5. Security and Privacy Actions that Enable Speed in Government

By Franklin S. Reeder

Introduction

The "right to be left alone"[1] and to be "secure in our homes and our persons" are core values as old as the republic. The introduction of ever-more capable information and communications technologies has raised new challenges as to how we can protect those values, while at the same time exploiting the benefits that technological innovation offers.

The fast pace of development, deployment, and adoption of information technology[2] has created two opportunities:

- The expectation by the public that government services and information will be available 24/7 and increasingly rich in capability
- The capability to deliver information and services through multiple channels, including tapping into the creativity of individuals and companies who are seeking to develop new ways to deliver information and services, such as mobile apps

With the adoption of ever-more capable and sophisticated technologies to deliver faster, more efficient services, the federal government faces major challenges. Specifically, the government now faces two types of risks:

- The risk to the integrity of government systems and infrastructure
- Unwarranted invasions of privacy, the unintended but real consequences of greater reliance on modern technology

While some of the reforms in existing privacy and security policy and practice may require legislation, much can be done within existing legal authorities to mitigate the risk we assume in using information technology. Existing legal authorities can also reduce the potential of unwarranted intrusions upon personal privacy. Some specific, actionable recommendations are presented in this chapter to respond to both security and privacy concerns. This chapter seeks to provide a framework for thinking about and addressing these concerns.

The Internet has created the global village that was, until recently, merely a figure of speech. Social networking—YouTube, Twitter, Facebook and others—and other new technologies offer exciting opportunities for the public to connect with one another and with their government. The notion that our troops in far-off places can communicate face-to-face with their families

1. "The Right to Privacy," Samuel Warren and Louis Brandeis, *Harvard Law Review,* December 15, 1890.
2. The rapid adoption of the smartphone best illustrates this phenomenon. According to *Technology World,* "… in late 2006, the quarter before Apple announced its now-iconic iPhone, only 715,000 smart phones were sold, representing just 6 percent of U.S. mobile-phone sales by volume. … That changed when Apple's iPhone sold 1.12 million units in its first full quarter of availability. [In May 2012, six years later] Nielsen report[ed] that smart phones represent more than two-thirds of all U.S. mobile-phone sales. Nielsen also reports that 50 percent of all U.S. mobile-phone users—which equates to about 40 percent of the U.S. population—now use smart phones." In contrast, it took nearly 65 years for the telephone to reach 40 percent market penetration. (May 9, 2012).

via Skype or that wage-earners can gain immediate access to their Social Security earnings records still boggles our minds. But, as recent revelations about misuse of personal data suggest, social networking and other innovative technologies can create potential hazards for those who use them. Our growing dependence on these technologies for everything from routine financial transactions to the operation of the power grid potentially makes us more vulnerable to failures in that technology.

The leaders of federal programs that regulate and implement such technologies must preserve the trust that citizens and businesses place in government. This trust depends on protecting the privacy and security of the data and systems used to collect information, analyze and share data, make decisions, disclose, and provide access.

Privacy and security are not inherently in conflict. Indeed, properly secured systems can substantially reduce the likelihood of unauthorized disclosures of personal information or data tampering. At times, however, privacy and security can be in conflict, such as when security involves surveillance of individual actions on networks or when protecting privacy impedes security professionals from seeing information about vulnerabilities and threats that come from or through individuals. The key is to have an open debate about and clear understanding of the rules of engagement, so that citizens understand how government actions affect them.

With the adoption of ever-more capable and sophisticated technologies to deliver faster, more efficient services, the federal government faces major [security and privacy] challenges.

Overarching Principles for Responding to Security and Privacy Concerns

Before discussing the challenges of security and privacy, it is important for government to have a set of principles from which to guide its actions in responding to security and privacy concerns. Government leaders can maintain public trust and avoid needless intrusions into the personal information of the individuals with whom they are in contact by considering three simple, interrelated principles: consultation, transparency, and choice.

