Testimony of Professor Peter P. Swire

C. William O'Neill Professor of Law
The Ohio State University

Visiting Senior Fellow
Center for American Progress

Before the
Subcommittee on Commercial and Administrative Law
and the
Subcommittee on the Constitution
of the
Judiciary Committee of the U.S. House of Representatives

Oversight Hearing on "Personal Information Acquired by the Government From Information Resellers: Is There Need for Improvement"

April 4, 2006

I thank the Committee for the invitation to testify before you today on the draft GAO Report "Privacy: Opportunities Exist for Agencies and Information Resellers to More Fully Adhere to Key Principles."

The testimony briefly describes my background and the history of today's topic. In 1974, when the Privacy Act was passed, the most important databases used by the government were developed by the government. Today, by contrast, the private sector assembles a far greater portion of the databases that are useful and relied on by government agencies. The big question is how we update our laws and practices to this new reality.

The overall theme of my testimony is that we are still early on the learning curve about how to incorporate private databases into public-sector actions. My testimony first gives some comments on the way the Report interprets the Fair Information Practices. It then makes the following principle recommendations:

1. Because agencies make such important decisions based on the data, it is essential to have accurate data and effective ways to get redress for the mistakes that inevitably occur.

2. New mechanisms of accountability are likely needed as agencies rely more heavily on non-government suppliers of data. There should be expanded use of privacy impact assessments. The government contractor provisions in S. 1789, a data-breach bill, also illustrate additional steps that may be useful.

3. Greater expertise and leadership is needed in the executive branch on privacy issues, notably including policy leadership within the Executive Office of the President. The lack of such leadership on privacy has led to significant, avoidable problems.

4. As we continue along the learning curve, it is important to merge today's discussion about privacy protection with the ongoing debates about the need for information sharing within the government. The Committee may wish to support creating a National Academy of Sciences study on privacy and information sharing, including the use of commercial data by the federal government.

Background of the Witness

I am the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University. I am also a Visiting Senior Fellow at the Center for American Progress, a think tank based here in Washington, D.C.[1]

I have written extensively on a wide range of information privacy and security issues, including as lead author of a book on U.S. and E.U. privacy law, published by the Brookings Institution in 1998. From 1999 until early 2001, I served in the U.S. Office of

Management and Budget, as the Chief Counselor for Privacy. My writings appear at www.peterswire.net.[2]

Introduction: Moving up the Learning Curve about Government Use of Commercial Databases

My overall theme today is that the GAO Report is a step along our learning curve about the government's use of commercial databases that contain personal information. This hearing continues the process of clarifying the topic, so that we can better use commercial information when that is appropriate but also avoid the risks that arise from incorrect use of personal information.

A brief look at the history helps us understand why the present use of commercial databases is so different from the past. The Privacy Act was passed in 1974 due to the new accumulations of government information about individuals. This was the mainframe era, when government agencies such as the Social Security Administration and the Internal Revenue Service had the most computerized and detailed records that existed about most Americans. The Privacy Act put limits on how information could be shared among agencies, and essentially prevented one massive database of government records from being created.

Today, by contrast, the private sector holds enormously more and more detailed computerized records than does the government about individuals in our country. Today, an ordinary laptop has more computing power than the mainframe of the 1970s. Today, our personal computers can share data at a volume unimaginable not long ago. In the private sector, many records, and especially those in the public domain, are gathered by companies that specialize in the business of re-selling that information. The private sector relies on these information resellers for many purposes, including fraud prevention, target marketing, and finding people for reasons that range from newspaper interviews to witnesses for litigation.

Because the private sector finds it useful and cost-effective to rely on information resellers, it is not surprising that government agencies would also wish to use these services in analogous settings. The GAO Report that is the subject of today's hearing demonstrates these analogous uses, such as fraud prevention and location of witnesses for litigation. The GAO Report also shows that information from resellers is used for additional purposes that are specific to the public sector, notably and apparently most often for law enforcement investigations.

To summarize the history, government agencies held the largest databases of personal information in the 1970s. Today, the largest volume of data is held in the private sector, and this hearing concerns the rules of the road for government access to those private-sector databases.

Comments on the Fair Information Practices

As the GAO Report correctly states, Fair Information Practices ("FIPs") have been used as a key basis for privacy laws and practices, both in the United States and around the world. Most prominently, the Organization for Economic Cooperation and Development in 1980 promulgated the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." During the past quarter-century, the Guidelines have remained influential in forming privacy law and policy. The precise implementation of the OECD principles has also varied considerably as privacy laws have been created for different countries, different sectors, and at different stages of technological development.

