AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

109TH CONGRESS, 2d Session | HOUSE OF REPRESENTATIVES | REPORT 109–675

FEDERAL AGENCY PROTECTION OF PRIVACY ACT OF 2005

SEPTEMBER 25, 2006.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. SENSENBRENNER, from the Committee on the Judiciary, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 2840]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 2840) to amend title 5, United States Code, to require that agencies, in promulgating rules, take into consideration the impact of such rules on the privacy of individuals, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
The Amendment	2
Purpose and Summary	5
Background and Need for the Legislation	6
Hearings	11
Committee Consideration	12
Vote of the Committee	12
Committee Oversight Findings	13
New Budget Authority and Tax Expenditures	13
Congressional Budget Office Cost Estimate	13
Performance Goals and Objectives	15
Constitutional Authority Statement	15
Section-by-Section Analysis and Discussion	15
Changes in Existing Law Made by the Bill, as Reported	18
Markup Transcript	24
Additional Views	67

49–006

THE AMENDMENT

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Federal Agency Protection of Privacy Act of 2005".

SEC. 2. REQUIREMENT THAT AGENCY RULEMAKING TAKE INTO CONSIDERATION IMPACTS ON INDIVIDUAL PRIVACY.

(a) IN GENERAL.—Title 5, United States Code, is amended by adding after section 553 the following new section:

"§ 553a. Privacy impact assessment in rulemaking

"(a) INITIAL PRIVACY IMPACT ASSESSMENT.—

"(1) IN GENERAL.—Whenever an agency is required by section 553 of this title, or any other law, to publish a general notice of proposed rulemaking for a proposed rule, or publishes a notice of proposed rulemaking for an interpretative rule involving the internal revenue laws of the United States, and such rule or proposed rulemaking pertains to the collection, maintenance, use, or disclosure of personally identifiable information from 10 or more individuals, other than agencies, instrumentalities, or employees of the Federal government, the agency shall prepare and make available for public comment an initial privacy impact assessment that describes the impact of the proposed rule on the privacy of individuals. Such assessment or a summary thereof shall be signed by the senior agency official with primary responsibility for privacy policy and be published in the Federal Register at the time of the publication of a general notice of proposed rulemaking for the rule.

"(2) CONTENTS.—Each initial privacy impact assessment required under this subsection shall contain the following:

"(A) A description and analysis of the extent to which the proposed rule will impact the privacy interests of individuals, including the extent to which the proposed rule—

"(i) provides notice of the collection of personally identifiable information, and specifies what personally identifiable information is to be collected and how it is to be collected, maintained, used, and disclosed;

"(ii) allows access to such information by the person to whom the personally identifiable information pertains and provides an opportunity to correct inaccuracies;

"(iii) prevents such information, which is collected for one purpose, from being used for another purpose; and

"(iv) provides security for such information, including the provision of written notice to any individual, within 14 days of the date of compromise, whose privacy interests are compromised by the unauthorized release of personally identifiable information as a result of a breach of security at or by the agency.

"(B) A description of any significant alternatives to the proposed rule which accomplish the stated objectives of applicable statutes and which minimize any significant privacy impact of the proposed rule on individuals.

"(b) FINAL PRIVACY IMPACT ASSESSMENT.—

"(1) IN GENERAL.—Whenever an agency promulgates a final rule under section 553 of this title, after being required by that section or any other law to publish a general notice of proposed rulemaking, or promulgates a final interpretative rule involving the internal revenue laws of the United States, and such rule or proposed rulemaking pertains to the collection, maintenance, use, or disclosure of personally identifiable information from 10 or more individuals, other than agencies, instrumentalities, or employees of the Federal government, the agency shall prepare a final privacy impact assessment, signed by the senior agency official with primary responsibility for privacy policy.

"(2) CONTENTS.—Each final privacy impact assessment required under this subsection shall contain the following:

"(A) A description and analysis of the extent to which the final rule will impact the privacy interests of individuals, including the extent to which such rule—

"(i) provides notice of the collection of personally identifiable information, and specifies what personally identifiable information is to be collected and how it is to be collected, maintained, used, and disclosed;

"(ii) allows access to such information by the person to whom the personally identifiable information pertains and provides an opportunity to correct inaccuracies;

"(iii) prevents such information, which is collected for one purpose, from being used for another purpose; and

"(iv) provides security for such information, including the provision of written notice to any individual, within 14 days of the date of compromise, whose privacy interests are compromised by the unauthorized release of personally identifiable information as a result of a breach of security at or by the agency.

"(B) A summary of any significant issues raised by the public comments in response to the initial privacy impact assessment, a summary of the analysis of the agency of such issues, and a statement of any changes made in such rule as a result of such issues.

"(C) A description of the steps the agency has taken to minimize the significant privacy impact on individuals consistent with the stated objectives of applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the privacy interests of individuals was rejected.

"(3) AVAILABILITY TO PUBLIC.—The agency shall make copies of the final privacy impact assessment available to members of the public and shall publish in the Federal Register such assessment or a summary thereof.

"(c) WAIVERS.—

"(1) EMERGENCIES.—An agency head may waive or delay the completion of some or all of the requirements of subsections (a) and (b) to the same extent as the agency head may, under section 608, waive or delay the completion of some or all of the requirements of sections 603 and 604, respectively.

