epic.org

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

March 27, 2012

The Honorable Daniel Akaka
Chairman
Subcommittee on Oversight of Government Management,
the Federal Workforce, and the District of Columbia
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Akaka,

Thank you for your request for comments from the Electronic Privacy Information Center ("EPIC") regarding S. 1732, the Privacy Act Modernization for the Information Age Act of 2011 ("Privacy Act Modernization bill").

EPIC is a nonpartisan, public interest research organization, established in 1994 to focus public attention on emerging privacy and civil liberties issues. We maintain two of the most popular privacy sites on the Internet –EPIC.ORG and PRIVACY.ORG—and testify frequently before Congress. EPIC has been a longtime advocate for promoting the privacy protections afforded by the Privacy Act of 1974. EPIC has both submitted amicus briefs to the US Supreme Court in Privacy Act cases and has also submitted extensive comments to federal agencies that have proposed to exempt systems of records from Privacy Act obligations.[1]

Overall, the Privacy Act Modernization bill makes beneficial changes to the Privacy Act of 1974: it strengthens the civil remedies and criminal penalties for improper disclosure of individual records; it establishes a Federal Chief Privacy Officer within the Office of Management and Budget and establishes a Chief Privacy Officers Council; and it updates agency Federal Register requirements for publishing system of records notices.

---

[1] *See,* Brief of *Amicus Curiae* Electronic Privacy Information Center (EPIC), Federal Aviation Administration, et al., v. Stanmore Cawthon Cooper (2011)(No. 10-1024), *available at* http://epic.org/amicus/cooper/Cooper-EPIC-Brief.pdf; Brief of *Amici Curiae* Electronic Privacy Information Center, et. al and 16 Legal Scholars and Technical Experts, Buck Doe v. Elaine Chao, Secretary of Labor, 540 U.S. 614 (2004), *available at* http://epic.org/privacy/chao/Doe_amicus.pdf; EPIC, Administrative Agency comments on a Notice of Privacy Act System of Records, Docket No. DHS-2011-0094 (Dec. 23, 2011), *available at* http://epic.org/privacy/1974act/EPIC-SORN-Comments-FINAL.pdf; EPIC, Administrative Agency comments In the Matter of Privacy Act Notice Concerning Aviation Security Screening Records, Docket No. DOT/TSA 010-OST-1996-1437 (Feb. 23, 2003), *available at* http://epic.org/privacy/airtravel/tsacomments2.24.2003.html. EPIC has submitted over 20 administrative agency comments urging federal agencies to uphold system of records privacy protections afforded by the Privacy Act. *See*, EPIC: Administrative Procedure Act (APA) Comments, *available at* http://epic.org/open_gov/apa/epic-apa-comments.html.

We support certain proposed provisions because they strengthen government accountability, act to deter agencies from violating the Privacy Act, and create oversight mechanisms for Privacy Act compliance. For example, the new law creates a Federal Chief Privacy Officer within OMB that will work together with the Chief Privacy Officers Council to establish best practices and privacy compliance for the federal government's "collection, use, sharing, disclosure, transfer, storage, security, and disposition of personally identifiable information."[2] This type of oversight will ensure that agencies properly comply with the Privacy Act. If an agency does not abide by the Privacy Act requirements, the updated law has provisions to deter noncompliance. At a minimum, the new the law would grant $1000 monetary relief to complainants that "substantially prevail[]" in proving that an agency intentionally and willfully disclosed personal records in violation of the Privacy Act.[3]

The criminal fines for violating the act would also increase under the new law. The increase in civil remedies and criminal penalties is a beneficial change to the current act because it encourages accountability and acts to deter agencies from violating the Privacy Act. When government agencies are held responsible through fines and other penalties for the way in which they illegally disclose records or otherwise violate the Privacy Act, they should be more likely to uphold the law. Lastly, the updated Federal Register system of records notice requirements will inform the public of agencies' decision-making process behind establishing or revising a system of records. Because systems of records contain extensive records on various individuals of the public, it is imperative that the government informs the public of its collection and intended uses of personal information.

EPIC does, however, have recommendations and suggested language, detailed below, to improve the bill's proposed privacy protections.

When it enacted the Privacy Act, 5 U.S.C. § 552a, in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect, and required transparency in agency information practices.[4] The Supreme Court has also underscored the importance of the Privacy Act's restrictions upon agency use of personal information, noting that:

> "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[5]

---

[2] Amendments to 44 U.S.C. 3504, S. 1732, 112th Cong. §4.

[3] Privacy Act Modernization for the Information Age Act of 2011, S. 1732, 112th Cong.§ 552a(g)(4).

[4] S. Rep. No. 93-1183 at 1 (1974).

