Testimony to:

House Committee on Government Reform
Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations

From: U.S. Public Policy Committee (USACM) of the Association for Computing Machinery (ACM)

By: Prof. Ben Shneiderman, University of Maryland

National Identification Card Systems

November 16, 2001

Thank you Chairman Horn for the opportunity to testify at this timely and important hearing. I want to commend you, Ranking Member Schakowsky, the Subcommittee members, and your staff for turning the attention of Congress to today's discussion regarding proposals for a National Identity card system.

By way of introduction, I am Ben Shneiderman, a Professor in the Department of Computer Science at the University of Maryland at College Park. In addition, I am Founding Director of the Human-Computer Interaction Laboratory, and Member of the Institute for Advanced Computer Studies and the Institute for Systems Research at the University of Maryland. I am a Fellow of the Association for Computing Machinery and a Fellow of the American Association for the Advancement of Science.

This statement represents the Association for Computing Machinery's (ACM) Committee on U.S. Public Policy (USACM). ACM is a non-profit educational and scientific computing society of 75,000 computer scientists, educators, and other computer professionals committed to the open interchange of information concerning computing and related disciplines. The Committee on U.S. Public Policy acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. It seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community.

Introduction

In the two months since the deplorable acts of terror were perpetrated against America, a number of legislative measures and regulatory actions intended to ensure the safety and security of our citizens have been proposed. While most proposals have been well intentioned, some have been misguided in that they overlook the potential for unintended

consequences or underestimate the technical challenges and risks inherent in their implementation.

Recently, information technology vendors have suggested that a comprehensive National Identity card system could be created and implemented in as little as 90 days. Implementing such a complex system is a challenging system engineering matter. Such rapid construction of an effective and novel socio-technical system would be unprecedented. A constructive alternative may be focused efforts that build on existing systems such as state motor vehicle identification and passports.

Practical Concerns

From a practical standpoint, a National Identity card system would not have prevented the tragic terrorist acts of September 11. Evidence suggests the suspected hijackers made no effort to conceal their identities. In fact, several of the suspected terrorists possessed state-issued ID cards with their pictures and names.

Proponents of the National Id system suggest that cards will authenticate the identity of individuals. **However, the positive identification of individuals does not equate to trustworthiness or lack of criminal intent.**

The quality of forged public documents is often so good that they are accepted as authentic. According to the Suspicious Activity Reports (SAR) filed by U.S. financial institutions, thousands of counterfeit credit cards have been reported over the last several years. The credit card industry has accepted that losses due to high-quality counterfeit cards are simply a cost of doing business.

As with any system that depends on human and technological components, insider abuse is a risk. Currently, there is no method of ensuring that forgery, bribery, or coercion will not put the proposed form of identification in the possession of those with criminal intent. As the recent Virginia case demonstrates, motor vehicle department employees have issued unauthorized drivers' licenses for financial gain or other personal reasons.

Socio-Technical Challenges

A national ID system requires a complex integration of social and technical systems, including humans to enter and verify data, plus hardware, software and networks to store and transmit. Such socio-technical systems are always vulnerable to error, breakdown, sabotage and destruction by natural events or by people with malicious intentions.

For this reason, the creation of a single system of identification could unintentionally result in degrading the overall safety and security of our nation, because of unrealistic trust in the efficacy the technology. The National ID card itself is only the most visible component of a system that would require supporting bureaucracies and elaborate

databases that would operate in everyday situations. In particular, a National ID system requires an extensive database of personal information on every citizen. Who would enter the data, update it, and verify it. Who would determine when the data is no longer trustworthy? Who would review audit trails and approve access?

We must ask whether there is now a secure database that consists of 300 million individual records that can be accessed in real time? The government agencies which come close are the Internal Revenue Service and the Social Security Administration, neither of which are capable of maintaining a network that is widely accessible and responsive to voluminous queries on a 24 hour by 7 days a week basis.

Can records on everyone in the United States or even all foreign visitors be organized and maintained in one database? Compiling the necessary database to support the system would require a massive data-collection effort beginning with the interconnection of databases held by local, state and national government networks and some private entities. Determining what information to include in the database will no doubt prove to be controversial.

Once the problem of gaining access to the amount of information required is solved, there still would be challenges in creating a system that could communicate with all of the varied computer networks that would house components of individual identification. The difficulty of communicating with intra-federal, intergovernmental, and private sources of information in real time environment is unprecedented.

An underlying software foundation is required to make the system work. In addressing the problems of building a large enough network and/or creating a workable cross database network communication system, redundancy and backup issues must be addressed. Formulating protocols and procedures for the proper maintenance of databases that are enforceable are part of this technical challenge.

Once the information is gathered, how will the information be transmitted? Who will have access to the information? Will there be limitations on how the information can be used by front line workers?

The next question involves how persons present their identification to those in authority who demand it. Will the identification be a card, with a photo, signature, thumbprint or other identifying biometric? While biometric technology is advancing rapidly, new socio-technical concerns have arisen that need to be addressed before large-scale implementation.

