Center for American Progress

STATEMENT OF PROFESSOR PETER P. SWIRE
C. WILLIAM O'NEILL PROFESSOR OF LAW
MORITZ COLLEGE OF LAW, THE OHIO STATE UNIVERSITY
SENIOR FELLOW, CENTER FOR AMERICAN PROGRESS

BEFORE

THE U.S. SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

ON

"PROTECTING PERSONAL INFORMATION: IS THE FEDERAL GOVERNMENT DOING ENOUGH?"

JUNE 18, 2008

Chairman Lieberman, Ranking Member Collins, and members of the Committee:

Thank you for the opportunity to testify today on the topic of "Protecting Personal Information: Is the Federal Government Doing Enough?" Chairman Lieberman, I salute you for your personal leadership on these issues, such as your privacy agenda that stated: "Joe Lieberman believes that a technologically advancing world demands a new compact to keep personal information private and shed light on the workings of government."[1] This committee played a key role on a bipartisan basis in enacting the E-Government Act of 2002, a valuable statute that has placed Privacy Impact Assessments at the center of privacy protection in the federal government. I also commend the Government Accountability Office for its thorough and thoughtful new report on protecting privacy in federal agencies.

My testimony highlights two emerging areas where I believe the Committee can and should take prompt action—biometrics and identification systems. I briefly highlight my recommendations here, and explain the basis for them in the full testimony.

For biometrics, such as fingerprints, I recommend three actions.

First, the E-Government Act of 2002 should be amended to provide that the default for storage and transmission of biometrics should be in encrypted form. An exception to this encryption policy should be permitted only if it is justified in a Privacy Impact Assessment, and has received specific authorization from the Chief Privacy Officer for the agency. It is worth considering whether similar requirements should be imposed on private-sector users of biometrics, in order to prevent private-sector compromise of biometrics that are used by the government.

Second, access to biometric databases should be subject to effective audit systems.

Third, the Committee should ask for a report from key federal privacy offices, including the Department of Homeland Security and the Department of Justice, on the "biometric encryption" approach that is designed to use fingerprints and other biometrics with greater security and privacy. The report should examine the advantages and disadvantages of this approach compared to current biometrics approaches, and should propose settings for pilot projects of the biometric encryption approach.

For identification systems, the Center for American Progress recently published a report that I co-authored with Cassandra Q. Butts, "The ID Divide: Addressing the Challenges of Identification and Authentication in American Society."[2] The testimony describes key aspects of that report. In terms of action by this Committee, I submit the following recommendation:

To address the full range of privacy and other risks from identification systems, this Committee should thus consider an expansion of the E-Government Act of 2002 to have a more thorough due diligence process of new identification systems. The analysis should include consideration of the following principles: achieve real security or other goals; accuracy; inclusion; fairness and equality; effective redress mechanisms; and equitable financing for systems.

In addition, I have reviewed a near-final draft of the testimony for this hearing of Ari Schwartz, Vice President of the Center for Democracy and Technology. Mr. Schwartz has been a leader for the past decade on how privacy should be protected in the federal government. His testimony does an excellent job of recommending next steps for federal privacy protection. I specifically agree with his five key recommendations:

1. Expanding Privacy Act coverage
2. Limiting Privacy Act loopholes
3. Improving Privacy Impact Assessments
4. Creating a Chief Privacy Officer at OMB who will run a separate CPO Council
5. Increasing and improving privacy reporting and audits

<u>Background</u>

I am 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. I also serve on a pro bono basis as a Policy Fellow with the Center for Democracy and Technology.