"(2) NATIONAL SECURITY.—An agency head may, for national security reasons, or to protect from disclosure classified information, confidential commercial information, or information the disclosure of which may adversely affect a law enforcement effort, waive or delay the completion of some or all of the following requirements:

"(A) The requirement of subsection (a)(1) to make an assessment available for public comment, provided that such assessment is made available, in classified form, to the Committees on the Judiciary of the House of Representatives and the Senate, in lieu of making such assessment available to the public.

"(B) The requirement of subsection (a)(1) to have an assessment or summary thereof published in the Federal Register, provided that such assessment or summary is made available, in classified form, to the Committees on the Judiciary of the House of Representatives and the Senate, in lieu of publishing such assessment or summary in the Federal Register.

"(C) The requirements of subsection (b)(3), provided that the final privacy impact assessment is made available, in classified form, to the Committees on the Judiciary of the House of Representatives and the Senate, in lieu of making such assessment available to the public and publishing such assessment in the Federal Register.

"(d) PROCEDURES FOR GATHERING COMMENTS.—When any rule is promulgated which may have a significant privacy impact on individuals, or a privacy impact on a substantial number of individuals, the head of the agency promulgating the rule or the official of the agency with statutory responsibility for the promulgation of the rule shall assure that individuals have been given an opportunity to participate in the rulemaking for the rule through techniques such as—

"(1) the inclusion in an advance notice of proposed rulemaking, if issued, of a statement that the proposed rule may have a significant privacy impact on individuals, or a privacy impact on a substantial number of individuals;

"(2) the publication of a general notice of proposed rulemaking in publications of national circulation likely to be obtained by individuals;

"(3) the direct notification of interested individuals;

"(4) the conduct of open conferences or public hearings concerning the rule for individuals, including soliciting and receiving comments over computer networks; and

"(5) the adoption or modification of agency procedural rules to reduce the cost or complexity of participation in the rulemaking by individuals.

"(e) PERIODIC REVIEW OF RULES.—

"(1) IN GENERAL.—Each agency shall carry out a periodic review of the rules promulgated by the agency that have a significant privacy impact on individuals, or a privacy impact on a substantial number of individuals. Under such

periodic review, the agency shall determine, for each such rule, whether the rule can be amended or rescinded in a manner that minimizes any such impact while remaining in accordance with applicable statutes. For each such determination, the agency shall consider the following factors:

"(A) The continued need for the rule.

"(B) The nature of complaints or comments received from the public concerning the rule.

"(C) The complexity of the rule.

"(D) The extent to which the rule overlaps, duplicates, or conflicts with other Federal rules, and, to the extent feasible, with State and local governmental rules.

"(E) The length of time since the rule was last reviewed under this subsection.

"(F) The degree to which technology, economic conditions, or other factors have changed in the area affected by the rule since the rule was last reviewed under this subsection.

"(2) PLAN REQUIRED.—Each agency shall carry out the periodic review required by paragraph (1) in accordance with a plan published by such agency in the Federal Register. Each such plan shall provide for the review under this subsection of each rule promulgated by the agency not later than 10 years after the date on which such rule was published as the final rule and, thereafter, not later than 10 years after the date on which such rule was last reviewed under this subsection. The agency may amend such plan at any time by publishing the revision in the Federal Register.

"(3) ANNUAL PUBLICATION.—Each year, each agency shall publish in the Federal Register a list of the rules to be reviewed by such agency under this subsection during the following year. The list shall include a brief description of each such rule and the need for and legal basis of such rule and shall invite public comment upon the determination to be made under this subsection with respect to such rule.

"(f) JUDICIAL REVIEW.—

"(1) IN GENERAL.—For any rule subject to this section, an individual who is adversely affected or aggrieved by final agency action is entitled to judicial review of agency compliance with the requirements of subsections (b) and (c) in accordance with chapter 7. Agency compliance with subsection (d) shall be judicially reviewable in connection with judicial review of subsection (b).

"(2) JURISDICTION.—Each court having jurisdiction to review such rule for compliance with section 553, or under any other provision of law, shall have jurisdiction to review any claims of noncompliance with subsections (b) and (c) in accordance with chapter 7. Agency compliance with subsection (d) shall be judicially reviewable in connection with judicial review of subsection (b).

"(3) LIMITATIONS.—

"(A) An individual may seek such review during the period beginning on the date of final agency action and ending 1 year later, except that where a provision of law requires that an action challenging a final agency action be commenced before the expiration of 1 year, such lesser period shall apply to an action for judicial review under this subsection.

"(B) In the case where an agency delays the issuance of a final privacy impact assessment pursuant to subsection (c), an action for judicial review under this section shall be filed not later than—

"(i) 1 year after the date the assessment is made available to the public; or

"(ii) where a provision of law requires that an action challenging a final agency regulation be commenced before the expiration of the 1-year period, the number of days specified in such provision of law that is after the date the assessment is made available to the public.

"(4) RELIEF.—In granting any relief in an action under this subsection, the court shall order the agency to take corrective action consistent with this section and chapter 7, including, but not limited to—

"(A) remanding the rule to the agency; and

"(B) deferring the enforcement of the rule against individuals, unless the court finds that continued enforcement of the rule is in the public interest.

"(5) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit the authority of any court to stay the effective date of any rule or provision thereof under any other provision of law or to grant any other relief in addition to the requirements of this subsection.

