing robust privacy programs and achieving compliance across its many agencies. While the IRS, USPS, and DHS are usually cited as privacy leaders in the Federal Government, every agency can improve its privacy efforts. “We will see privacy become more of a priority,” says Linda Koontz, Director of Information Management Issues at the GAO.

² OMB Memorandum 05-08: Designation of Senior Agency Officials for Privacy, asks each agency to “identify to OMB the senior official who has the overall agency-wide responsibility for information privacy issues.” The Consolidated Appropriations Act of 2005, §522a, also contained language which required a Chief Privacy Officer to be designated.

Privacy regulations: Facing the challenge of complex rules

The Federal Government is subject to a number of laws and regulations governing privacy. Agencies must prioritize and harmonize the many mandates from OMB, Congress, and other federal authorities. “Privacy laws are a very complex spider web. Many times, we are looking from one law to another to make sure we are compliant with both and to determine if there is any conflict,” says Barbra Symonds, Director of Privacy and Information Protection at the IRS.

Applicable rules include generating a SORN under the Privacy Act of 1974; conducting PIAs under the E-Government Act of 2002; designating senior officials responsible for privacy and/or CPOs and establishing privacy and data protection policies and training under the Consolidated Appropriations Act of 2005. Freedom of Information Act rules must also be understood and addressed.

Some agencies have privacy-related rules pertaining directly to their specific circumstances, such as the Taxpayer Browsing Protection Act for the IRS, which seeks to limit unauthorized access to information. Additionally, there is the impending impact of new legislation from Congress.

New rules often emerge in reaction to breaches. In 2006, the OMB responded to the highly-publicized theft of a laptop and hard drive from the VA with memos that mandated more stringent security mechanisms and required breaches involving PII to be reported to the US-CERT within one hour.

The efforts of the USPS to meet the year-end deadline for a new e-discovery rule illustrate the difficulties agencies face in meeting privacy requirements.

Under the e-discovery rule, agencies must be able to identify the electronic location of data regarding any litigation and provide it to lawyers. To do this the USPS must convert from its current manual system and examine where all its data is located—a difficult task, since many of its systems cannot communicate with each other. “We’re looking at and reviewing various applications on how we can do this in a more efficient way,” says Emily Andrew, acting CPO at the USPS.

Key Takeaways:

- Privacy requirements are likely to increase on an ad-hoc basis and become even more complex; and
- Systems modernization can play a role in privacy compliance.

“Privacy has to be baked
into the system.”

Maya Bernstein, Senior Advisor,
Privacy Policy U.S. Department of Health
and Human Services (HHS)

Implementing an Effective Program

To achieve success with a privacy program, agencies must be proactive and dedicated to ensuring that privacy is built into its practices and systems at every step. PwC has found that organizations are most successful when they take a strategic, holistic approach to designing privacy programs, beginning with the creation of an overarching privacy framework. With the support of such a framework—a blueprint for what the agency is trying to accomplish—an effective privacy program illustrates a strong commitment to the protection of privacy by managing risk, rather than taking a checklist approach to regulation.

The privacy framework should define the underlying principles that guide

the privacy program and support the agency’s mission. It should be integrated across agency activities—permeating the organization through the implementation of policies, procedures, and functional activities—and perceived as a means for an agency to achieve its mission, rather than a checklist of inconvenient requirements. “I try to promote that you’re able to be more successful with achieving your goals and your mission by having the right privacy controls and assurances in place,” says Symonds of the IRS.

