May 1, 2003

The Honorable Mitchell E. Daniels, Jr.
Director, Office of Management and Budget
Executive Office of the President
725 17th Street, NW
Washington, DC 20503

Dear Director Daniels,

As leaders of the Association for Computing Machinery's (ACM) U.S. Public Policy Committee (USACM), we are writing regarding the Office of Management and Budget's (OMB) efforts to develop guidelines for agencies to follow in compliance with the new privacy requirements of Public Law 107-347. In particular, we are offering comments on the development of public web site privacy practices that utilize standardized machine-readable format protocols.

Section 208 of Public-Law 107-347 mandates OMB "shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format." This description is currently closely associated with the Platform for Privacy Preferences (P3P). P3P is a protocol for exchanging machine-readable information about a set of web site privacy practices. P3P may be used as a component of a privacy program because it provides a mechanism for communicating privacy rules to users, but it is not capable of monitoring whether or not web sites adhere to their stated privacy policy. Although P3P-enabled software tools may assist users in identifying changes to web site privacy policies, P3P does not provide an automated way for users to withdraw their information from a site that changes its policy in a way that the user finds objectionable. In addition, it does not provide any notice of changes to published privacy policies to visitors who are not using P3P-enabled software tools.

The Code of Fair Information Practices is the foundation for the Privacy Act of 1974 and other privacy laws of the United States. It prohibits secret databases and mandates fairness, accountability, and due process for individuals about whom information is gathered. P3P focuses on disclosures related to some principles of Fair Information Practices, but web sites that use P3P still need to take additional steps to make sure that their policies actually support all of the Fair Information Practices Principles. Therefore, our comments extend to the requirements for processes and procedures that provide adequate safeguards for the protection of online privacy based on public law or policy. In OMB's efforts to ensure individual online privacy safeguards, we recommend that privacy protection go beyond simply informing the public of privacy practices of federal agency web sites. At a minimum, OMB guidelines should:

· restrict the retention and sharing of data by and among federal agencies regarding users' online sessions unless expressed permission for retention is received based on informed consent of what will be retained on the agency or user's computer and for what specific purposes the information will be used;

. limit real-time online communication transactional information so that it relates to the specific purpose for which the user initiated electronic contact with the agency, and discard it at the close of the session;

. establish a separate protocol for processing requests for services or information wherein the agency retains only the information necessary to make a contextual response to the user;

· require that decisions to acquire new or communication enhancing technologies for public access to government information consider the acquisition's potential impact on user privacy and provide a mechanism after implementation to respond to unforeseen threats to security or user privacy;

. require agency web sites to communicate to all visitors whenever changes are made to published privacy rules and ensure that all published privacy rules reflect the current online privacy policy of the agency;

. provide automated processes to reestablish "consent" (as defined by the Canadian Standards Association Model of Fair Information Practices) of individual users when agencies web site privacy polices are changed to ensure that personal information is not used or disclosed for purposes other than those for which it was collected.

· provide for information assurance of federal computer systems accessed by the public;

· ensure that all users receive notice of their right to challenge personal information and suspected breeches in the use of personal information, based on an agency's published privacy policy;

. provide contact information for an agency's designated person to administer the review of privacy complaints, and the appeals process on decisions reached by the agency (anonymous statistical data on such incidents should be maintained for audit and system evaluation purposes); and,

. direct agencies to consult with National Institute of Science and Technology in the development of privacy definitions and policies that reflect the mandates set forth in the Privacy Act and other privacy statues and regulations.

We are ready and willing to contribute our expertise, advice, and leadership in computing, networking, security, cryptography, and privacy. Please contact the ACM Public Policy Office in Washington at (202) 478-6312 if we can be of assistance.

Sincerely,

Barbara Simons, Ph.D.
Eugene H. Spafford, Ph.D
Co-Chairs

U.S. ACM Public Policy Committee
Association for Computing Machinery

About USACM:

USACM is the U.S. Public Policy Committee of the Association for Computing Machinery (ACM). ACM is the leading nonprofit membership organization of computer scientists and information technology professionals dedicated to advancing the art, science, engineering and application of information technology. Since 1947, ACM has been a pioneering force in fostering the open interchange of information and promoting both technical and ethical excellence in computing. Over 70,000 computer scientists and information technology professionals from around the world are members of ACM.