

**Testimony of Professor Peter P. Swire
Before the
White House Privacy and Civil Liberties Board**

December 5, 2006

To the Members of the Board:

To begin, my thanks to you for the opportunity to testify here today, at the first public hearing of the White House Privacy and Civil Liberties Board. I will briefly describe my background relevant to today's hearing, and then discuss a Due Diligence Checklist that I hope will be helpful to the Board as you participate in the development of government information sharing projects.

Background

I am currently the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University, and a Senior Fellow at the Center for American Progress. I live in the Washington, D.C. area. From 1999 until early 2001 I served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget. If the title had existed at that time, I would likely have been called the Chief Privacy Officer for the U.S. government, working on issues of both public- and private-sector uses of personal information.

Most relevant to today's topic, in early 2000 I was asked by the President's Chief of Staff, John Podesta, to chair a White House Working Group on how to update electronic surveillance laws for the Internet age. Among the 14 participating agencies were the major intelligence agencies and the Department of Justice. The Administration announced proposed legislation in June of 2000. Although legislation did not pass that year, the topics that we covered in our proposed legislation were essentially those included in the USA-PATRIOT Act, passed in the fall of 2001.

Since that time, much of my research and writing has been on issues at the intersection of national security, privacy, and civil liberties. For instance, my article on "The System of Foreign Intelligence Surveillance Law" is the most detailed public work on the history and practice of the Foreign Intelligence Surveillance Act. That article, and my other writings, are available through www.peterswire.net.

Privacy and Information Sharing in the War on Terrorism

Of particular relevance to this hearing today is my most recent article, "Privacy and Information Sharing in the War on Terrorism." The article was published recently in the Villanova Law Review symposium in memory of privacy scholar Richard Turkington.

The core of the article is a set of ten “due diligence” questions for assessing proposed information sharing programs. In many of my writings, I stress the crucial benefits to the government of new information technology and new information sharing programs. The emphasis in the due diligence list, however, is on the downsides of information sharing. Proponents of a program will often be optimistic about what it can achieve. The due diligence process, whether in corporate takeovers or for information sharing, is designed to highlight possible problems that may need to be addressed.

The Due Diligence Checklist, which I hope can be of use to the Board in its own review of new programs, is printed here:

Table 1: Due Diligence Checklist for a Proposed Information Sharing Program

<ol style="list-style-type: none">1. Will the proposed sharing tip off adversaries?2. Does the proposal improve security? Cost-effectively?3. Is the proposal “security theater”? How much does it provide only the appearance of security?4. Are there novel aspects to the proposed surveillance and sharing? What risks, if any, accompany these novel aspects?5. Are there relevant lessons from historical instances of abuse? What checks and balances would mitigate risks of such abuse?6. Do fairness and anti-discrimination concerns reduce the desirability of the proposed program?7. Are there ways that the proposed measure could make the security problems worse?8. What are the ramifications internationally and with other stakeholders?9. Are there additional, privacy-based harms from the proposed measure?10. Will bad publicity undermine the program?
--

(Source: Peter P. Swire, "Privacy and Information Sharing in the War Against Terrorism," 51 Villanova L. Rev. 951 (2006), available at <http://ssrn.com/abstract=948118>.)

In the time available, I will highlight two of the due diligence points.

The first question on the list is whether information sharing will tip off adversaries. Consider the example of sharing a terrorist watch list. Greater information sharing clearly helps to the extent that many border guards and other allies may use the list to catch the suspects. On the other hand, sharing information with many border guards increases the possibility that suspects will be tipped off that they are on the list, and thereby elude capture.

Much of my recent research has concerned the "Security Disclosure Model," which addresses the topic of when disclosure helps or hurts security. (The model is set forth in Peter P. Swire, "A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?," 3 J. on Telecomm. & High Tech. L. 163 (2004), available at <http://ssrn.com/abstract=531782>.) One main finding of the model is that when to do information sharing is a difficult case, and there should be no presumption either in favor of or against information sharing.

The fourth item of the list is to identify the novel aspects of a proposed program and consider whether the innovation is justified. This conservative intuition is associated with the name of Edmund Burke, who criticized many innovations of the French Revolution for their radical nature and unintended consequences. An eloquent summary of Burkean conservatism comes from supply-side economist Jude Wanniski: "[S]ociety is a vast and complicated historical product which may not be tinkered with at will like a machine; it is a repository of collective human wisdom to be regarded with reverence, and if reformed at all must be with due respect for the continuity of its traditions." In the words of philosopher and economist Friedrich Hayek, "the result of the experimentation of many generations may embody more experience than one man possesses."

The Burkean perspective is a useful corrective to the tendency to believe that "everything has changed" since 9/11. Many things have changed since the attacks, but many things have not. As a step in the due diligence for proposed programs, it is useful to identify the novel aspects of a proposed program and consider possible unintended consequences. The program should move forward if, but only if, the case for it is convincing.

In conclusion, this Due Diligence Checklist draws on my own experience in government, trying to serve our Nation by asking thoughtful and effective questions about new information sharing and other surveillance programs. The checklist is an attempt to draft a highly pragmatic way to temper the enthusiasm of proponents, and to move forward with surveillance activities only after they have been subject to thorough due diligence.