

President

Coralee Whitcomb

Chairman of the Board

Hans Klein

Secretary

Herbert Kanner

Treasurer

Steve Teicher

Directors

Kwami Ahiabenu II

Netiva Caftori

L. Jean Camp

John Dwyer

Robert Guerra

Gene Haldeman

Harry Hochheiser

Glenn Manishin

Dara O'Neil

February 14, 2002**CPSR supports Maryland HB281's limits on the use of Social Security Numbers.**

What if one key opened every lock that you used? Although this may sound convenient, it comes with a obvious risk: if your keys fell into the wrong hands, the recipient would have virtually unrestricted access to your car, house, safe deposit box, or other areas that might include sensitive belonging and information.

Social Security Numbers (SSNs) act as keys that unlock all of our data. In computer systems, SSNs often act as primary keys -identifiers that unambiguously identify entries in a database. For a single database, primary keys are needed to avoid confusion –many people can have the same name, but only one person can have a given key, or id number. Given a primary key, a database user can retrieve the information stored in the database about the person associated with that ID number. Using the same primary key in different databases is the computer equivalent of using one key for many locks: if the primary key is shared among many databases, sharing information in those databases is much easier.

SSNs simplify the process of profiling citizens. Businesses or other organizations that maintain databases keyed by SSNs can easily exchange information and build profiles by simply by combining records that have the same SSN. The use of a standard, common identifier eliminates the uncertainty and increases the value of the combined database, in a manner that would not be possible if each organization created its own ID numbers.

Profiles built using SSNs might include sensitive information that can be used without our knowledge. These profiles might include sensitive information regarding our finances, education, or health care. Furthermore, they can be built without our knowledge, consent, or access. Once created, these profiles can vastly increase the power of businesses to market (or deny) services, hire and fire employees, and otherwise make decisions that affect our lives based on information that we may not know that they have.

The widespread use of SSNs increases our vulnerability to costly fraud and identity theft. SSNs can and have been used as the single key piece of information needed to "steal" identities. If the SSN was not used as a shared identifier in multiple contexts, identity thieves would have to find numerous ID numbers before they would be able to do the damage that they can currently do with one SSN.

SSNs should not be used for authorization purposes: Banks, credit cards, and others commonly ask clients to provide the last four digits of the SSN in order to access account information. In computer security terms, this amounts to using SSNs as a form of authentication ("I really am who I say I am") and authorization ("I have the right to access this information") in addition to its primary use for identification ("this is who I am"). The use of different measures for these three functions increases security and complicates theft. Familiar examples of this approach include the use of usernames and passwords for Internet services or web sites, and PIN numbers that accompany ATM cards. Banks, credit card issuers, and others should use similar measures, as SSNs are too widely available to be effective in restricting access to sensitive information.

SSNs may not be unique or reliable. Instances of multiple SSNs being issued to one person, and of one number being issued to multiple people, have been documented. SSNs are also potentially unreliable, as they do not have check digits that can be used to mathematically verify that they are valid. As a result, there is no guarantee that a social security number is the right number for the right person.

Despite these problems, SSNs are often treated as if they are assumed to be accurate and infallible, thus creating further difficulties for individuals who experience problems with SSNs that are incorrectly assigned or entered incorrectly.

Deputy Director
Susan EvoyP.O. Box 717
Palo Alto, CA
94302650-322-3778
650-322-4748 (fax)cpsr@cpsr.org
www.cpsr.org

Claims of consumer convenience resulting from the use of SSNs are self-serving. Defenders of the use of SSNs might argue that the use of the SSN is convenient for individuals. If one ID number is used in multiple contexts, there are fewer numbers that we must keep track of. This claim does not stand up to closer scrutiny: in today's world of proliferating phone numbers, credit card numbers, association membership numbers, and other identifiers, SSNs provide (at best) marginal simplification of an extremely complex situation.

The public costs of identity theft and loss of privacy may be comparable to (or greater than) the private costs of database modification and lost marketing opportunities associated with elimination of SSNs from private databases. Institutions that operate large databases might argue that eliminating SSNs would be prohibitively expensive. Modifying existing databases to replace SSNs with new (perhaps randomly-assigned) ID numbers would certainly involve a small expense, but the costs should be negligible compared to the expense of (for example) preparing for the year 2000 calendar change.

In evaluating claims of the expense of transition away from SSNs, we must ask what interests are truly at stake: are defenders of SSNs concerned about the cost of updating databases, or of losing information and related revenue that is generated by sharing records based on these ID numbers? Costs associated with existing systems must also be considered. Although precise numbers may be hard to come by, the costs of identity theft and loss of privacy may outweigh the institutional costs of modified database practices.

HB 281's limits on the use of Social Security Numbers would help consumers reduce the risk of identity theft, and protect the privacy of citizens.

Resource:

CPSR's SSN Frequently-Asked Questions (FAQ):

<http://www.cpsr.org/cpsr/privacy/ssn/ssn.faq.html>

About CPSR:

Computer Professionals for Social Responsibility (CPSR, <http://www.cpsr.org>) is a public-interest alliance of computer scientists and others concerned about the impact of computer technology on society. CPSR works to influence decisions regarding the development and use of computers because those decisions have far-reaching consequences and reflect our basic values and priorities.

As technical experts, CPSR members provide the public and policymakers with realistic assessments of the power, promise, and limitations of computer technology. As concerned citizens, CPSR members direct public attention to critical choices concerning the applications of computing and how those choices affect society.

Additional Endorsement

This statement has been endorsed by the Institute of Electrical and Electronics Engineers, Inc. – United States of America. IEEE-USA is an organizational unit of the Institute of Electrical and Electronics Engineers created in 1973 to promote the careers and public-policy interests of the more than 230,000 electrical, electronics, computer, and software engineers who are U.S. members of the IEEE, including over 10,500 members who live and work in Maryland.