"(6) RECORD OF AGENCY ACTION.—In an action for the judicial review of a rule, the privacy impact assessment for such rule, including an assessment prepared

or corrected pursuant to paragraph (4), shall constitute part of the entire record of agency action in connection with such review.

"(7) EXCLUSIVITY.—Compliance or noncompliance by an agency with the provisions of this section shall be subject to judicial review only in accordance with this subsection.

"(8) SAVINGS CLAUSE.—Nothing in this subsection bars judicial review of any other impact statement or similar assessment required by any other law if judicial review of such statement or assessment is otherwise permitted by law.

"(g) DEFINITION.—For purposes of this section, the term 'personally identifiable information' means information that can be used to identify an individual, including such individual's name, address, telephone number, photograph, social security number or other identifying information. It includes information about such individual's medical or financial condition.".

(b) PERIODIC REVIEW TRANSITION PROVISIONS.—

(1) INITIAL PLAN.—For each agency, the plan required by subsection (e) of section 553a of title 5, United States Code (as added by subsection (a)), shall be published not later than 180 days after the date of the enactment of this Act.

(2) REVIEW PERIOD.—In the case of a rule promulgated by an agency before the date of the enactment of this Act, such plan shall provide for the periodic review of such rule before the expiration of the 10-year period beginning on the date of the enactment of this Act. For any such rule, the head of the agency may provide for a 1-year extension of such period if the head of the agency, before the expiration of the period, certifies in a statement published in the Federal Register that reviewing such rule before the expiration of the period is not feasible. The head of the agency may provide for additional 1-year extensions of the period pursuant to the preceding sentence, but in no event may the period exceed 15 years.

(c) CONGRESSIONAL REVIEW.—Section 801(a)(1)(B) of title 5, United States Code, is amended—

(1) by redesignating clauses (iii) and (iv) as clauses (iv) and (v), respectively; and

(2) by inserting after clause (ii) the following new clause:

"(iii) the agency's actions relevant to section 553a;".

(d) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 5 of title 5, United States Code, is amended by adding after the item relating to section 553 the following new item:

"553a. Privacy impact assessment in rulemaking.".

PURPOSE AND SUMMARY

H.R. 2840, the "Federal Agency Protection of Privacy Act of 2005," requires agencies to prepare privacy impact assessments for proposed and final rules that pertain to the collection, maintenance, use, or disclosure of personally identifiable information from ten or more individuals, other than agencies, instrumentalities, or employees of the Federal Government. With limited exceptions, such assessments must be made available to the public for comment. While H.R. 2840 makes no substantive demands upon Federal agencies with respect to privacy, it does require these agencies to analyze how the rule will impact the privacy interests of individuals. This requirement is similar to other analyses that agencies

currently conduct, such as those required by the Regulatory Flexibility Act [1] and the E-Government Act of 2002.[2]

H.R. 2840 requires the agency to explain: (1) what personally identifiable information will be collected; (2) how such information will be collected, maintained, used, disclosed, and protected; (3) whether a person to whom the personally identifiable information pertains is allowed access to such information and whether such person may correct any inaccuracies; (4) how information collected for one purpose will be prevented from being used for another purpose; and (5) the steps the agency has taken to minimize any significant privacy impact that a final rule may have. In addition, the bill permits judicial review of certain final agency actions, and requires agencies to review rules on a periodic basis that have either a significant privacy impact on individuals or a privacy impact on a significant number or individuals. The bill includes a limited waiver from certain requirements for national security reasons and to prevent the disclosure of other sensitive information.

BACKGROUND AND NEED FOR THE LEGISLATION

THE FEDERAL GOVERNMENT'S USE OF PERSONAL INFORMATION AND APPLICABLE LAW

The Federal Government collects personally identifiable information on every American and uses this data for a wide variety of purposes, including law enforcement, antiterrorism activities, public safety, fraud detection, and debt collection.[3] Under certain circumstances, this information may be disseminated to various agencies within the Federal Government or shared with State and local governments.[4]

Pursuant to the Privacy Act of 1974,[5] Federal agencies are generally prohibited from disclosing personally identifiable information

---

[1] Pub. L. No. 96–354, 94 Stat. 1164 (1980) (codified at 5 U.S.C. §§ 601 *et seq.*). The Regulatory Flexibility Act requires an agency to describe the impact of proposed and final regulations on small entities (such as small businesses) if the proposed regulation is expected to have a significant economic impact on a substantial number of small entities. The agency must prepare an initial regulatory flexibility analysis (IRFA) and the IRFA, or a summary thereof, must be published for public comment in the Federal Register together with the proposed rule. Similar requirements pertain to final rules. The Small Business Regulatory Enforcement Fairness Act of 1996 subjects the regulatory flexibility analysis to judicial review. Pub. L. No. 104–121, § 242, 110 Stat. 857, 865 (1996) (codified at 5 U.S.C. § 611).

[2] Pub. L. No. 107–347, § 208, 116 Stat. 2899, 2921 (requiring a Federal agency inter alia to conduct a privacy impact assessment before developing or procuring an information technology system that collects, maintains or disseminates information in an identifiable form).

