June 18, 2008

PRIVACY

Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-795T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Concerns have been raised about the privacy and security of personal information in light of advances in information technology and the increasingly sophisticated ways in which the government obtains and uses information. Federal agencies' use of personal information is governed by the Privacy Act of 1974 and the E-Government Act of 2002, while the Office of Management and Budget (OMB) provides implementation guidance and oversight. These laws and guidance are based on the Fair Information Practices , a set of widely accepted principles for protecting privacy.

GAO was asked to testify on its report, being released today, concerning the sufficiency of privacy protections afforded by existing laws and guidance. To do this, GAO analyzed privacy laws and guidance, compared them with the Fair Information Practices, and obtained perspectives from federal agencies as well as an expert forum.

What GAO Recommends

In its report GAO identified alternatives that the Congress should consider, including revising the scope of privacy laws to cover all personal information, requiring that the use of such information be limited to a specific purpose, and revising the structure and publication of privacy notices.

OMB commented that the Congress should consider these alternatives in the broader context of existing privacy and related statutes.

To view the full product, including the scope and methodology, click on GAO-08-795T. For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

Although privacy laws and guidance set minimum requirements for agencies, they may not consistently protect personally identifiable information in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles. Based on discussions with privacy experts and agency officials, as well as analysis of laws and related guidance, GAO identified issues in three major areas:

Applying privacy protections consistently to all federal collection and use of personal information. The Privacy Act's definition of a "system of records," which sets the scope of the act's protections, does not always apply whenever personal information is obtained and processed by federal agencies. For example, if agencies do not retrieve personal information by identifier, the act's protections do not apply. This has led experts to agree that the Privacy Act's system-of-records construct is too narrowly defined. An alternative for addressing these issues could include revising the system-of-records definition to cover all personally identifiable information collected, used, and maintained systematically by the federal government.

Ensuring that use of personally identifiable information is limited to a stated purpose. According to the Fair Information Practices, the use of personal information should be limited to a specified purpose. Yet current laws and guidance impose only modest requirements for describing the purposes for personal information and limiting how it is used. For example, agencies are not required to be specific in formulating purpose descriptions in their public notices. Overly broad specifications of purpose could allow for unnecessarily broad ranges of uses, thus calling into question whether meaningful limitations had been imposed. Alternatives for addressing these issues include setting specific limits on use of information within agencies and requiring agencies to establish formal agreements with external governmental entities before sharing personally identifiable information with them.

Establishing effective mechanisms for informing the public about privacy protections. Public notices are a primary means of establishing accountability for privacy protections and giving individuals a measure of control over the use of their personal information. Although the *Federal Register* is the government's official vehicle for issuing public notices, critics have questioned whether system-of-records notices published in the *Federal Register* effectively inform the public about government uses of personal information. Options for addressing concerns about public notices include requiring that purpose, collection limitations, and use limitations are better addressed in the content of privacy notices, and revising the Privacy Act to require that all notices be published on a standard Web site, with an address such as www.privacy.gov.