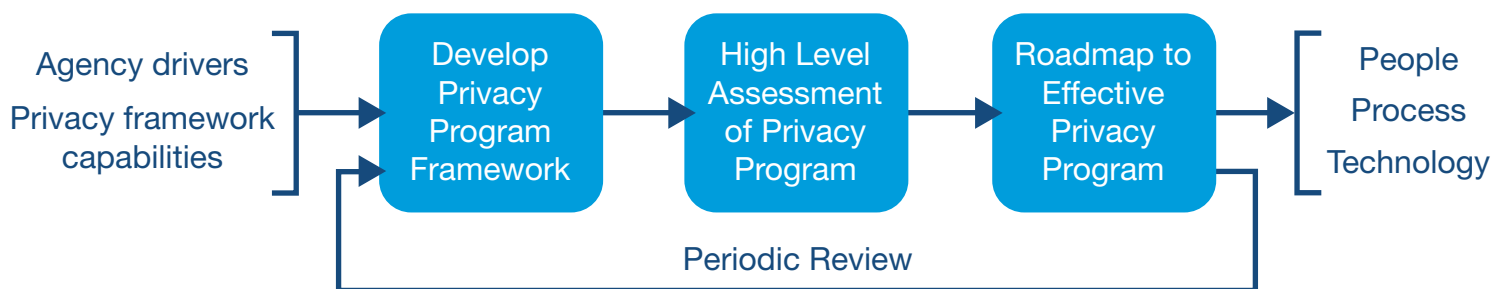
Creating a privacy framework to support the agency’s privacy program is integral to formalizing the program, as it lends new initiatives and internal policies the credence their

successful implementation requires. A privacy framework that supports the overarching mission of a privacy program will generate an overall understanding and acceptance of the importance of privacy protection.

A well-founded privacy program includes the following key activities:

- Establishing privacy policy;
- Implementing procedures and controls;
- Analyzing the data life cycle; and
- Continuously evaluating program performance and implementing targeted programmatic improvements.

Developing & Managing Privacy Programs



Establishing privacy policy. It is essential to devise clear privacy policies agency-wide, and if necessary additional supporting policies at the component level. An overall privacy policy should define how PII will be handled by the agency. Privacy policy should be used as a set of guidelines for all agency and component activities. “We have to set our people up to succeed and not fail,” says Steve Yonkers, Privacy Officer of DHS US-VISIT, which has worked hard to incorporate privacy policies from the start. (See sidebar: *DHS US-VISIT: Starting by embedding privacy.*)

Policies must be reasonable, easy-to-follow, and widely applicable across a range of duties and activities. To ensure policies are pertinent and useful, and can be incorporated into activities such as system development, PwC recommends developing policies that are relevant, yet broad enough to apply to the wide variety of activities each agency performs. Supporting procedures and controls should be developed for specific functions and technologies as needed throughout the organization (See section: *Implementing procedures and controls*, page 12 middle column).

Policies should ensure privacy is considered in the design phase of any new program or system to avoid the delay and extra cost of retro-fitting. “Privacy has to be baked into the system,” says Maya Bernstein, Senior Advisor, Privacy Policy U.S. Department of Health and Human Services (HHS). To promote early consideration of privacy concerns, it is important to include privacy activities in the systems development life cycle and the change management process. Too often, however, this is not the case, and agencies must then take steps

DHS US-VISIT—Starting by embedding privacy

The US-VISIT program of the Department of Homeland Security had a privacy program in place prior to the agency beginning operations on January 5, 2004. The program set policies around information it would gather and defined rules for PII. It also posted required policy and SORNs and conducted and posted its PIAs before the program started. “Privacy was included from the very inception of the program itself,” says Steve Yonkers, Privacy Officer of DHS US-VISIT.

On all of its projects, US-VISIT uses integrated project teams to help design new systems. The CPO or representatives from his team participate regularly in planning and development meetings to help identify risks early. They are part of the clearance and approval process with sign-off authority. “We don’t wait until we get a document to start reviewing it. We are there when it is being crafted

in the first place. By the time it gets to clearance, we should be able to easily and quickly approve it,” says Yonkers.

US-VISIT additionally works to ensure privacy measures are being followed. “That means you are going to have to go out and talk to people. You’re going to have to get their feedback on whether these rules are working for them,” says Yonkers. (See *Evaluating program performance*)

Setting privacy parameters around data sharing has been a key consideration for US-VISIT. Many other agencies want access to its database, which contains biometric and biographical information for over 60 million foreign nationals. Sharing this information within DHS for immigration, law enforcement, and national security purposes was under US-VISIT’s original purview. However, a decision had to be made early on about access limits

for the State Department, the Federal Bureau of Investigation (FBI), and State and Local law enforcement officers. Yonkers says DHS’ decision was based on the principle that “You only share the minimum amount of information necessary for that office or individual to perform their job.”