[3] *See, e.g.,* Gun Control Act of 1968, 18 U.S.C. §§ 921 *et seq.* (requiring gun dealers to submit personally identifiable information about prospective buyers to the Department of Justice); Bank Secrecy Act, 12 U.S.C. §§ 1951 *et seq.* (requiring financial institutions to maintain records of personal financial transactions that have a "high degree of usefulness in criminal, tax, or regulatory investigations or proceedings" pursuant to 12 U.S.C. § 1953(b)); Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104–193, 110 Stat. 2105 (1996) (requiring employers to report certain information for newly hired employees to the Department of Health and Human Services to facilitate the collection of unpaid child support obligations).

[4] According to one privacy think tank, Federal agencies routinely share personally identifiable information with other Federal agencies without the knowledge or consent of those whose information is being exchanged. Privacilla.org, *Privacy and Federal Agencies: Government Exchange and Merger of Citizens' Personal Information is Systematic and Routine* (Mar. 2001), *http://www.privacilla.org/releases/Government—Data—Merger.html.* Between September 1999 and February 2001, for example, there were 47 instances where Federal agencies announced "that they would exchange and merge personal information from databases about American citizens." *Id.* at 1.

[5] Pub. L. No. 93–579, § 3, 88 Stat. 1897 (codified at 5 U.S.C. § 552a). According to one treatise, the Privacy Act "gives individuals greater control over gathering, dissemination, and ensuring accuracy of information collected about themselves by agencies" and that its "main purpose" is to "forbid disclosure unless it is required by the Freedom of Information Act." ADMINISTRATIVE

to other Federal or State agencies or to any other person,[6] subject to certain specified exceptions.[7] An agency that releases such information in violation of the Privacy Act may, under certain circumstances, be sued for damages sustained by an individual as a result of such violation.[8] In addition, the Privacy Act grants individuals the right to have agency records corrected upon a showing that such records are inaccurate, irrelevant, out-of-date, or incomplete.[9]

Other laws intended to protect personal information include the E-Government Act of 2002 and the Federal Information Security Management Act of 2002, which *inter alia* were enacted "to provide enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy, national security, records retention, access for persons with disabilities, and other relevant laws."[10] These Acts require agencies to conduct privacy impact assessments for the purpose of enhancing protection for personal information collected by or maintained in government information systems.

PERSISTENT WEAKNESSES IN INFORMATION SECURITY AND ACCURACY

As technological advances facilitate the collection, use, and dissemination of personally identifiable information, the potential for misuse of such information increases. As the Government Accountability Office (GAO) warned more than 5 years ago:

> Our nation has an increasing ability to accumulate, store, retrieve, cross-reference, analyze, and link vast numbers of electronic records in an ever faster and more cost-efficient manner. These advances bring substantial Federal information benefits as well as increasing responsibilities and concerns.[11]

Thanks to the wide use of Social Security numbers[12] and the availability of other personally identifiable information through technological advances,[13] data security breaches appear to be oc-

---

CONFERENCE OF THE UNITED STATES, FEDERAL ADMINISTRATIVE PROCEDURE SOURCEBOOK—STATUTES AND RELATED MATERIALS 863 (2d ed. 1992).

[6] 5 U.S.C. § 552a(b). The types of information that may not be disclosed include medical, educational, criminal, financial, and employment records. 5 U.S.C. § 552a(a)(4).

[7] The Privacy Act, for example, excepts disclosures that constitute a "routine use" of such information by an agency that "is compatible with the purpose for which it was collected." 5 U.S.C. § 552a(7), (b)(3). It also permits disclosure for law enforcement purposes, in response to a Congressional request, pursuant to court order, for the purpose of carrying out a census, or to a consumer reporting agency. 5 U.S.C. § 552a(b).

[8] 5 U.S.C. § 552a(g)(4).

[9] 5 U.S.C. § 552a(d).

[10] Pub. L. No. 107–347, § 2(b)(11), 116 Stat. 2899, 2901 (2002).

[11] U.S. Government Accountability Office, Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information, GAO-01-126SP, at 1 (Apr. 2001).

[12] Although originally created as part of the Social Security Administration's recordkeeping system to track workers' earnings and eligibility for certain benefits, Social Security numbers have become the "identifier of choice" by government agencies and private industry as a standard identifier. U.S. Government Accountability Office, Social Security Numbers—Stronger Protections Needed When Contractors Have Access to SSNs, GAO-06-238, at 6 (Jan. 2006). Unfortunately, however, Social Security numbers "present a particular threat because they are the primary identifiers that let thieves open credit lines, apply for loans or otherwise pose as another person." Tom Zeller, Jr., *Students Surfing Public Records Learn It's Easy to Find Out a Lot,* N.Y. TIMES, May 18, 2005, at C1.