The GAO Report uses the OECD Guidelines to test current practices in federal agencies and by information resellers. In doing so, the Report differs from my understanding of the FIPs with respect to the public domain and public records.

The Report briefly mentions but then does not rely on the concept of "publicly available information." (P. 11) Information that has been published in a newspaper, put on a Web site, or otherwise made public is treated differently than information that is kept confidential in the files of a government agency or doctor's office. The idea of "minimization of use" does not apply to information that is publicly available. Instead, this is the realm of the public domain, protected by the First Amendment and the analogous free press provisions in Europe and elsewhere, where we expect and encourage intensive scrutiny and use of facts and ideas. In my reading, the Report appears to criticize agencies and resellers for failure to minimize use of data in the public domain. That criticism is not consistent with how we have written privacy laws in the United States. The Gramm-Leach-Bliley Act, for instance, only applies to "nonpublic personal information." Public personal information is generally outside the scope of privacy laws, and such public information is one significant portion of the reselling industry.

This lack of attention to the public domain undermines a key finding of the Report, that "the nature of the information reseller business is fundamentally at odds with the principles of collection limitation, data quality, purpose specification, and use limitation. These principles center on strictly limiting the collection and use of personal information." (p. 9)[3] To the extent that resellers are collecting public domain information and presenting it in more usable form, then I do not agree with the Report's conclusion that resellers are "fundamentally at odds" with the Guidelines.

What should be in public records? With that said, the important debate then shifts to what information is properly in the public domain. In particular, there is a major and complicated debate about what personal information should be included in "public records" that are released by government.

During my time at OMB, we examined exactly that question in a report about privacy and the use of personal information in bankruptcy records.[4] The key question was whether any changes should be made to the definition of "public record" as traditional paper records shifted online. The clear answer was that some changes were needed. In particular, we recommended that Social Security Numbers and bank account

numbers not be placed in online records, because of the high risk of identity theft. It didn't make sense, in our view, to have people's bank account numbers be available for easy browsing. Since that time, the Courtroom 21 Project and many state-level projects have been working on the right way to have records go online while still protecting privacy. There should be ongoing legislative attention to this definition of public records, and I am concerned that there has been little or no focus on the issue at the federal level since the bankruptcy report in January, 2001.

Beyond public records – toward framework legislation for privacy protection. Information resellers also provide personal data beyond that contained in public records or other parts of the public domain. For instance, resellers may provide so-called "credit header" information to identify individuals, and may draw on an array of private-sector sources of information to create lists for marketing, antifraud, and other purposes. There are longstanding debates about the private-sector uses of credit header and other information. I will not try to sort through those debates today.

The simple point for this discussion is that some government uses of commercial databases are quite analogous to private-sector uses. The benefits of using the data are often similar, such as to locate individuals or prevent fraud. The risks of using the data are also often similar, such as facilitating identity theft or giving individuals the feeling that they have lost control over their personal information and thus their identity.

Where public agencies are using data for the same tasks as private entities, then similar sorts of safeguards are generally appropriate in both the public and private sectors. To address these similar risks, I have begun working with a number of companies and public interest groups to see if the time has come in this country for framework legislation to protect privacy. In short, similar risks of commercial databases should be treated similarly, whether the users are in the public or private sector.

Where government is unique. On the other hand, as discussed below in connection with redress, some government uses of data are different. The government makes uniquely important decisions based on personal information, including decisions to investigate and detain people in connection with criminal activity or to prevent terrorism. Where the government is making these sorts of unique decisions, then unique measures on data accuracy and redress are likely appropriate.

<u>The Need for Data Accuracy and Effective Redress.</u>

Because of the unique importance to individuals of governmental decisions, it is especially important to have accurate data on the front end, as agencies receive personal information. It is also especially important to have an effective means of redress on the back end, to correct the mistakes that inevitably occur.

In order to assure accuracy, it likely makes sense over time for the government to test and audit the accuracy of data received from commercial resellers. Better

governmental decisions will result from improved understanding about the accuracy (or inaccuracy) of types of data.

The need for data accuracy is a crucial basis for the fair information of practice of access, as discussed in the GAO Report. The idea, familiar from the Fair Credit Reporting Act, is that individuals should have access to their records and thus be able to correct mistakes. My experience, such as in the negotiation of the Safe Harbor with Europe in 2000, is that access has also been an especially controversial component of privacy debates in the U.S. Just last week, the House Energy and Commerce Committee included a provision for consumer access to information reseller databases as part of the data breach bill, H.R. 4127. By contrast, the version of the bill passed by the House Financial Services Committee, H.R. 3997, does not contain a consumer access provision.

