Memo #6: Privacy and Security

The introduction of information and communications technologies has raised challenges as to how we can protect privacy and security while exploiting the benefits that innovation offers. The Internet has created the global village that was, until recently, merely a figure of speech. But, as recent revelations about misuse of personal data suggest, social networking and other innovative technologies create potential hazards for those who use them. And 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.

While some of the reforms in existing policy may require legislation, much can be done with existing legal authorities to mitigate the risk we assume in using information technology while also reducing the potential unwarranted intrusions upon personal privacy. Some specific, actionable recommendations follow for both security and privacy:

With respect to security:

1. Under the current policy regime, lengthy checklists and outdated guidance cause agencies to waste scarce resources on measures that do little to mitigate risk. 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. Changing Federal Information Security Management Act (FISMA) implementation from a compliance approach that focuses on process rather than outcomes to one of continuous monitoring is the single most important action that leaders can take. We recommend that OMB use the authority provided under the existing statute to encourage this important reform.

   Moreover, the debate on whether and how the government should impose cybersecurity standards on the private sector asks the wrong questions. By modeling best practices, the government can lead by example and develop de facto standards of due diligence that will render these questions moot.

2. 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 comprising civil values. We thus recommend revisiting authority structures to reflect the reality of a changing world; namely (1) the 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, and (2) the need to redefine the roles and relationship between national security and non-national security systems, to encourage sharing of cyber information across agencies.

   With respect to information privacy, a "Code of Fair Information Practices" first articulated in 1973[1], underpins most privacy laws, including the Privacy Act of 1974. We need a new set of principles for leaders to follow that govern cases where security and privacy conflict in cyberspace, Such principles may include:

[1] *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/tocprefacemembers.htm]

- Risk analysis that informs the level of protection, detection, and mitigation– high risk/threat gets more oversight
- Notice to individuals if their machines are causing a problem
- Court review for access to electronic records
- Proper review where cyber protection requires individual surveillance consistent with law
- Examine content of messages only in cases of imminent threat
- Privacy-by-design and Privacy-enhancing security technologies should be favored in system development
- Officials with a privacy interest (e.g., agency CPOs) should be in the room during consideration of actions needed for cyber protection, not after the fact
- Correct for false positives – destroy information that should not have been tracked via mitigation
- Audits should be done to ensure accountability.