[13] *See, e.g.,* Tom Zeller, Jr., *Students Surfing Public Records Learn It's Easy to Find Out a Lot,* N.Y. TIMES, May 18, 2005, at C1 (noting that "all it takes to obtain reams of personal data is Internet access, a few dollars and some spare time").

curring with greater frequency.[14] In turn, identity theft has swiftly evolved into one of the most prolific crimes in the United States.[15] According to the Federal Trade Commission, identity theft "topped the list" of consumer complaints filed with the agency in 2005.[16] Based on a survey conducted in 2003, the Commission estimated that nearly 10 million consumers were victims of some form of identity theft in the preceding 12 months.[17] In turn, American businesses suffered an estimated $48 billion in losses, while consumers incurred an additional $5 billion in out-of-pocket losses.[18] The Justice Department estimates that "3.6 million households, or about 3 percent of all households in the nation, learned that they had been the victim of at least one type of identity theft during a 6-month period in 2004."[19] Unfortunately, "several factors have combined to make identity theft a particularly intractable crime: the growth of the Internet and digital finance, decades of expanding consumer credit worldwide, the hodgepodge nature of local and Federal law enforcement, and the changing but often still inadequate regulations governing the credit industry."[20]

Notwithstanding the serious consequences that can result when personally identifiable information can be accessed by unscrupulous individuals, the GAO has emphasized the vulnerability of personal data maintained by the Federal Government. In 2000, the GAO found that "federal computer security is fraught with weaknesses and that, as a result, critical operations and assets continue to be at risk."[21] In addition, it noted that "information security weaknesses place enormous amounts of confidential data, ranging from personal and tax data to proprietary business information, at

---

[14] *See, e.g., Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use: Hearing Before the S. Comm. on the Judiciary,* 109th Cong. (2005) (statement of William H. Sorrell, Attorney General of the State of Vermont and President of the National Association of Attorneys General, at 2) (noting the "rising incidence of [security] breaches at private companies and public institutions that exposed consumers' personal information to unauthorized third parties" and that "these breaches involve the personal information of tens of thousands, hundreds of thousands, and even millions of records about consumers nationwide"); Eric Dash, *Regulators Start Inquiry in Data Loss,* N.Y. TIMES, June 22, 2005, at C1 (reporting that "information from 40 million credit and debt card accounts was exposed after an intruder gained access to CardSystems' [a credit card payment processor] computer network"); Jon Swartz, *Tapes with Data on 3.9M Missing,* USA TODAY, June 6, 2005, at 1B (reporting that CitiFinancial, the consumer finance division of Citigroup Inc., "is notifying 3.9 million U.S. customers that computer tapes containing . . . Social Security numbers, names and addresses" were missing); Molly M. Peterson, Into the *(Privacy) Breach,* CONGRESSDAILY AM, May 11, 2005, at 5 (noting that Bank of America, LexisNexis, Direct Shoe Warehouse and Time Warner, among other businesses, had disclosed "large-scale data security lapses in recent months"); Paul Nowell, *Bank of America Says Tapes with Customer Data Lost,* ASSOCIATED PRESS, Feb. 25, 2005 (reporting that the Bank of America Corporation lost computer data tapes "containing personal information on 1.2 million Federal employees, including some members of the U.S. Senate").

[15] *See, e.g.,* Timothy L. O'Brien, *Gone In 60 Seconds,* N.Y. TIMES, Oct. 24, 2004, at C1 (noting that identity theft is "at the forefront of one of the fastest-growing white-collar crimes in the country").

[16] Press Release, FTC Releases Top 10 Consumer Fraud Complaint Categories, at 1 (Jan. 25, 2006), *at http://www.ftc.gov/opa/2006/01/topten.htm.* Identity theft accounted for 37% of the 686,683 complaints filed with the agency. *Id.*

[17] *Data Breaches and Identity Theft: Hearing before the S. Comm. on Commerce, Science, and Transportation,* 109th Cong. (2005) (prepared statement of Deborah Platt Majoras, Chair, Federal Trade Commission, at 3).

[18] *Id.*

[19] Press Release, U.S. Dep't of Justice Bureau of Justice Statistics, 3.6 Million U.S. Households Learned They Were Identity Theft Victims During a Six-Month Period in 2004, at 1 (Apr. 2, 2006). These findings were based on interviews conducted from July through December 2004 as part of the Bureau of Justice Statistics National Crime Victimization Survey. *Id.*

[20] Timothy O'Brien, *Gone in 60 Seconds,* N.Y. TIMES, Oct. 24, 2004, at C1.

[21] U.S. Government Accountability Office, Information Security: Serious and Widespread Weaknesses Persist At Federal Agencies, GAO-00-295, at 2 (Sept. 2000).

risk of inappropriate disclosure."[22] Agencies cited in this highly critical report included the Treasury Department,[23] the Department of Health and Human Services,[24] and the Social Security Administration.[25]

Problems with how Federal agencies secure and protect personal information persist.[26] Federal agencies that have failed to secure personally identifiable information in recent years include the Veterans Administration (VA) and the Pentagon. The VA maintains detailed records to facilitate the management of its finances, oversight of its employees, and delivery of health care benefits to military veterans and their families. For example, the privacy of those who receive treatment in VA facilities was compromised by VA employees who wrote more than $1.2 million in fraudulent benefit checks from 1998 to 2001.[27] In 2002, computer equipment con-

---

[22] *Id.*

[23] *Id.* at 9 (noting, for example, that the IRS's computer security controls "continued to place taxpayer and other data in IRS' automated systems at serious risk of unauthorized disclosure, modification, or destruction").

[24] *Id.* at 12–13 (noting that the most "significant" problems were associated with the Department's Health Care Financing Administration, which was responsible in fiscal year 1999 for processing health care claims for more than 39.5 million beneficiaries and outlays of $299 billion).

[25] *Id.* at 14 (noting that such weaknesses "might allow an individual or group to fraudulently obtain [Social Security] payments by creating fictitious beneficiaries or increasing payment amounts").