[5] *Doe v. Chao*, 540 U.S. 614, 618 (2004).

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[]."[6] It is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion.

Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[7] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[8]

Increasingly, agencies have utilized Privacy Act exemptions to allow "mission creep" for collecting an ever-expansive list of records on a growing number of individuals. Under the Privacy Act, agencies articulate a broad-based rationale for collecting and maintaining records on individuals. Oftentimes, these records become a part of a government information sharing environment. Fusion centers are a part of the information sharing environments, and serve as hubs for aggregating records from various sources, including federal, state, local, and tribal agencies.[9] The "sharing" between government agencies largely disregards privacy protections and results in the diminution of the Privacy Act.

Although we favor many of he proposed changes, we would like to call your attention to several further matters that should be addressed.

1) The Privacy Act Modernization Bill's Proposed Definition of "Routine Use" is Overly Broad and Vague, and Insufficiently Safeguards Against Unwarranted Information Disclosure.

The current "routine use" provision of the Privacy Act, 5 U.S.C. § 552a(a)(7), states:

> (7) the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected

The Privacy Act Modernization bill amends the 5 U.S.C. § 552a(a)7 definition of "routine use" to:

> (7) the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which, as determined by the agency, is compatible with the purpose for which it was collected and is appropriate and reasonably necessary for the efficient and effective conduct of Government.

---

[6] S. Rep. No. 93-1183 at 1.

[7] Pub. L. No. 93-579 (1974).

[8] *Id.*

[9] EPIC: Information Fusion Centers and Privacy, http://epic.org/privacy/fusion/; Information Sharing Environment, http://ise.gov/scope-ise (last visited March 15, 2012).

Terms such as "as determined by the agency" and "appropriate and reasonably necessary for the efficient and effective conduct of Government" are overly broad and vague, and can easily lead to abuse of privacy rights under the Privacy Modernization Act. The Privacy Act's legislative history and a subsequent report on the Act indicate that the routine use for disclosing records must be specifically tailored for a defined purpose for which the records are collected. The legislative history states that:

> [t]he [routine use] definition should serve as a caution to agencies to think out in advance what uses it will make of information. This Act is not intended to impose undue burdens on the transfer of information . . . or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.[10]

The Privacy Act Guidelines of 1975—a commentary report on implementing the Privacy Act— interpreted the above Congressional explanation of routine use to mean that a " 'routine use' must be not only compatible with, but related to, the purpose for which the record is maintained."[11]

Agencies are already in the practice of establishing overly broad purposes under which they are permitted to collect and disclose records on individuals. Oftentimes in a tautological fashion, agencies will state in their Federal Register system of records notice that the purpose for maintaining and collecting records is to collect and maintain records on a certain group of individuals.[12]

EPIC would recommend no changes to the original definition. In the alternative, to prevent agencies from claiming broad-based routine use disclosure exemptions, EPIC proposes the following language for 5 U.S.C. § 552a(a)(7):

> (7) the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected. Under this provision, the purpose for which the agency collects information cannot be "to collect information and/or records."

Clarifying the definition in this manner would aid in preventing unwarranted disclosure of individual records, and is true to the Privacy Act's legislative intent.

---

[10] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).

[11] *Id.*

[12] *See, for example,* Privacy Act of 1974; Department of Homeland Security/United States Secret Service—003 Non-Criminal Investigation Information System of Records, 76 Fed. Reg. 66937 (proposed Oct. 28, 2011).

2) The Proposed Act Should Require Federal Agencies to Evaluate and Consider Public Comments on Proposed System of Records Before the Systems Take Effect.

The Privacy Act requires federal agencies to publish notice of their systems of records in the Federal Register. The current Privacy Act provision governing agency Federal Register requirements, 5 U.S.C. § 552a(e)(11), states:

> (11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.

The Privacy Act Modernization bill provision 5 U.S.C. § 552a(e)(2)(K) places similar Federal Register notice requirements on agencies. The Privacy Act Modernization bill 5 U.S.C. §§ 552a(e)(2)(K)(i)-(iii) states:

> (K) in regards to the establishment or revision of a system of records under subparagraph (D)—
>
> (i) at least 30 days prior to creation or modification of a system of records, publish the entire text of the proposed sys- tem of records notice in the Federal Register and on the centralized website established under subparagraph (D);
>
> (ii) provide an opportunity for interested persons to submit written or electronic data, views, or arguments to the agency regarding the proposed system of records notice;
>
> (iii) within 180 days after publication of a proposed system of records notice, publish on the centralized website established under subparagraph (D), a response to the comments received, along with notice of whether the system of records notice as published has taken effect.