Principle One: Consultation. The E-Government Act of 2002 requires agencies to conduct privacy impact assessments for electronic information systems that contain identifiable personal information and make those assessments available to the public, especially when a new system is being developed or an existing system is being modified. By engaging the groups of citizens that may be affected in conducting those assessments, agencies can forestall misunderstanding about their practices and intent and even get ideas on how a system can be designed that minimizes intrusion.

Principle Two: Transparency. While the Privacy Act of 1974 has numerous notice requirements, such as notices in the Federal Register and on forms used to collect personal information, it is highly problematic whether they achieve the intended purpose. Ensuring that those notices as well as privacy policies are displayed prominently, are brief, and are in plain English can help to allay public concern. Intermediary groups (e.g., veterans' service organizations for

veterans or AARP for senior citizens) can often provide a valuable channel through which to communicate agency policies and intent and solicit feedback.

Principal Three: Choice. In some instances, there is a trade-off between privacy and convenience; e.g., if I allow a website to track my patterns or history of use, I may be able to avoid re-entering information or have options presented to me based on past behaviors. For some individuals, that is a convenience; for others, it is an intrusion. Wherever possible, offer choice.

Responding to Security Concerns

Security Concern One: Reliance on compliance-based reporting. Under current policy, lengthy checklists and outdated guidance cause agencies to waste scarce resources on measures that do little to mitigate risk. The problem is exacerbated when oversight organizations, like the inspectors general and the Government Accountability Office, produce reports on compliance against those outdated policies, wasting time and energy and incentivizing exactly the wrong behavior among agencies.

There is hard evidence that continuous monitoring, measurement, and mitigation against a defined set of high risks are far more effective in addressing real threats in an environment in which those who seek to do us harm move quickly. While agencies should still be required to report annually to OMB and Congress under the Federal Information Security Management Act of 2002 (FISMA), effective security requires that continuous monitoring, measurement, and mitigation must replace the current regime of periodic, compliance-based reporting.

> **Recommendation:** Change FISMA implementation from a compliance approach that focuses on process rather than outcomes to one of continuous monitoring. This change is the single most important action that leaders can take to improve cybersecurity. OMB should use the authority provided under the existing statute to encourage this important reform.

Security Concern Two: Responding to cybersecurity threats. The national security and intelligence communities have cybersecurity competencies that are critical to protecting civil systems such as banking and utilities. Those capabilities can and should be used without compromising civil values.

The debate on whether the federal government should impose cybersecurity standards on the private sector asks the wrong question by posing the issue as an ideological rather than a practical question.

> **Recommendation:** Congress and the Administration should revised authority structures to reflect the reality of a changing world:
> - The increased critical role in information security for the Department of Homeland Security, which did not exist at the time the underlying statutes and current OMB policies were last revised
> - The need to redefine the roles and relationship between national security and non-national security systems which would encourage sharing of cyber information across agencies

By modeling best cybersecurity practices, the federal government can lead by example and develop *de facto* standards of due diligence that will render that question moot. Leaders who adopt this approach will incentivize similar, sound action from state and local governments, businesses, and the general public.

Security Concern Three: Notification of cybersecurity threats. The government could provide notice to individuals if their machines are causing a cybersecurity problem. Due to the likelihood that external devices will be connected to the agency's information networks—i.e., those not owned and controlled by the agency—strict business rules and constant vigilance are required to ensure that those devices are not used to install malware; e.g., viruses; or steal data, and unknown devices need to be isolated.

> **Recommendation:** For public-facing systems that involve access to sensitive information, agencies could adapt a commonly used commercial technique and establish an air gap between what the public can access and sensitive agency information stores.

Security Concern Four: Assessing security risks. Government leaders need to consider the cybersecurity implications (risk and mitigation strategy) of each business decision. The currently in-vogue phrase is security "baked-in," the notion that security needs to be designed into every new piece of technology. This applies to policies as well. For example, let's look at the decision on whether, and if so under what conditions, employees should be allowed to bring their own devices into the workplace and/or connect them to the agency's networks. Such a decision will require careful consideration of how sensitive agency information will be protected from loss, tampering, or exfiltration.[3] The reflexive reaction to each new technological innovation that could pose a cyber threat is to say "no." Such an approach denies the public, both as taxpayers and as users of government services, the substantial efficiencies and other benefits from innovation.