[26] For example, the GAO, in a report issued in August 2005 regarding certain data mining activities undertaken by five Federal agencies, found that while the agencies "took many of the key steps required by Federal law and executive branch guidance for the protection of personal information, none followed all key procedures." U.S. Government Accountability Office, Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain, GAO-05-866, at 3 (Aug. 2005). In particular, the GAO cited that "[a]gencies' compliance with key security requirements that are intended to protect the confidentiality and integrity of personal information was inconsistent." *Id.*

Also last year, the GAO reported that the Internal Revenue Service (IRS) failed to address 21 out of 53 information security weaknesses that the GAO previously cited in 2002. U.S. Government Accountability Office, Information Security: Internal Revenue Service Needs to Remedy Serious Weaknesses over Taxpayer and Bank Secrecy Data, GAO-05-482, at 2 (Apr. 2005). The GAO concluded, "Collectively, these weaknesses increase the risk that sensitive taxpayer and Bank Secrecy Act data will not be adequately protected from unauthorized disclosure, modification, use or loss." *Id.*

Earlier this year, the GAO found that "[s]ignificant weaknesses in information security controls at HHS [Department of Health and Human Services] and at CMS [Centers for Medicare & Medicaid Services] in particular put at risk the confidentiality, integrity, and availability of their sensitive information and information systems." U.S. Government Accountability Office, Information Security: Department of Health and Human Services Needs to Fully Implement Its Program, GAO-06-267, at 2 (Feb. 2006). The GAO continued:

> HHS has not consistently implemented effective electronic access controls designed to prevent, limit, and detect unauthorized access to sensitive financial and medical information at its operating divisions and contractor-owned facilities. Numerous electronic access control vulnerabilities related to network management, user accounts and passwords, user rights and file permissions, and auditing and monitoring of security-related event exist in its computer networks and systems. In addition, weaknesses exist in controls designed to physically secure computer resources, conduct suitable background investigations, segregate duties appropriately, and prevent unauthorized changes to application software. These weaknesses increase the risk that unauthorized individuals can gain access to HHS information systems and inadvertently or deliberately disclose, modify, or destroy the sensitive medical and financial data that the department relies on to deliver its vital services.

Id.

And, in response to a request from House Judiciary Committee Chairman Sensenbrenner to review the security of Social Security numbers and cards, the GAO reported last March that while the Social Security Administration had undertaken some measures to help safeguard these items, the agency still needed to resolve various critical issues. U.S. Government Accountability Office, Social Security Administration: Improved Agency Coordination Needed for Social Security Card Enhancement Efforts, GAO-06-303, at 3–4 (Mar. 2006).

[27] *See Hearing II Information Technology: Hearings Before the H. Comm. on Veterans' Affairs, Subcomm. on Oversight and Investigations,* 106th Cong. (2000) (prepared testimony of Michael Slachta, Jr., Assistant Inspector General for Auditing, Office of Inspector General, Department of Veterans Affairs).

Continued

taining the personal information for approximately 562,000 individuals was stolen from a Pentagon contractor that handles medical claims for the military.[28]

In May 2006, it was discovered that personal information for more than 26 million veterans and 2.2 current military servicemembers was "stolen from the residence of a Department of Veterans Affairs employee who had taken the data home without authorization."[29] Fortunately, the computer containing this personal information was subsequently retrieved without any detectable data breach.[30] In response to this incident, the Comptroller General of the United States testified on June 8, 2006 that among the actions agencies should take is "to develop a privacy impact assessment—an analysis of how personal information is collected, stored, shared, and managed in a Federal information system—whenever information technology is used to process personal information."[31]

In addition to the security of personal information data collected and maintained by Federal agencies, a related concern pertains to the accuracy of such information. In the absence of data quality, an American may be mistakenly denied a job, subjected to additional screening at an airport, or even worse erroneously placed on a criminal or terrorist watch list. As Justice Sandra Day O'Connor observed:

> Surely it would not be reasonable for the police to rely, say, on a recordkeeping system, their own or some other agency's, that has no mechanism to ensure its accuracy over time and that routinely leads to false arrests, even years after the probable cause for any such arrest has ceased to exist (if it ever existed).

Well before this incident, the GAO, in addition, had repeatedly cited weaknesses in the VA's computer security systems:

> Over the past several years we have reported on VA's computer security weaknesses. In September 1998 we reported that computer security weaknesses placed critical VA operations such as financial management, health care delivery, and benefits payments at risk of misuse and disruption. We reported in October 1999 that VA's success in improving computer security largely depended on strong commitment and adequate resources being dedicated to the information security program plan. In May 2000 we testified that VA had still not adequately limited the access granted to authorized users, appropriately segregated incompatible duties among computer personnel, adequately managed user identification and passwords, or routinely monitored access activity.
>
> Earlier this month, we reported that serious computer security problems persisted throughout the department and VHA because VA had not yet fully implemented an integrated security management program and VHA had not effectively managed computer security at its medical facilities. Consequently, financial transaction data and personal information on veterans' medical records continued to face increased risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction. Specifically, as we reported, VA's New Mexico, North Texas, and Maryland health care systems had not adequately controlled access granted to authorized users, prevented employees from performing incompatible duties, secured access to networks, restricted physical access to computer resources, or ensured the continuation of computer processing operations in case of unexpected interruption.