This hearing today cannot resolve the general issue of access. I support effective access where that is feasible, but my experience is that there should be important exceptions, such as for law enforcement investigations and some anti-fraud efforts. In those settings, the benefits of access, such as improving data accuracy, are weighed against the risks of access, which notably include tipping off criminals about the investigation or giving fraudsters access to sensitive information.

However accurate data becomes as the input for government decisions, there will inevitably be some mistakes. For programs where the government is making decisions about individuals based on commercial databases, it thus is necessary to have an *effective means of redress* for those mistakes.

Special redress measures are required in government programs because of the serious and special nature of many of the decisions made by the government. Consider the consequences in the private sector if the wrong person ends up on a target marketing list provided by a reseller. The consequence for the company is the waste of a postage stamp, and the consequence for the individual is one more advertising leaflet that gets placed in the circular file.

By contrast, a mistake by the government can be far more serious. The wrong person may be detained as part of a law enforcement or immigration proceeding. The wrong person may be singled out for secondary screening or placed onto a watch list. The Committee likely knows about the troubles that Senator Edward Kennedy and Representative John Lewis have had getting off of watch lists. Last month, Senator Ted Stevens of Alaska publicly discussed the problems confronting his wife, Catherine. A short form of Catherine, you see, gives her the same name as someone now barred from entering the country, the singer Cat Stevens.

To the extent the government increasingly relies on commercial databases to make these government decisions, there must be an opportunity for redress that matches the importance of the government actions. When the system is so hard to manage even for Senators and Congressmen, then that is a sign that something better needs to be done for all 300 million Americans.

To summarize on accuracy and redress, the importance of government decisions means that, for the purchase of information from commercial resellers, special measures are likely needed for the government sector. Accuracy that is good enough for marketing is not necessarily good enough to detain a suspect. Redress measures that get someone off that marketing list are likely not sufficient for terrorist watch lists or other government programs. Recent reports give some good guidance for how those redress mechanisms should look.[5]

Mechanisms for Accountability and the Need for White House Leadership

As the history shows, the Privacy Act was designed for a world where the largest stores of data came from government databases. Today, privacy issues in government increasingly come from databases created in the private sector. To address this new reality, the government should continue to develop mechanisms for accountability. These mechanisms include: assurance of data quality; effective means of redress; privacy impact assessments; other measures in the procurement process; and greater Executive Branch leadership on privacy.

One step that has already been taken is in the OMB guidance under the E-Government Act of 2002. This guidance recognized for the first time that Privacy Impact Assessments (PIAs) should be performed for commercial sources: "when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources." By including this assessment of commercial sources of information, the guidance did a good update of protections. The guidance then went on to state: "Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement." I think that use of a PIA may also be appropriate in the latter setting, especially where a commercial product is regularly used by the government and a large number of queries are made by the government.

The Senate Judiciary Committee has included a number of relevant provisions in its version of the proposed data breach legislation, S. 1789. Section 401 of that bill would require the General Services Administration to evaluate privacy and security issues on contracts for information of over $500,000. Section 402 would create procedures for evaluating and auditing of private-sector entities that support an agency's use of personal information. Section 403 requires a PIA before a contract is entered into for government contracting for access to private-sector databases. These provisions are quite detailed, and I have not studied them closely enough to have a view on each aspect. Taken together, however, the provisions show possible mechanisms for assessing the risks and benefits of new contracts for government purchase of personal information from the private sector.

Another component of assuring accountability is to have expertise and leadership on privacy issues within the federal government. This Committee took an important step in that direction in 2002, when it crafted the language that created the Chief Privacy

Officer for the Department of Homeland Security. This was the first time that such a privacy official had been specifically created by an Act of Congress. Having testified on the subject in that hearing in 2002, it is a particular pleasure for me to participate today with the current occupant of that position, Ms. Maureen Cooney, and to hear of the many actions the office is taking to protect privacy while also protecting our nation.

The Congress took another important step to institutionalize privacy protections when it created the Privacy and Civil Liberties Board as part of the intelligence reform law in 2004. After a lamentable delay, which lasted until this February, the members of the Board have now been nominated and confirmed. I have had the pleasure to meet with the Board's leadership, and I hope and believe the Board will play an important role in addressing privacy and civil liberties issues within the scope of its jurisdiction.