From 1999 until early 2001 I served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget. In that role, I was essentially acting as Chief Privacy Officer for the U.S. government. I was responsible for coordinating administration policy on public- and private-sector uses of personal information, and served as point of contact with privacy and data protection officials in other countries. During this time, along with many other activities, we: responded to agency questions about the Privacy Act; created guidance for privacy policies on federal web sites; issued guidance on the use of cookies on federal sites; and instituted Privacy Impact Assessments as a "best practice" for new federal information systems.[3]

Since leaving OMB, I have worked and written on a very wide variety of privacy and computer security issues. For instance, I was the only person to testify to Congress on privacy issues at the time of the creation of the Department of Homeland Security, and have written on government privacy issues arising from information sharing, foreign intelligence surveillance, the Patriot Act, and many other topics. My testimony and other writings appear at www.peterswire.net and www.americanprogress.org.

New policy needed for biometrics

Biometrics is the first priority area where I believe that federal privacy policy needs to improve. The term "biometric" means something that measures your biology, such as a fingerprint, iris scan, or DNA sample. The focus of my remarks is on what computer scientist Terrence Boult has called the "biometric dilemma"—the more we use biometrics, the more likely they will be compromised and hence become useless for security. Professor Boult's basic point is that fingerprints and other "secrets" become more widely known once they are used repeatedly, and thus don't remain "secret" after all.

The federal government has been rapidly increasing its reliance on biometrics in recent years, especially fingerprints. Privacy and security protections have not kept pace, however. Recent statements by Homeland Security Secretary Chertoff show the reason for concern. Secretary Chertoff spoke in Canada in April in support of the "Server in the Sky" program to share fingerprints among the U.S., Canada, the U.K., and Australia.[4] In a briefing with the Canadian press, Chertoff made the statement that fingerprints are "not particularly private":

> QUESTION: Some are raising that the privacy aspects of this thing, you know, sharing of that kind of data, very personal data, among four countries is quite a scary thing.
>
> SECRETARY CHERTOFF: Well, first of all, **a fingerprint is hardly personal data because you leave it on glasses and silverware and articles all over the world, they're like footprints. They're not particularly private.**

Fortunately, despite this statement by Secretary Chertoff, the Department of Homeland Security does include fingerprints and other biometrics in its definition of "personally identifiable information," the information that triggers a privacy impact assessment when used by government.

The problem remains, however, that current protections for biometric information are systematically weak. Secretary Chertoff, in the same Canadian visit, said that "It's very difficult to fake a fingerprint." That is not true. A quick web search on "fake fingerprints" turns up cheap and easy methods for do-it-at-home fake fingerprints. As discussed by security expert Bruce Schneier, one technique is available for under $10. It was tried "against eleven commercially available fingerprint biometric systems, and was able to reliably fool all of them."[5] In brief, the digital image of the print is sent to a laser printer. It is then easily transferred to a gel that covers the imposter's finger.

Two policies can help ensure that federal biometric efforts are done well, with benefits for privacy and security. If biometrics are badly deployed, by contrast, we could create a new generation of identity theft problems from fake fingerprints and other biometrics. It is hard enough to get a new Social Security number once you have been the victim of identity theft. Once your fingerprint is known, though, you can't get a new finger.

The first policy is to use effective encryption in connection with current forms of biometrics. DHS and other federal agencies are creating an increasing number of databases containing fingerprints and other biometrics. At the same time, federal agencies have suffered a series of serious data breaches, such as the well-known incident where the Veterans Administration lost the personal information of over 26 million veterans. The combination of biometric databases and data breaches is a scary prospect, indeed—a similar data breach with respect to fingerprints could mean that fingerprints would be permanently insecure for all of the millions of people whose information was in the data breach.

In response, federal policy should be to store and transmit biometrics in encrypted form. The use of strong encryption greatly reduces the risks from data breaches, because identity thieves won't be able to read the fingerprints or other data even if they get access to a federal database or stolen laptop. **The E-Government Act of 2002 should be amended to provide that the default for storage and transmission of biometrics should be in encrypted form. An exception to this encryption policy should be permitted only if it is justified in a Privacy Impact Assessment, and has received specific authorization from the Chief Privacy Officer for the agency. It is worth considering whether similar requirements should be imposed on private-sector users of biometrics, in order to prevent private-sector compromise of biometrics that are used by the government.** These requirements would not apply to publicly viewable biometrics, such as the picture of a face.