The requirement that agencies respond to the comments is a positive addendum to the current Privacy Act. Requiring agencies to respond to the comments that they receive with a statement of their basis and purpose of the system of records will hold agencies accountable and help limit the instance of arbitrary and unfounded system of records. Additionally, agencies should no longer be allowed to make their system of records go into effect on the same day that comments are due.[13] This alarming practice effectively defeats the current Privacy Act system of records public comment opportunity. Agencies cannot meaningfully consider public comments on the privacy risks of a proposed system of records if the system will go into effect the same day that comments are due. To combat this issue, EPIC proposes the following change to the Privacy Act Modernization bill language:

> K) in regards to the establishment or revision of a system of records under

---

[13] *See, for example*, Notice of Privacy Act System of Records, Department of Homeland Security/ALL—017 General Legal Records System of Records, 76 Fed. Reg. 72428 (proposed Nov. 23, 2011); Notice of Privacy Act System of Records, Department of Homeland Security/ALL-030 Use of the Terrorist Screening Database System of Records, 76 Fed. Reg. 39408 (proposed July 6, 2011).

subparagraph (D)—(ii) provide an opportunity for interested persons to submit written or electronic data, views, or argument to the agency regarding the proposed system of records notice. The comment period must end before the effective date of the proposed system of records. . . (iv) If the agency receives adverse comments on the proposed system of records, the agency will withdraw the proposed system of records before it becomes effective and may issue an NPRM.[14]

3) The Proposed Amendments to the E-Government Act of 2002 Insufficiently Warn Individuals of Government Security Breaches Affecting Individual Records

The amendments to the E-Government Act of 2002 are generally positive. However, the amendments should be changed to ensure that the government adequately warns individuals of government security breaches affecting individual records. The proposed section 3565 addresses agency privacy breach requirements:

> The Director shall establish and oversee policies and procedures for agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable information and for which harm to an individual could reasonably be expected to result, including--
> (1) a requirement for timely notice to be provided to those individuals whose personally identifiable information could be compromised as a result of such breach, except no notice shall be required if the breach does not create a reasonable risk of identity theft, fraud, or other unlawful conduct regarding such individual;
> (2) guidance on determining how timely notice is to be provided;
> (3) guidance regarding whether additional actions are necessary and appropriate, including data breach analysis, fraud resolution services, identity theft insurance, and credit protection or monitoring services; and
> (4) requirements for timely reporting by the agencies of such breaches to the director and the Federal information security incident center referred to in section 3546.

EPIC recommends the following changes to the proposed privacy breach requirements:

> (1) a requirement that within 30 days for ~~timely~~ notice to be provided to those individuals whose personally identifiable information could be compromised as a result of such breach, ~~except no notice shall be required if the breach does not create a reasonable risk of identity theft, fraud, or other unlawful conduct regarding such individual~~;
> ~~(2) guidance on determining how timely notice is to be provided~~;
> (2) guidance regarding whether additional actions are necessary and appropriate, including data breach analysis, fraud resolution services, identity theft insurance, and

[14] This language is modeled after the Federal Aviation Administration regulation concerning direct final rules. FAA Rulemaking Procedures, 14 C.F.R. § 11.13 (2012).

credit protection or monitoring services with the presumption that the additional actions are necessary; and
(4) requirements for ~~timely~~ reporting within 30 days by the agencies of such breaches to the director and the Federal information security incident center referred to in section 3546.

This language places a concrete deadline on agencies to notify individuals that their personal information could be compromised as a result of a government security breach. Additionally, this language places a presumption in favor of breach notification.

4) Agency Chief Privacy Officers Should Have a Sufficient Level of Independence to Investigate Agency Misconduct

The Privacy Act Modernization bill includes a provision amending 42 U.S.C. 2000ee-1.[15] This provision details the authority of privacy officers and civil liberties officers to investigate agency privacy regulation compliance. It is crucial that any officer charged with investigating a federal agency have a sufficient level of independence in order to conduct the investigation properly

To improve independence, the Act should provide mechanisms to ensure the independence of such officers, such as giving them protections equivalent to that of the Inspector General. The Inspector General could also be charged with ensuring the legitimacy of any investigation launched by one of the privacy or civil liberties officers by having such investigation depend on either the approval of monitoring of the Inspector General.

With government agency databases amassing hundreds of thousands of records on individuals, it is imperative that the agencies are accountable for their information practices.

The Privacy Act Modernization for the Information Age Act of 2011 is a step in the right direction towards more government transparency. Including the aforementioned recommendations will strengthen privacy protections envisioned by the original Privacy Act.

Sincerely,

Marc Rotenberg,
EPIC Executive Director

Khaliah Barnes,
EPIC Open Government Fellow

---

[15] Amendments to 42 U.S.C. 2000ee-1, S. 1732, 112th Cong. §5.