



March 28, 2006

The Honorable Joe Barton
Chairman

The Honorable John D. Dingell
Ranking Member

House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Barton and Ranking Member Dingell:

As Chair of the U.S. Public Policy Committee of the Association for Computing Machinery (USACM), I write to provide some comments on the proposed amendment you recently released that you may bring before the House Energy and Commerce Committee as early as this week. Earlier this year USACM wrote to you and other Members of Congress urging Congress to consider Fair Information Practice (FIP) principles as the basis for legislation to protect consumers' electronic information.¹ In many respects this amendment is a welcome step forward in embracing three of the FIP principles by requiring information brokers to verify the accuracy of personal information, allowing consumers access to personal information, and introducing additional accountability through mandatory audit logs. We also wish to offer comments on the so-called "safe harbor" provision for notification to consumers and the provisions concerning obsolete records.

Accuracy and Access

We applaud the addition of language requiring information brokers to verify the accuracy of the data they collect, assemble or maintain. Databases are only as good as the accuracy of the information they contain. Ensuring that companies follow verification procedures for that data is an important part of the FIP principles.

Likewise, we welcome the reinsertion of the proposal granting consumers the right to view the information that information brokers hold about them. As we stated in our earlier letter, consumers should have access to the personal information held about them

¹ Our previous letter is available at <http://www.acm.org/usacm/weblog/index.php?p=345>

by data brokers and other commercial entities, and they should have the right to dispute and/or correct erroneous information. Respecting consumers' rights to access their own information is a key principle within the FIPs, and providing access also can lead to improvements in other areas (e.g., accuracy).

Accountability

We also are pleased to see the addition of the audit log requirement for information brokers. The ability to retrace each and every access to, change in, or transmission of such data will support greater accountability (also one of the FIPs' principles we discussed earlier) and overall security.

Safe Harbor

Any legislation intended to make personal information held by businesses more secure should protect consumer privacy while embracing technology neutral methods to do so. We are generally concerned that a risk-based standard for whether companies have to notify consumers upon a breach may not improve security practices. Notification is often an effective method for ensuring that companies continually improve their security practices. Clearly if there is a breach, regardless of the risk to consumers, a company's security system should be hardened to deal with the vulnerabilities. If there are multiple breaches, then notification should be required. Beyond this, we are concerned with the technology-based presumptions that would automatically enable the safe harbor from notification.

We view it as a positive step to include additional methods or technologies alongside encryption as a way to mitigate risk after a breach. We are concerned, however, that specifying technologies to mitigate risk without ensuring that these tools are part of a comprehensive system is problematic. If the goal is to prevent exposed data being used for identity theft, then the standard should address both the robustness of the technology used in the system and how it is implemented. Encryption or other techniques for obfuscating data are valuable security tools; however, without comprehensive security practices in place they are, by themselves, incomplete protection.

For example, reliance on encryption, particularly if it is not properly used, can create a false sense of security. Often this will lead to so-called "brittle" protections, where whole systems fail as a consequence of simple component failures. A company may use an Encrypting File System to store all its customers' personal information. If an unauthorized user gained access to the system but not to the encryption keys, all of this information would be encoded and useless. However, if someone was able to compromise the account or accounts of authorized users on the system, the mere presence of encryption does not reduce the threat of identity theft. All the personal information on that server would now be available to the thief through his or her compromise of a password, which might equivalently compromise the decryption key.

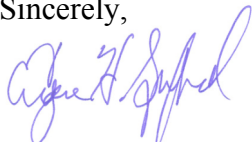
We recommend that rather than relying on specific technologies, the test for a safe harbor should be whether personally identifiable information might be extracted or inferred from the data that is disclosed. We also recommend that Congress should urge the FTC, as it develops its rulemaking or guidance, to draw upon existing, widely accepted, voluntary consensus technical standards. For example, ISO 17799 on information security management and ISO 18033 on data encryption are comprehensive and detailed security standards that have been adopted by the international community. Considering international standards may be particularly important given that consumers' information may be easily sent offshore to different countries that provide information technology support to U.S. companies.

Obsolete Data

Another important addition to the underlying legislation is the new provision regarding the destruction of obsolete paper records. This provision mirrors the underlying bill's existing text related to the secure disposal of electronic records. However, while the underlying bill clearly states that electronic data should be disposed of to make personal information "permanently unreadable or undecipherable," the new provision for paper records does not have the same emphasis on secure disposal. We would recommend making the new provision more explicit and requiring that non-electronic data containing personal information be disposed of in a "secure" manner. Secure disposal techniques would ensure that any personal information contained in the disposed data is irrecoverable.

Again, we appreciate the opportunity to offer additional comments on the bill. 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, and we are encouraged by Congress' attention to this important issue. Please feel free to call on USACM (through ACM's Policy Office at 202-659-9712) should you have any questions or need further technical expertise on this matter.

Sincerely,



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