This policy—using encryption of the full fingerprint or other biometric in storage and in transit—reduces the risk of important types of data breach. It reduces the problem that an *unauthorized* person will gain access to the fingerprint, because an accidental spill or an intrusion by a hacker will only gain access to encrypted data. It does not help, however, against misuse by those who are authorized to see the biometrics. A major computer security risk is that an insider will break the rules. In most computer security settings, a majority of the harms come from this sort of malicious insider—those who have access but go beyond their authority. One important counter-measure is to perform audits on access to sensitive systems, in order to detect, deter, and help punish such violators. **Access to biometric databases should thus be subject to effective audit systems.** An audit system caught State Department contractors earlier this year who had improperly accessed the passport files of Sen. Obama and other presidential candidates. Effective audits should similarly be in place for access to sensitive databases containing biometrics.

Encryption within the central database, however, does not provide long-term protection for fingerprints and other biometrics. The reason is that the number of *authorized* users generally climbs swiftly in today's information -sharing environment. The "Server in the Sky" program, discussed by Secretary Chertoff, is one example. It proposes to share fingerprint databases among four nations, and other information-sharing programs are in the works for state and local officials and also to more countries over time. The fingerprint requirements that apply to most non-U.S. visitors to the U.S. are encouraging other countries to require U.S. travelers to provide our fingerprints as a condition of entry to a growing list of other countries. We are thus moving toward a new reality where fingerprints for a large and growing portion of our population are insecure—they are being held in many settings where a breach can occur. And, once the breach does occur, then we know we can't give the person a new fingerprint. Unlike a credit card number, which is "revoked" when a problem happens, my fingerprint is no longer a good identifier once others can use it as well.

Fortunately, slightly more sophisticated biometric technology can greatly reduce these identity theft and other privacy risks. Ann Cavoukian, the Privacy Commissioner for Ontario, has been a global leader in promoting what is called "biometric encryption." With biometrics expert Alex Stoianov, she has published: "Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy." [6] As explained by a prominent biometrics researcher:

> "In Biometric Encryption, you can use the biometric to encrypt a PIN, a password, or an alphanumeric string, for numerous applications—to gain access to computers, bank machines, to enter buildings, etc. The PINs can be 100s of digits in length; the length doesn't matter because you don't need to remember it. And most importantly, all one has to store in a database is the biometrically encrypted PIN or password, not the biometric template."[7]

The privacy and security advantages of this approach are large. The system owner, such as an employer, gains the advantages of traditional biometrics approaches, such as being confident that only the correct person can gain access. For the individual, there is the large privacy advantage that a breach by the system owner will not compromise the fingerprint or other biometric. Only that one PIN is lost, and the individual can generate a new PIN/password using the same fingerprint or other biometric. In the long run, systems owners also benefit, because this approach is much less likely to be based on a compromised fingerprint than under the current, flawed approach.

After careful review of the technical and policy literature, Cavoukian and Stoianov highlighted six advantages of the biometric encryption approach:

1. NO retention of the biometric image or template
2. Multiple/cancellable/revocable identifiers
3. Improved authentication security: stronger binding of user biometric and identifier
4. Improved security of personal data and communications
5. Greater public confidence, acceptance, and use; greater compliance with privacy laws
6. Suitable for large-scale applications

In terms of legislative action, this Committee should support a careful federal examination of this promising approach, which appears likely to be better from both a privacy and a security perspective. As a first step, **the Committee should ask for a report from key federal privacy offices, including the Department of Homeland Security and the Department of Justice, on the biometric encryption approach. The report should examine the advantages and disadvantages of this approach compared to current biometrics approaches, and should propose settings for pilot projects of the biometric encryption approach.** This sort of prompt review of the biometrics encryption approach can form the basis going forward for better security and privacy in the deployment of biometric systems.

