



USACM

U.S. Public Policy Committee of the ACM

April 4, 2005

The Honorable Lamar Alexander
United States Senate
302 Hart Senate Office Building
Washington, DC 20510

Dear Senator Alexander,

As chair, I write on behalf of the U.S. Public Policy Committee of the Association for Computing Machinery (USACM) to thank you for the opportunity to comment on Title II of the Real ID Act, which was added to the supplemental appropriations bill now pending in the Senate. We wish to express our concern that the legislation would significantly increase the risk of identity theft while decreasing personal privacy. We also join those, such as yourself, who anticipate that this Act will create a de facto national identification system with several critical shortcomings.

As you are well aware, the Real ID Act sets minimum standards for state driver's licenses and calls for an interstate compact to govern the sharing of this data among the states. Its authors argue that these provisions, along with the other aspects of the bill, are intended to respond to the recommendations of the 9/11 Commission that more be done to disrupt terrorist travel. While we share the authors' goal to prevent terrorists from entering into and traveling around the United States, as computer scientists and engineers, we wish to express our concern on the more technical aspects of Title II of the Real ID Act.

The legislation's mandate for electronic data collection and storage coupled with its sharing of state driver's license databases among the states and their agencies will increase the risk of identity theft. Any database of personal information presents privacy risks; however, separately administered, linked databases are more troubling because all data could be exposed from an insecure point in any of the databases or along the communications pathways used to share data.

The bill's language is vague regarding such critical issues as the principles and methods behind the creation, implementation, and administration of these databases and information-sharing arrangements. It contains no guidance regarding how the shared databases should be secured or how the personal information contained within them

should be handled. Further, it does not specify how to hold the administrators and users of these databases accountable for proper maintenance and use. For example, there are no details about: (1) what agents (public or private) would be trusted to access to these databases; (2) by what method(s) would the data and interstate searches of the data be secured; (3) how we would ensure that each state database and any related infrastructure maintain the highest level of security; (4) would one state be allowed to store records (including possibly inaccurate ones) from another state; and, (5) how would database use be tracked or audited so that abuse may be caught and problems uncovered. The bill also repeals existing law related to a consultative regulatory process, leaving no clear mechanism for addressing these questions. In light of the recent spate of events regarding criminals and others gaining unauthorized access to large collections of personal information, as well as current concerns about the epidemic of identity theft in the United States, these are troubling oversights.

It is also worth noting that these systems are always vulnerable to human error, breakdown, destruction by natural events, and sabotage – both by outsiders and by trusted people with malicious intentions. Substantial private sector experience demonstrates these risks escalate when unrelated organizations share data extensively. Accordingly, the simple fact of making personal data more widely available across the country in electronic form will increase the risk of identity theft. Therefore, any legislation mandating the linking and sharing of large numbers of databases containing personally identifiable information should specify a minimal level of security and require that adequate security be demonstrated prior to implementation of such a system. We also recommend that good practice, as demonstrated around the world, is having a defined mechanism where individuals can review records about them and correct errors without undue effort or obstacle.

As you know, many privacy and civil liberties groups have expressed concern that the bill's provisions for creating national driver's license standards are tantamount to creating a system of national identification. ACM has a long-standing statement expressing its concern over creation of national ID cards because of technical issues as well as concerns about privacy. In addition to the problems of error and identity theft mentioned above, the following are a few of the other technical and procedural problems that such a system might pose: (1) knowing the identity of a person reveals nothing of that person's intent – every criminal and terrorist has an identity but they have no record prior to their first offense; (2) there is a history of clerks in various states succumbing to bribery to grant driver's licenses to unqualified persons; this bill provides a national ID to someone who can find any lax or corrupt clerk anywhere in the US – a trivial task given the number involved; and (3) having a single ID will habituate some guards to checking for the form of the ID rather than the content, thus leading to weaker security than when guards must study an ID to determine its origin and validity.

I wish to offer you the technical and policy expertise of our committee. USACM is the U.S. Public Policy Committee of the Association for Computing Machinery, which is the world's first educational and scientific computing society with almost 80,000 members worldwide. ACM members include leading computer scientists, engineers, and other

professionals from industry, academia, and government. USACM's mission is to provide non-partisan scientific data, educational materials, and technical analysis to policymakers. Please contact ACM's Office of Public Policy at (202) 659-9711 if we can provide any assistance on this or related issues.

Sincerely,

Eugene H. Spafford, Ph.D.
Chair
U.S. Public Policy Committee of ACM (USACM)