Id. (prepared statement of Statement of Joel C. Willemssen, Director, Civil Agencies Information Systems Accounting and Information Management Division, U.S. Government Accountability Office) (footnote references omitted).

[28] Jennifer 8. Lee, *Identity Theft Complaints Double in '02, Continuing Rise,* N.Y. TIMES, Jan. 23, 2003, at A18.

[29] David Stout & Tom Zeller, Jr., *Vast Data Cache About Veterans Has Been Stolen,* N.Y. TIMES, May 23, 2006, at A1; Ann Scott Tyson & Christopher Lee, *Data Theft Affected Most in Military—National Security Concerns Raised,* WASH. POST, June 7, 2006, at A1.

[30] Christopher Lee, *VA to Encrypt Data After Loss of Second Computer,* WASH. POST, Aug. 15, 2006, at A11.

[31] *Once More into the Data Breach—The Security of Personal Information at Federal Agencies: Hearing Before the H. Comm. on Government Reform,* 109th Cong. (2006) (prepared statement of David M. Walker, Comptroller General of the United States, at 2).

> In recent years, we have witnessed the advent of powerful, computer-based recordkeeping systems that facilitate arrests in ways that have never before been possible. The police, of course, are entitled to enjoy the substantial advantages this technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.[32]

GAO INVESTIGATION OF THE GOVERNMENT'S USE OF DATA PROVIDED BY INFORMATION RESELLERS

On March 9, 2005, Chairman Sensenbrenner, Ranking Member Conyers, Constitution Subcommittee Chairman Chabot, and Constitution Subcommittee Ranking Member Nadler requested the GAO to review the "legality of data acquisition, verification, and security procedures" and to examine the "overall magnitude of government contracts with ChoicePoint Inc. and similar database companies."[33] In response to this request, the GAO prepared an 87-page report on the results of its investigation together with several recommendations.[34] The GAO found that agency practices for handling personal information were "uneven."[35] For example, although agencies notify the public through Federal Register notices about their collection of personal information, they "do not always indicate specifically that information resellers are among those sources."[36] In addition, the GAO observed that "some agencies lack robust audit mechanisms to ensure that the use of personal information from information resellers is for permissible purposes, reflecting an uneven application of the accountability principle."[37] The GAO also noted the absence of guidance from the Office of Management and Budget regarding the applicability of the Privacy Act to information obtained from resellers.[38]

HEARINGS

The Committee on the Judiciary held no hearings on H.R. 2840. In the 108th Congress, the Committee's Subcommittee on Commercial and Administrative Law and the Subcommittee on the Constitution jointly held one hearing on similar legislation (H.R. 338) on July 22, 2003.[39] Testimony was received from United States Senator Charles E. Grassley (R-IA), former Congressman Bob Barr

---

[32] *Arizona v. Evans,* 514 U.S. 1, 17–18 (O'Connor, J., concurring) (original emphasis).

[33] Letter from F. James Sensenbrenner, Jr., Chairman, Committee on the Judiciary, U.S. House of Representatives, *et al.* to David M. Walker, Comptroller General of the United States, U.S. Government Accountability Office, at 1 (Mar. 9, 2005) (on file with the Subcommittee on Commercial and Administrative Law).

[34] U.S. Government Accountability Office, Personal Information: Agency and Reseller Adherence to Key Privacy Principles, GAO-06-421 (Apr. 2006). On April 4, 2006, the Subcommittee on Commercial and Administrative Law and the Subcommittee on the Constitution held a joint oversight hearing on this report. *Personal Information Acquired by the Government from Information Resellers: Is There Need for Improvement?: Hearing Before the Subcomm. on Commercial and Administrative Law and the Subcommittee on the Constitution of the H. Comm. on the Judiciary,* 109th Cong. (2006).

[35] U.S. Government Accountability Office, Personal Information: Agency and Reseller Adherence to Key Privacy Principles, GAO-06-421, at 51 (Apr. 2006).

[36] *Id.* at 5.

[37] *Id.* at 5–6 (original emphasis).

[38] *Id.* at 6, 50, 56–59.

[39] *Defense of Privacy Act and Privacy in the Hands of the Government: Joint Hearing on H.R. 338 Before the Subcomm. on Commercial and Administrative Law and the Subcomm. on the Constitution of the H. Comm. on the Judiciary,* 108th Cong. (2003).

(R-GA) on behalf of the American Conservative Union, and representatives from the American Civil Liberties Union and the Center for Democracy & Technology.

COMMITTEE CONSIDERATION

On May 17, 2006, the Subcommittee on Commercial and Administrative Law met in open session and ordered favorably reported the bill, H.R. 2840, by voice vote, a quorum being present. On June 7, 2006, the Committee met in open session and ordered favorably reported the bill, H.R. 2840, with an amendment, by voice vote, a quorum being present.

VOTE OF THE COMMITTEE

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee notes that the following rollcall vote occurred during the Committee's consideration of H.R. 2840.

1. An amendment by Mr. Conyers, as amended by Mr. Nadler, making the provisions of the Federal Agency Protection of Privacy Act relating to privacy impact assessments (subject to any restrictions set forth in the Act) applicable to the collection, maintenance, use, or disclosure of personally identifiable information, including any action or authorization relating to the wiretapping or other electronic surveillance of communications by citizens of the United States, and the acquisition or compilation of call records, unless such actions are conducted pursuant to a court order or warrant, or the provisions of the FISA Act. Defeated 12 to 14.

