January 19, 2006

Dear Members of the United States Congress:

As chair, I write on behalf of the U.S. Public Policy Committee of the Association for Computing Machinery (USACM) to commend you for the time and energy you have devoted to crafting much-needed data security legislation. As more organizations (including governmental entities) gather personal information, there is an increasing danger of fraud (such as identity theft) and erosion of personal privacy.

We at USACM—part of a nonprofit professional society comprising computer scientists, researchers, information technology (IT) consultants, attorneys with IT expertise, educators, and more—are acutely aware of the risks to individuals posed by unprotected or poorly protected personal information. For that reason, we are writing to express some of the technical community's concerns in this area.

Several relevant bills are now pending before Congress, many of which have a number of provisions in common (e.g., data breach notification, a new regulatory framework for data brokers and others who handle personal information). As your work proceeds, we would like to draw your attention to (and encourage you to base your deliberations on) a set of principles originally distilled in a seminal U.S. Department of Health, Education, and Welfare report.[1] These "Fair Information Practice" principles[2] have long been held in high regard and followed within the privacy and security communities, as well as serving as the basis for privacy laws enacted around the world. Adherence to Fair Information Practice principles when collecting, using, and storing large amounts of personal information will help protect the public, now and in the future. The principles include the following basic concepts:

- **Security**. Personal information should be maintained securely, whether the data is in storage, transmission, or transport (e.g., on magnetic tape). Security programs should be based on a formal, well-developed regulatory framework, government and industry standards, and accepted best practices, including the use of strong, meaningful, properly implemented encryption techniques. S. 1326, S. 1789, and H.R. 4127 make reference to using encryption techniques to secure data; the House bill goes somewhat further to specify the use of National Institute of Standards and Technology (NIST) standards regarding the implementation of encryption. We note that, properly used, encryption can be a valuable tool but will not, by itself, guarantee the security of any information: attention should also be paid to such things as access control, long-term storage, and information sharing, as well as to securing non-electronic versions of personal information (e.g,. backup tapes, archival printouts).

- **Limitation/Minimization**. Organizations should collect only the personal information that is needed for a specific purpose and should retain that information only as long as it is

needed for that purpose. In addition, information collected initially for one purpose should not be used for a different purpose without the consent of the individuals whose personal information is involved. Along these lines, H.R. 4127 was amended recently to include a provision that would require the disposal of obsolete personal information in electronic form by such means as erasing it or rendering it permanently undecipherable. We also suggest that disposal of obsolete information media (e.g., printouts, CDs) also be performed in a secure manner.

- **Access/Participation**. Consumers should have access to their personal information held by data brokers and other commercial entities, and they should have the right to dispute and/or correct erroneous information. Indeed, giving consumers access to their own data (something technology can certainly facilitate) could increase the overall accuracy (see below) of that information, as well. For example, S. 1789, in its provisions relating to the accuracy of consumer information held by data brokers, contains access provisions that appear to embrace this principle.

- **Accuracy/Integrity**. Organizations should be obliged, where appropriate, to keep personal information as accurate and up-to-date as possible. Technology, if used properly, can enhance accuracy through such means as searching for duplicate or erroneous records, and performing consistency checks. As mentioned above, S. 1789 contains specific language regarding the accuracy of consumers' personal information held by data brokers.

- **Accountability**. Someone should be designated within every organization who is responsible for the security and integrity of the personal information being held or used by that organization. Recourse should be established for anyone who is harmed as a result of his or her data being exposed or rendered inaccurate as a result of inadequate protection. In this regard, H.R. 4127 requires that organizations name a person or official who has the responsibility for the organization's data security program, as well as spelling out details for conducting post-breach audits of data-broker security programs.

- **Notice**. Consumers deserve to be given notice when their personal information is collected, used, or shared (three things that today's technologies make simple). Most of the bills under consideration require covered entities to notify consumers when their personal information is compromised -- this is a prudent first step in implementing this principle.

- **Choice/Consent**. Data security legislation should support greater individual control over sensitive personal information. For example, limiting the use of a consumer's Social Security number without his or her express consent was often discussed during the development of the bills now pending, although it remains to be seen if such a provision will make its way into a particular bill. In addition, some state legislation enables consumers to prevent third-party access to their records at credit bureaus without their explicit permission. Adopting provisions such as these would strengthen consent considerations and consumer protections.

Incorporating Fair Information Practice principles into data security legislation would go a long way toward securing consumers' personal information and restoring a sense of privacy. Indeed, given the pace at which technology and data exploitation are outstripping public policy, it is more

important than ever that policymakers understand where technology can be applied advantageously and where its application can introduce new risks to personal information.

I would also like to offer you the technical and policy expertise of our committee. USACM's mission is to provide non-partisan scientific data, educational materials, and technical analysis to policymakers. Please feel free to contact ACM's Office of Public Policy at (202) 659-9711 if we can provide any assistance on this or related issues.

Sincerely,

Eugene Spafford, Ph.D

Chair, ACM U.S. Public Policy Committee (USACM)

---

[1] United States Department of Health, Education and Welfare (HEW), 1973, "Records, Computers and the Rights of Citizens," available online at <http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm>.

[2] See <http://www3.ftc.gov/reports/privacy3/fairinfo.htm> for more information on FIPs.