> **Recommendation:** Government leaders should:
> - Routinely conduct a security risk assessment of each change that they are contemplating
> - Look beyond changes that they are contemplating to devices and technologies that are coming into the marketplace to consider how to exploit their potential while mitigating the risk they might impose

Responding to Privacy Concerns

With respect to information privacy, a "Code of Fair Information Practices" first articulated in 1973[4] underpins most privacy laws, including the Privacy Act of 1974.

This code, while still valid, does not address the new complexities of working at the intersection of privacy and security as information moves more quickly and the technology and potential wrongdoers become more capable.

We need a new set of guidelines for leaders to follow that respond to privacy concerns.

3. Perhaps the most dramatic example of failure to consider security implications was the theft in May 2006 of a laptop computer that contained unencrypted sensitive information on 26.5 million veterans. The database had been loaded onto the laptop for analytic purposes. Fortunately the laptop was recovered and a forensic analysis revealed no evidence that the data had been used or of identity theft. The loss and potential harm to veterans could easily have been averted by two simple policy decisions: (1) a set of business rules on the amount of live, personally identifiable data that would be permitted to be downloaded onto any portable device; and (2) firm policies requiring encryption of those data.

4. *Records, Computers and the Rights of Citizens,* Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Department of Health Education and Welfare, July 1973 [available at http://aspe.hhs.gov/datacncl/1973privacy/tocpreface-members.htm]

Privacy Concern One: Appropriate handling of personal information. As noted above, privacy and security are not inherently in conflict. Indeed, the public has a right to expect that agencies will deploy robust security measures to protect against both intentional and inadvertent compromise of their personally identifiable data. For the purposes of determining what level of security is appropriate, it may be helpful to analogize to the public health model. Most of us can protect ourselves against common threats by practicing good hygiene and preventive medicine, but at-risk populations, from the very old and very young to those who may be immune-compromised, must employ more aggressive measures.

> **Recommendation:** Agency risk analysis should inform the level of protection, detection, and mitigation, in terms of how deep to go in addressing a cybersecurity threat. Information and systems that confront high cyber risks or threats should receive more oversight to protect privacy. On the other hand, for many agencies that do not process highly sensitive personal information, following the minimum levels in relevant National Institute of Standards guidance may be sufficient.

Privacy Concern Two: Using electronic surveillance. As the nation's adversaries become more skilled in the use of advanced information technologies, protection of the nation's security increasingly entails electronic surveillance.

> **Recommendation:** The government should undertake a proper review where cyber protection requires individual surveillance consistent with law. The following guidelines are offered for such a review:
>
> - Agency head approval should be required in cases where cyber protection requires individual surveillance. In cases of multiple agency activity (e.g., the Departments of Homeland Security and Justice), activity involving the Executive Office of the President, or when exigencies require action in the moment, prior review by an independent entity such as the President's Civil Liberties Oversight Board should be required.
> - Any review should be ex ante, except in emergency cases when notice should occur as soon as possible thereafter.
> - The content of messages should be examined only in cases of high risk or threat. Much can be accomplished by constant monitoring of the pattern of traffic without looking at the content of messages.

Conclusion

The recommended actions outlined above are but steps in the continuing journey to protect our core values. Innovative uses of information and communications technology will continue to be developed. For example, how many of us anticipated the widespread use of portable devices, social networking, or new surveillance technologies? Policy makers and those who operate the engines of government need to continue to adapt both its policies and practices to protect privacy and security in a world that is not, in any sense, standing still.

Franklin S. Reeder *writes, consults and teaches on information policy issues. He formerly served as Director, Office of Administration, the White House, and served in several senior positions at the Office of Management and Budget.*