The ID Divide

The second priority area is to ensure better privacy protections are build into government identification systems. I was recently co-author, with Cassandra Q. Butts, of "The ID Divide: Addressing the Challenges of Identification and Authentication in American Society." This report was based on a working group of experts in a wide range of contexts: national and homeland security; immigration; voting; electronic health records; online authentication; computer security; and privacy and civil liberties. The project, at the Center for American Progress, arose from the recognition that the next administration will face identification and authentication issues that cut across this range of issue areas.

The story from the Indiana primary about the 12 nuns who were turned away from voting because they lacked a government-issued ID, illustrates the sorts of challenges facing Americans who are increasingly being asked to identify themselves. And in 2006 the personal identification data of 26.5 million veterans was lost from a government laptop, one in a series of data breaches that threaten the integrity of everyone's identification.

The 12 nuns are among over 20 million other voting age citizens without drivers' licenses, and they join the 26.5 million veterans and many millions of other Americans who suddenly find themselves on the wrong side of what we call the ID Divide—Americans who lack official identification, suffer from identity theft, are improperly placed on watch lists, or otherwise face burdens when asked for identification. The problems of these uncredentialed people are largely invisible to credentialed Americans, many of whom have a wallet full of proofs of identity. Yet those on the wrong side of the ID Divide are finding themselves squeezed out of many parts of daily life, including finding a job, opening a bank account, flying on an airplane, and even exercising the right to vote.

In considering this ID Divide, the report developed a set of six principles for identification systems:

1. Achieve real security or other goals

New identification systems proposed in the name of security should be subject to a due diligence review to ensure that they actually promote security and do so cost-effectively compared to other available options. Similarly, identification systems proposed for other purposes, such as immigration policy, should only be deployed after they are shown to be effectively related to achieving the specified policy goals. This principle comes first for a simple reason—the financial and other costs of a new system are justified only if they actually achieve security or other goals. If they do not, then the analysis should end at this step.

2. Accuracy

A system will only work in the long run if it has a high level of accuracy. Any system, such as a watch list, has "false positives" (people treated as terrorist suspects mistakenly) and "false negatives" (people who are dangerous who evade detection by the system). A proposed system should be carefully vetted to ensure that the accuracy produced by the system will result in a manageable number of false positives and negatives.

3. Inclusion

As ID checks spread, it becomes increasingly important to ensure that people have a workable way to reduce the effects of the ID Divide. In many instances, there may be opportunities to rely on authentication approaches other than full identification. Where identification is used, however, then a goal of the policy process should be to foster inclusion of eligible persons.

4. Fairness and equality

New authentication and identification systems should be designed with consideration of their effects on the less wealthy and others who would suffer disproportionate burdens from any given design. Equality principles are especially important with respect to fundamental rights, such as the right to vote, and for any system where use of the ID is vital to daily tasks, such as opening a bank account or proving eligibility for a job. Where necessary, in order to enable people to live fully in society, fees should be waived based on financial hardship. Procedures for reasonable exceptions should also be developed, in recognition that any one method of identification will not work for the entire eligible population.

5. Effective redress mechanisms

Stricter and more numerous identification systems mean that burdens increase greatly on individuals who are mistakenly put on watch lists or otherwise disadvantaged by the system. An integral part of system design must be to have effective redress mechanisms. Otherwise, individuals will be turned into second-class citizens, deprived of the ability to conduct daily activities of life in a normal way. An effective security system must have not just on-ramps, but off-ramps as well. A properly designed system will allow government to distinguish between those who actually pose a threat and those who do not, and to proactively remove names from the watch list without a formal petition. If the security system remains the one-way street it is now, then it will inevitably collapse from its own weight.