Key Takeaways:

- It is possible to build privacy into a new program, even when it is in the conceptual phases;
- Integrating privacy personnel speeds up the process of implementing a new program;
- The effectiveness of the program must be assessed; and
- Careful decisions must be made around sharing data.

to retro-fit privacy requirements into operations, programs, and systems, which can be difficult and costly.

Some areas require specialized policy, due to the proliferation of data through growing numbers of interagency data requests, as well as the increased ease of data transmission and the ability to store data outside of systems. Third-party data sharing is one example of an area in which specific privacy protection policies might be implemented. To facilitate data sharing, agreements such as Memorandums of Understanding (MOU) must be signed to establish that the proper authorizations, notifications and controls are in place.

Other related policies might ensure that the parties sharing data follow approved data protection practices. Additionally, new technologies and techniques (e.g. radio frequency identification [RFID], data mining) that offer new avenues for the abuse of privacy must be carefully considered and addressed, as well as agency use of private databases, commercial data resellers, and third-party contractors.

Homeland Security Presidential Directive 12 (HSPD-12) is one such instance where PwC believes specialized policy attention is required. HSPD-12 mandates the distribution of new federal employee badges with enhanced identification

and authorization information. Privacy policy experts from multiple agencies have been debating what data to encode in the design of the new badges. Agencies are clarifying why they are collecting the information, deciding on the scope of notification, and—since the badges will include biometric information and possibly RFID chips, fingerprints and potentially additional PII—considering what should be done if the cards should fall into the wrong hands. The card data may easily be used for purposes other than those originally intended. For example, the embedded RFID technology may also be used to track the movements and attendance of employees without their consent.

Although headlines focus on hackers and thieves, most breaches arise from simple employee negligence. Laptops are lost or stolen from cars; information is accidentally posted on an agency's web site; data is stored in applications and forms outside of agency systems, typically lacking minimum security requirements; or paper files are discarded without shredding. Therefore, policies should not only address processes and technology, but also define appropriate employee behaviors, paying special attention to areas that may not be intuitive to everyone. Ruth Hill Bro, a Partner with U.S. law firm Baker & McKenzie's Privacy Practice, lists some simple prevention policies:

- Assume emails will be forwarded to individuals not listed on the original distribution list;
- Avoid reusing paper;
- Leave PII at the office;
- Do not share PII;
- Do not work with sensitive data in public spaces;
- Avoid careless talk in elevators or on cell phones; and
- Read and adhere to your employer's IT and data policies.

Implementing procedures and controls. PwC has found that sufficient processes, procedures, controls and assurances must be in place to support privacy policies, especially when it comes to high priority or special care areas. Standardization of such procedures can help ensure consistency in how privacy is addressed throughout organizations. For example, DHS requires that Privacy Impact Assessments (PIA) be completed using the same template across the Department. This ensures each unit follows the same procedures in evaluating privacy for each of its programs, systems, and, when required, proposed rules. Procedures and controls, like policies, should be easy to follow, meet legal guidelines and work in tandem with security requirements. Privacy procedures and controls should be both technical (e.g., requiring multiple passwords or encrypting information sent to and from browsers) and process-oriented (e.g., limiting system access or simply avoiding wholesale data collection).

Procedures for responding to breaches, for example, should guide agencies in taking measured action as soon as an issue arises. An agency may require that lost handheld devices be reported immediately in order to send "kill pills" that erase all

data as quickly as possible. Proper record retention and destruction procedures are also high priority among government agencies and have been a particular focus of the USPS for the last several years. (See sidebar: *Streamlining records management policies at the USPS.*)

Privacy procedures should also govern information gathering, streamlining how data is gathered and used across the organization while maintaining the integrity and privacy of the data collected. For example, the IRS collects data from a business unit or IT system once and then leverages it internally multiple times, decreasing information replication or redundancy for security and privacy purposes. This helps the agency more efficiently meet both its business needs and privacy requirements.

Analyzing the data life cycle. With policy and regulations in mind, PII data flows should be mapped throughout the entire agency, and updated for each project, to present a clear picture of what information is being gathered, stored, and shared, as well as how it is used and when it is deleted. "A person leaves and a database disappears or people get rid of a computer and they aren't aware that there is sensitive information on it," says the CDT's Schwartz.