That jurisdiction is limited, however, to the intelligence community. As the GAO Report indicates, much of the current agency use of commercial databases occurs for other purposes. There is thus a notable gap of White House or inter-agency leadership on how to address the subject of today's hearing. When it comes to overall government policies for how to use commercial databases consistent with privacy, there is no policy official in the White House who has privacy as a principal concern.

I believe there should be. From my own experience in such a role, there are numerous and difficult issues that face agencies in the handling of personal information. Agencies benefit from an inter-agency structure that allows government-wide issues to be addressed in a coordinated fashion. These issues are sometimes technical and can be handled as such. These issues, however, often have a large policy component that benefits from policy leadership.

One recent example shows the need for leadership and privacy expertise from the Executive Branch. You may have seen press reports in the past two weeks that the IRS is proposing to change its rules to allow tax preparers for the first time to sell tax returns to outside parties, or even to have the outside parties release tax returns publicly. The release of tax returns would happen only with signed consent, but this consent can easily happen when a tax preparer tells the busy customer just to "sign here and here and here."

When I worked at OMB, my office reviewed proposals such as this. We would have noticed the total absence of limits on redisclosure and resale. The proposed rule would not have gone forward the way it did here. If such a mistake had happened, we would have moved quickly to correct it. Without a White House ability to spot and correct such mistakes, privacy problems will continue to be much worse than they ought to be.

Information Sharing as One Area for Further Study

Up to this point, I have focused on topics covered by the GAO report. I am concerned, however, that the report has been done in isolation from the way that many issues of government data use are being considered today. I refer to the view, voiced by

the 9/11 Commission and elsewhere, that the government must do much more "information sharing" in the wake of the September 11 attacks.

Everyone in this town knows the importance of how you frame an issue. If you have a hearing one day about "the need for information sharing," then most people will cheer and we will want to open up the spigots to those flows. If you hold another hearing the next day about "invasion of privacy and identity theft," then some of those same people might cheer and say we should stop this over-use of data.

To achieve national security and privacy, we need to bring these two discussions together. I am currently doing research on this topic. The DHS Advisory Committee on Privacy and Security recently released a document that addresses some of the same issues.[6]

My own research in this area has convinced me both of its importance and complexity. I therefore offer a suggestion to the Committee about one step to consider – a National Academy of Science study on privacy and information sharing, including the use of commercial data by the federal government. The National Academy of Sciences has done other excellent work on mixed topics of science and policy. Assembling a group of experts to do such a study may be the most promising route to moving us up the learning curve. We know that the sources of data are very different today than when the Privacy Act was drafted in 1974. The proper use and dissemination within the government of today's data is thus a timely and important topic for study, and then for action.

---

[1] Today's testimony draws in part on "*Protecting Privacy in the Digital Age*: American Progress Recommendations on Government's Use of Commercial Databases," (May 4, 2005), available at http://www.americanprogress.org/site/pp.asp?c=biJRJ8OVF&b=651807.

[2] In 2004-05 I was a member of the Information Policy Forum, an unpaid group of persons from the non-profit sector that Lexis/Nexis asked for advice on information policy issues. I am no longer on that group, and am not affiliated with any information resellers.

[3] Later, the Report says that the purposes for collecting data must be those stated in advance or those "compatible" with the original purposes. By paraphrasing the OECD Guidelines, the Report misses one of the topics that was most debated in 1980, that uses are permitted where they are "not incompatible" with the original purposes. That is, use of personal data is in fact permitted, so long as the use is "not incompatible" with the original uses. In my experience, this shift in terminology has often been used as a basis for explaining why the Guidelines permit greater use of personal information, and more exceptions to privacy laws, than might otherwise be understood.

[4] U.S. Office of Management and Budget, Department of Justice, and Treasury Department, "Study of Financial Privacy and Bankruptcy," January 2001, available at http://www.privacy2000.org/presidential/OMB_1-01_Study_of_Financial_Privacy.htm.

[5] My Ohio State colleague Peter Shane has written "The Bureaucratic Due Process of Government Watch Lists," Mar. 6, 2006, available at http://law.bepress.com/expresso/eps/1084. Technologist Jeff Jonas and Paul Rosenzweig, now an official in the Department of Homeland Security, have written "Correcting False

Positives: Redress and the Watch List Conundrum," June 17, 2005, available at http://www.heritage.org/Research/HomelandDefense/lm17.cfm.

[6] Report of the Department of Homeland Security Data Privacy and Integrity Advisory Committee, "Framework for Privacy Analysis of Programs, Technologies, and Applications," Rep. No. 2006-1, adopted Mar. 7, 2006, available at http://www.privacilla.org/releases/DHS_Privacy_Framework.pdf.