6. Equitable financing for systems

A major criticism of the REAL ID Act has been its unfunded mandates. Congress has only provided the states with a small fraction of the expenses of implementing the federal requirements, now estimated at $4 billion over 10 years, but perhaps more. Along with such unfunded expenses to states and localities, REAL ID and other new identification systems impose off-budget costs on individuals who must spend time and money to meet the system's requirements. These include: tracking down birth certificates and other documentation; the time needed to try to resolve problems; and the costs to eligible individuals who get put on watch lists or otherwise cannot meet the system requirements. New identification systems, built for the common good, should thus be funded in a transparent and equitable way.

In order to implement these principles for identification, our report calls for a more thorough "due diligence" process when considering and implementing identification systems. The term "due diligence" is used in mergers and acquisitions and other important corporate transactions to describe the careful vetting before a company makes a major investment. Proponents of a merger (or, in our case, of a new identification program) can err on the side of optimism, concluding too readily that the benefits of a merger (or an ID or other security program) will demonstrably improve the situation. In response, a due diligence process looks for the characteristic ways that things might go wrong.

This insight of a due diligence process exactly corresponds to this Committee's support for a privacy impact assessment under the E-Government Act of 2002. The privacy impact assessment is a crucial step, and the Privacy Office at the Department of Homeland Security has made important strides in doing rigorous privacy impact assessments for some authentication systems, such as the Transportation Workers Identification Card.

When it comes to authentication systems, however, a broader analysis is required than exists currently under privacy impact assessments. **To address the full range of privacy and other risks from identification systems, this Committee should thus consider an expansion of the E-Government Act of 2002 to have a more thorough due diligence process of new identification systems. The analysis should include consideration of the principles of: achieve real security or other goals; accuracy; inclusion; fairness and equality; effective redress mechanisms; and equitable financing for systems.**

Identification systems are being rapidly considered and deployed in the Department of Homeland Security and elsewhere in the federal government. Our report on the ID Divide shows a range of serious questions about the wisdom of many of these identification systems, both as a policy matter and at the technical level. The biometrics discussion in this testimony, and included in the report, shows that badly implemented biometric and other identification approaches can actually increase the problem of identity theft, leading to new rounds of privacy and security problems for millions of Americans. This Committee should provide strong oversight of how new identification systems are actually being implemented, and should consider legislation to do an expanded due diligence review of new identification systems.

Conclusion

In conclusion, I thank the Committee for requesting the GAO report and for all of its work on privacy and computer security issues in the federal government. My testimony today has focused on two emerging areas of priority concern—new biometrics and identification systems. Attention to those issues should be given while also carefully considering the numerous other privacy issues raised by the GAO and in other testimony today, including by the Center for Democracy and Technology.

[1] "Joe Lieberman's Plan to Protect Personal Privacy and Break the Bush Wall of Secrecy: Safeguarding Personal Information and Making Government Open and Accountable to the Public," Jan. 9, 2004, available at http://www.fas.org/sgp/news/2004/01/lieb010904.html.

[2] http://www.americanprogress.org/issues/2008/06/id_divide.html.

[3] For contemporaneous descriptions of our privacy efforts, see Peter P. Swire, "The Administration Response to the Challenges of Protecting Privacy," (2000), available at http://www.peterswire.net/pspublications.htm; "How Well Did the Clinton Administration Do on Privacy Rights?" Jan. 23, 2001, available at http://seclists.org/politech/2001/Jan/0058.html.

[4] "Chertoff Says Fingerprints Aren't 'Personal Data'", available at http://thinkprogress.org/2008/04/16/chertoff-fingerprints/.

[5] Bruce Schneier, "Fun with Fingerprint Readers," (May 15, 2002), available at http://www.schneier.com/crypto-gram-0205.html#5.

[6] Ann Cavoukian & Alex Stoianov, "Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy," (March 2007), available at http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf.

[7] Id. at 16 (quoting Dr. George Tomko).