To mitigate the risk of privacy violations, agencies must understand how and by whom these tasks are executed and how the data is protected at each step. This includes analyzing the potential for inadvertent data transmission and identifying areas vulnerable to breaches. “The number one challenge is getting a complete picture about personal data,” says Bro of Baker & McKenzie. “It is a continual process. Laws change. Situations arise. You need to use data in a new way.”

Technology must be continually evaluated to ensure that it supports privacy protection and is not a source for potential privacy breaches. Vigilant checks must be performed to assure PII is secure system wide. For web sites, this means conducting a privacy inventory of elements such as domains linked to and from a web site, cookies and web beacons, and forms on web sites used to collect data.

Required privacy documentation, such as SORNs and PIAs, are very good tools for understanding how data is used and protected, as well as if it is being used for its intended purpose. Under the Privacy Act, agencies must

Streamlining records management policies at the USPS

A big focus of the USPS—the first federal agency to name a CPO in 2000—is on streamlining and standardizing its records management and retention policies. “Employees will know where to go to get the information that they need, and it’ll be consistent. That’s important because before, policies and procedures were located in various publications and that gets confusing and very hard to manage,” says Emily Andrew, acting CPO at the USPS.

The project, which began two years ago, involves updating existing policies and consolidating them into one process. The 12-member privacy team has been working closely with the businesses to determine appropriate information retention periods and considering ways to automatically dispose of information. “The goal is to have a one-stop shop for our employees so that they can go to one location to get information on record retention, storage, and disposal,” says Andrew.

Other important USPS projects include examining its Privacy Act systems of records and data flows to improve

efficiency and privacy, and limiting access to information on the USPS’s 250 million customers to the minimum data required to do a particular job. This is a big challenge given that the USPS has 600,000 employees in 38,000 retail units and over 200,000 employees have access to data online.

The USPS believes privacy requires constant vigilance. “We have our policies in place. We have implemented those policies. We’ve done training. And we are now doing a lot of compliance. As technology changes, we are continually looking at our policies and changing and updating them. The cycle again starts with implementation, then training, compliance and so forth,” says Andrew.

Key Takeaways:

- Agencies should centralize privacy policies, tools, and information for ease of accessibility; and
- Data retention parameters are an important part of privacy protection.

file a SORN for each new system or amendment it proposes, detailing what data is being gathered and how it will be used. PIAs are analysis tools to aid in discussing and documenting privacy provisions for programs, systems, and for some agencies, proposed rules. At a minimum, PIAs must describe the data collected and why, how the agency will use the information, who the agency will share the information with, notice given to individuals or opportunities for consent regarding intended collection and how it is shared, how the information is secured, and whether or not a SORN is being created. To be more effective, PIAs should also capture information such as personal data flows for each system, data management and protection mechanisms, processes used to determine privacy risks, and detailed risk mitigation measures. The most useful PIAs are completed at the concept stage, posted at program inception to elicit comments, and updated whenever there are major changes or subsequent modifications. All notifications should be clear and concise, accurately describe data usage, and address any shortfalls revealed in the assessment process. “The challenge is that you have to stick to what you originally said

you were going to do,” says Koontz at the GAO.

When building and deploying IT systems, for example, the IRS conducts PIAs at the concept stage and then updates them throughout the milestone review process. While the CPO lacks a full veto, she can vote against advancing to a new stage based on privacy vulnerabilities and the business units’ ability to mitigate those risks. “We are getting a larger weight in highlighting our concerns and proposing risk mitigation strategies,” says Symonds, of the IRS.

Evaluating program performance.

Measuring performance must go beyond auditing against OMB and Congressional reporting requirements. While auditing for compliance with the privacy requirements established by various privacy laws and OMB memorandums is important, government agencies must take a more strategic approach to measuring the operational success of their privacy programs. Ensuring policies, procedures and controls are working is crucial to gauging the success of any program. Effective performance management will determine whether

employees are behaving as required and systems and controls are operating as intended and it may bring to light areas where additional policy and controls are necessary.

Compliance efforts are more effective if there is a process for regularly monitoring and reporting the status of privacy initiatives. Tracking mechanisms to identify deficiencies and prioritize resources for remediation should be built into the privacy program. But identifying the shortcomings in policies and procedures is not enough, and agencies must go further to develop remediation and benchmarking processes that support continuous improvement.