Regardless of the method used to create a new identification tool, the system would require professionally trained staff at specialized terminals at every point at which the National ID card is to be used. Devices like card readers supporting databases and communication complexes would be necessary to support National IDs. An extensive and secure nation-wide communications network to connect multiple terminals to the database would also be required.

Security Risks of the Infrastructure

There are nearly 300 million residents in the United States. To what extent can a national identification system be created that would provide confidentiality, authentication, integrity, access control, and availability to a group of users who are geographically dispersed with an acceptable rate of false positives or negatives?

Confidentiality speaks not only to the issue of privacy, but to the safe transmittal of information over great distances. The current state of the Internet might make it unsuitable for this purpose. Authentication requires that the system must be able to accurately verify the identity of people. Integrity speaks to the high level of trust and acceptance this system must have to be depended upon by security and law enforcement. Access control must be limited to those with proper clearance and authority. This is important if confidentiality, authentication, and integrity are to be maintained.

The technology would have to prevent interruption of communications from natural or man made causes, interception of information by unauthorized parties, unauthorized modification of information stored in networks or while in transit, finally the system would have to insure that fabrication of information was not possible.

As this Subcommittee knows from its computer security efforts, strong system security is presently an unsolved socio-technical problem, even in the most advanced systems. There are a great many problems that need to be addressed to help secure our nation's infrastructure. My colleague Dr. Peter Neumann of SRI has documented the myriad ways that computerized identification systems have been compromised with sometimes devastating results.

Databases are vulnerable to exploitation and attack. A national identification database could provide a new target for malicious computer users. As evidenced by the poor computer security grades awarded last week by this Subcommittee, vandals have routinely corrupted government computer networks. Unauthorized intrusions to the National ID database may use that information as a means to conduct identity theft or to profit by the sale of that information to others with criminal intent.

The disclosure a few years ago that IRS personnel were reading the private tax returns of prominent Americans was unsettling for most of us. A National ID system places an even greater amount of information in reach of those who might abuse it.

Constructive alternatives

If a new and centralized approach is technically problematic and politically unpalatable, then how might we work to increase security? **Constructive first steps would be to define goals and develop metrics of success.** Improved air travel safety would have

wide public support, if the techniques to achieve that goal had modest impact on personal rights and privacy. A realistic goal would be to make verifications of passenger identity more reliable, while limiting the delay, intrusion and inconvenience to citizens.

Improving state motor vehicle identification cards might be accomplished by coordination among states to determine best practices for issuing, replacing, verifying, and monitoring usage. Such efforts might be coordinated by the National Association of State Chief Information Officers or the National Governors Association. Common practices or even national standards might be arrived at through public discussion. Adequate public discussion of proposals is essential to gain acceptance and to improve their quality.

A socio-technical systems approach would include quantification of weaknesses and vulnerabilities of the database security and network access, based on existing systems. Then realistic solutions to dealing with problems such as lost cards and mistaken identifications would have to be developed and tested. Special cases, such as people who do not wish to carry a card, tourists, professional visitors, and foreign students would have to be addressed.

Any complex socio-technical system, such as identity verification, requires well trained personnel whose performance is monitored regularly. Effective hiring and screening practices, chances to upgrade their skills, and participation in re-design are important contributors to success.

Improvements for citizens could also lead to higher data reliability and system efficacy. Citizen confidence and data accuracy could be improved by system designs that provide greater transparency by allowing citizens to inspect their contents and view a log of who uses their data.

More constructive ideas could emerge by encouraging research by computer and information scientists in collaboration with social scientists. They should also be encouraged to build bridges with legal and policy groups, so that their solutions are realistic and implementable.

Conclusion

It is important that Congress proceeds cautiously on the issue of a National ID card system. National ID cards involve risks and a variety of practical, organizational, and technical challenges. **Any efforts to improve homeland security should begin with clear statements of goals and quantifiable metrics of success.**

Computer technology can do much but it cannot see into the minds and hearts of people, nor can it replace the capability of vigilant citizens. **Face-to-face security checks must be a vital component of airport and other security systems.**

Despite growing public and political pressures for perceived security enhancements, the risks and challenges associated with a National ID card system need to be identified and understood before attempting deployment. The problems cannot be solved overnight, or in 90 days as has been suggested. Constructive alternatives such as improving existing state motor vehicle registration and passports are promising possibilities that could bring benefits sooner than establishing an entirely new system. **The emphasis must be on people first, then technology.** The Association for Computing Machinery and other leaders in the computing community are ready and willing to assist lawmakers in their efforts to enhance the safety and security of our nation.

For more information about USACM contact Jeff Grove, 202-659-9711, or see the web site http://www.acm.org/usacm

Prof. Ben Shneiderman ben@cs.umd.edu
Dept of Computer Science 1-301-405-2680
Univ of Maryland 1-301-405-6707 fax
College Park, MD 20742
Lab: http://www.cs.umd.edu/hcil Bio: http://www.cs.umd.edu/~ben