The USPS, for instance, has found that employee feedback, outside expert input, and benchmarking all help gauge progress. By getting involved in many different work groups and associations, the USPS privacy team seeks to learn from the experience of others. “It’s critical that we turn for advice both internally and externally to understand what’s going on both in the government and industry,” says Emily Andrew, Acting CPO at the USPS.

Embedding a Privacy Culture

Moving from a “checklist mentality” to a strategic approach to privacy often requires a complete cultural transformation. A culture of privacy appreciation drives success, and privacy programs thrive when agencies maintain:

- A culture of privacy protection and aligned “tone at the top”;
- Strong support from the top, a committed CPO, and program buy-in across the organization;
- Program and policy integration across disciplines;
- Effective communication and training; and
- Well-defined privacy roles for which employees are held accountable.

Success calls for top-down support, cooperation across disciplines and comprehensive training. “The biggest challenge in government is changing the culture to move from paperwork execution into more meaningful risk management,” says GAO’s Koontz.

Tone at the top, buy-in, and a strong CPO. Strong support from senior management spurs buy-in at all levels and provides the CPO with the authority to fulfill executive requirements. “Without that executive champion to say privacy matters and will be enforced and respected, it can be difficult to get business lines to comply,” says Symonds of the IRS.

Privacy officials should be involved in senior-level policy decisions and be considered senior advisors and partners in data protection and privacy compliance. The CPO should be part of the investment-management process for considering funding for new IT projects so that privacy concerns are addressed from the start. At the same time, the CPO must have the independence and clout to report breaches and to inform leadership, including the agency head, of privacy concerns. “You’re an advisor to the Secretary. You have to provide an objective look at what the department is doing. And you’ve got your basic good-government tasks that you have to get accomplished,” says Teufel of DHS, for which privacy is a leading

concern. (See sidebar: *Grappling with a privacy imperative at DHS.*)

Integration across disciplines. Within privacy programs, responsibilities often overlap, budgets are limited, and coordination across skills and job areas is challenging. Given the many facets of privacy programs, working closely with colleagues in IT, legal, security and day-to-day management is a core function of an effective privacy group. “We work with all our stakeholders very early in the process as they’re building their various applications,” says Andrew from the USPS. To encourage cross-discipline cooperation, the USPS has set up a privacy board comprised of representatives from key functional areas such as IT, marketing, legal, communications, human resources, government relations, and inspection services. Meeting at least quarterly, the board shares insights and helps vet privacy initiatives as they are being developed. This collaboration promotes awareness within the agency. Now, employees use the Privacy Office as the source for advice for privacy concerns or issues.

Grappling with a privacy imperative at DHS

Perhaps no other agency is more affected by privacy requirements than DHS as the Department uses personal data in the war on terror. Every day, DHS weighs the right to privacy against the need for national security. Additionally, there is increased pressure on DHS and its interpretation of privacy rules due to the fact that other agencies use DHS as a model for governing privacy.

Congress statutorily mandated a CPO at DHS, which underscores the importance it places on privacy. Hugo Teufel, who became DHS CPO in July 2006, will soon have 16 full-time employees and 12 contractors on his Privacy Office staff. "Privacy absolutely is a priority here," says Teufel.

Having a statutory role gives Teufel increased authority in implementing privacy controls at DHS. Since he reports directly to the head of the agency and works closely with DHS leaders, he is heard immediately when privacy issues arise. Teufel's

circle of colleagues includes the Deputy Secretary, the General Counsel, the Inspector General, the Assistant Director of Policy, the CIO, and other privacy officers at the various component groups within DHS. "Communication across these disciplines is key," he says.

One of Teufel's primary responsibilities is to advise senior leadership on the perception, liabilities, and impact of programs and processes. The DHS Privacy Office has an unwritten but well known code of addressing privacy "early and often" in working with its components and programs. Teufel and his staff work with senior executives to examine the legal basis and authorization for various items on DHS's agenda in the early phases of conception to ensure they fall within the boundaries of privacy rules.

One of Teufel's initial priorities is to streamline processes so requirements such as PIAs do not languish. He has begun examining requests coming into

the Privacy Office and how they are handled. He is planning to implement processes to handle higher workloads with rapid responses to any breaches.

Teufel's privacy team is also studying the privacy ramifications of new technology, such as the use of radio frequency identification (RFID) in ID cards and passports. "It is critical that we keep track of the latest technology that might be used to find our adversaries, and that we make sure it is used and developed in a way that does not infringe upon our privacy interests," says Teufel.

Key Takeaways:

- The agency's mission should include and influence privacy practices;
- Streamlining major processes will make meeting privacy requirements more efficient; and
- New technologies should be carefully evaluated for privacy impact before implementing them.

“We’re at the point now where people come to us as opposed to us having to always reach out,” says Andrew.

HHS has also taken a collaborative approach to privacy across its decentralized network of twelve operating units and eight agencies. Each unit is responsible for its own privacy program but each relies on four agency-wide, functionally-organized privacy groups. The HHS CIO serves as the senior privacy official and has specific authority over PIAs, e-government compliance, and systems implementation. A separate policy group oversees policy issues, while the public affairs unit publishes Privacy Act notices and responds to Freedom of Information Act (FOIA) and Privacy Act requests. The Office for Civil Rights handles enforcement of the HIPAA privacy rule. Coordination among the various privacy officers across the agency is handled via email, calls, and various internal committees. “You have to rely on your colleagues and a community of colleagues to help,” says Bernstein, of HHS.

Ongoing awareness and training.

Effective communication and training throughout the Department is imperative in achieving privacy compliance. Employees must understand their roles in protecting personal information and must know where to find help on privacy issues. “A policy is no good if it just sits on the shelf of the person who wrote it. It has to be socialized. Business owners of systems and of processes need to know their obligations in simple, plain English,” says Symonds of the IRS.

Training is a priority for many agencies. The IRS has active communication and training programs to highlight the business value of privacy. (See sidebar: *Getting the word out at the IRS.*) Both US-VISIT and the USPS offer general cross-agency training and customized training as-needed for those who may work more closely with PII. US-VISIT requires all of its employees to fulfill annual privacy training requirements and provides every employee with privacy policy and procedural guidance, handouts, emails, and Intranet postings throughout the year.

Training should be given to all employees who have access to PII to limit the risk of human error. US-VISIT recommends labeling data that is for official use only; posting guidance and notices as reminders for such repetitive tasks as data encryption; and requiring permission protocols with sign out sheets before information can leave a system. US-VISIT’s Privacy Office also conducts compliance spot checks such as walking through offices to see what personal data may be left unattended on desks.

But annual training and spot checks are not enough. A true awareness program requires regular reminders of the agency’s fundamental privacy principles and the importance of its supporting practices. Like US-VISIT, the USPS maintains a well-developed and informative website for employees about privacy matters. “Part of the job is to keep awareness alive. It is hard to change habits,” says Andrew of the USPS.

Getting the word out at the IRS

The IRS, which has the oldest government privacy program, is making a significant effort to inform employees of the importance of privacy protection and how they can promote it. “That is the whole key. You have to have an ongoing communication and awareness strategy,” says Barbra Symonds, Director of Privacy and Information Protection at the IRS.

The IRS carefully monitors and structures its marketing campaigns so employees will not ignore privacy as a result of information overload. The IRS emphasizes ways privacy can add value to the agency by helping people do their jobs better. This involves establishing clear steps for meeting privacy requirements and showing the privacy office can be relied upon for support in meeting privacy goals. The IRS additionally builds privacy policy into its technology.

At the beginning of every year, as programs are being planned, the privacy team sets out a 12-month series of privacy themes and messages to post on the Intranet, bulletin boards, posters, and wallet cards. These may include articles, privacy facts, and tips. “There

is always something fresh at least once a month to draw to the attention of the employees,” says Symonds.

Training is a critical aspect of emphasizing the privacy message. Recently the IRS brought in outside experts to revise training in order to make it more user-centric. Instead of multiple web-based courses taking 2.5 hours to complete, now there is one 45-minute umbrella course with a common theme of information protection. It includes four modules to satisfy mandatory requirements around privacy, IT security, unauthorized access to information, and disclosure. “It makes more sense in that an individual can understand all their responsibilities at one setting,” says Symonds, who also notes that the new approach saves time and money.

Key Takeaways:

- Privacy training, in conjunction with regular awareness efforts, is critical to communicating privacy messages; and
- Awareness efforts should be included in privacy program planning.

True Accountability. In order to be successful, privacy programs must be supported by building accountability for data, systems, and business processes into employee responsibilities and job reviews. Each program or function should have a designated individual owner that is responsible for privacy compliance. At HHS, for instance, responsibility for a particular program or system belongs to the sponsoring agency. “It is generally quite clear where a particular system resides or where the bottom line is,” says Bernstein of HHS. Without clear responsibilities and a motivation to uphold privacy functions, organizations risk privacy efforts falling to the side.

Building privacy into the culture of federal organizations is key to the effectiveness of privacy programs. Leadership support and engaged privacy officials, working in conjunction with representatives from key functional areas, will aid in ensuring the desired privacy practices proliferate throughout the organization. Regular training and an active awareness program will further instill the privacy culture in each employee and increase the program’s potential for success.

“What drives success is making privacy a consistent priority and realizing that it is an unending effort.”

Ari Schwartz, Deputy Director of the Center for Democracy and Technology (CDT)

Conclusion

The Federal Government will continue to face a major undertaking in protecting the wealth of PII it collects. The data is voluminous, the risk of inadvertent disclosure high, the consequences of breaches painful and costly, and the requirements challenging to implement. It is in each agency's best interest to reduce the risk of privacy breaches. No agency can afford to have its reputation tarnished by negative publicity. "One of the greatest risks of having a privacy misstep is being tried in the court of public opinion," says Baker & McKenzie's Bro. "This functions as an impetus for government agencies to take privacy seriously." The resulting erosion of public trust reaches beyond individual agency circumstances to broader political interests.

New privacy rules arise as incidents or breaches occur. As a result, privacy practices are often inconsistent in application and quality. A comprehensive and consistent approach to regulation is necessary in addressing new and increasingly important privacy protection requirements. Clearer direction may be forthcoming in future legislation.

This will likely include definitions and assessments of new technology and clarification of existing rules by OMB. Until then, agencies should adopt a privacy framework that is not only compliant with current requirements and tailored to meet its specific agency-wide needs, but forward-looking and flexible enough that new requirements will not require significant changes to their overarching privacy strategies.

Additional confusion arises regarding the role of privacy in agencies. Clarification starts with defining the role of the CPO and/or designated senior officials for privacy. Agencies must move beyond figureheads and actively engage their privacy leadership. In turn, employees at all levels of the organization must understand the reasoning behind and importance of privacy policies, and that sound privacy practices will help the organization meet its strategic objectives while securing the trust of the public. Collaboration across the organization ensures that privacy will not remain an isolated or ignored function. Addressing privacy broadly and training people in

policies, programs, vulnerabilities and acceptable practices are imperative.

Simply put, more government resources must be put to work safeguarding privacy. Doing the job right requires increased involvement, as well as time and money. Enhanced IT and security capabilities are needed, along with significant coordination with legal counsel, in implementing security strategy and privacy policies. Ideally, as government awareness of the importance of privacy grows, the resources directed to privacy protection will increase proportionately.

Reconciling a patchwork of rules, objectives and technologies will remain an on-going challenge. Since the job of privacy protection is never finished, prioritizing privacy efforts will continue to be crucial. There will always be new rules, new best practices, new technologies, and new threats and challenges. "What drives success is making privacy a consistent priority and realizing that it is an unending effort," says CDT's Schwartz.

Acknowledgements

PwC prides itself on the concept of Connected Thinking. For this paper we drew support and expertise from PwC staff with varied experience and knowledge from around our firm. A core group of PwC staff worked diligently to help produce this publication. These team members include:

Privacy subject champions

Carter Pate
PwC Managing Partner
703.918.1111

Melissa Glynn
PwC Principal
703.918.1268

Julie Nethery
PwC Federal Privacy Lead
703.918.3186

Privacy project team

Matthew Liberty
PricewaterhouseCoopers

Jessica Kirshner
PricewaterhouseCoopers

Emily Simons
PricewaterhouseCoopers

Allison Rea
Economist Intelligence Unit

Dan Armstrong
Economist Intelligence Unit

Nigel Holloway
Economist Intelligence Unit

Christopher Tepler
PricewaterhouseCoopers