ROLLCALL NO. 1

	Ayes	Nays	Present
Mr. Hyde			
Mr. Coble		X	
Mr. Smith (Texas)			
Mr. Gallegly			
Mr. Goodlatte		X	
Mr. Chabot		X	
Mr. Lungren		X	
Mr. Jenkins		X	
Mr. Cannon		X	
Mr. Bachus			
Mr. Inglis			
Mr. Hostettler		X	
Mr. Green		X	
Mr. Keller		X	
Mr. Issa			
Mr. Flake			
Mr. Pence			
Mr. Forbes		X	
Mr. King		X	
Mr. Feeney		X	
Mr. Franks		X	
Mr. Gohmert			
Mr. Conyers	X		
Mr. Berman			
Mr. Boucher			
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt			
Ms. Lofgren			

ROLLCALL NO. 1—Continued

	Ayes	Nays	Present
Ms. Jackson Lee	X		
Ms. Waters			
Mr. Meehan	X		
Mr. Delahunt	X		
Mr. Wexler	X		
Mr. Weiner	X		
Mr. Schiff	X		
Ms. Sánchez	X		
Mr. Van Hollen	X		
Ms. Wasserman Schultz	X		
Mr. Sensenbrenner, Chairman		X	
Total	12	14	

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee reports that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 3(c)(2) of rule XIII of the Rules of the House of Representatives is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 2840, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, June 29, 2006.

Hon. F. JAMES SENSENBRENNER, Jr., *Chairman,*
Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 2840, the "Federal Agency Protection of Privacy Act of 2005."

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Matthew Pickford, who can be reached at 226–2860.

Sincerely,

DONALD B. MARRON,
ACTING DIRECTOR.

Enclosure

cc: Honorable John Conyers, Jr.
Ranking Member

H.R. 2840—Federal Agency Protection of Privacy Act of 2005.

H.R. 2840 would require federal agencies to assess proposed regulations to determine their impact on the privacy of individuals. The legislation would exclude any agency rule that does not have an impact on personal identification information. H.R. 2840 also would require agencies issuing rules with a potentially significant impact on individual privacy to ensure that individuals have been given ample opportunity to participate in such rulemakings. In addition, the bill would require government agencies to notify any individual whose personally identifiable information has been unlawfully released by the government. Finally, agencies would have to review existing rules to consider the impact on the privacy of individuals at least every 10 years.

CBO estimates that implementing H.R. 2840 would have no significant effect on federal spending and no impact on federal revenues. The bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of State, local, or tribal governments.

Based on a review of the number and types of agency rules published in recent years, CBO expects that only a small percentage of the rules published annually affect the collection, maintenance, use, or disclosure of personally identifiable information. H.R. 2840 would add to existing regulatory procedures concerning the impact on the privacy of individuals that are already performed by agencies under the Privacy Act of 1974, the Paperwork Reduction Act, the e-Government Act of 2002, and other requirements related to information collected from the public that are specified by the Office of Management and Budget. Based on information from some agencies that would be affected by the bill, we expect that implementing H.R. 2840 would not require significant additional efforts by rulemaking agencies.

In the event that a federal agency inappropriately allows access to personally identifiable information, H.R. 2840 would require that agency to provide written notice to affected individuals within 14 days. The cost of such notification would depend on the number of security breaches that occur and the number of persons affected, but in most circumstances, it appears that agencies are likely to provide a written notice to affected individuals under current law. (For example, the Department of Veterans Affairs recently lost personal data for millions of veterans and active-duty military personnel, and notified approximately 17 million individuals at a cost of about $8 million.) Therefore, implementing H.R. 2840 would probably not lead to a significant increase in spending for such notification expenses.

The CBO staff contact for this estimate is Matthew Pickford, who can be reached at 226–2860. This estimate was approved by Robert A. Sunshine, Assistant Director for Budget Analysis.

PERFORMANCE GOALS AND OBJECTIVES

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R.2840 protects the privacy of all Americans by requiring that Federal agencies access, consider, and inform the public about the privacy impact of certain rules noticed for public comment under the Administrative Proce-

dure Act. The bill is intended to ensure that Federal agencies safeguard individual privacy rights by requiring them to consider the privacy implications presented by the collection, maintenance, use, disclosure, and protection of personally identifiable information.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds the authority for this legislation in article 1, section 8, and the Fourth Amendment of the Constitution.

SECTION-BY-SECTION ANALYSIS AND DISCUSSION

The following discussion describes the bill as reported by the Committee.

Sec. 1. Short Title. Section 1 sets forth the title of the bill as the "Federal Agency Protection of Privacy Act of 2005."

Sec. 2. Requirement That Agency Rulemaking Take Into Consideration Impacts on Individual Privacy. Section 2(a) of the Act amends title 5 of the United States Code to add a new section (553a) that requires an agency to prepare an initial privacy impact assessment for a proposed rule noticed for public comment (including an interpretive rule regarding the Internal Revenue Code) if such rule pertains to the collection, maintenance, use, or disclosure of personally identifiable information from ten or more individuals, other than agencies, instrumentalities, or employees of the Federal Government. The assessment must describe the impact that the proposed rule has on the privacy of individuals.

Pursuant to new section 553a(a)(1), the assessment (or summary thereof) must be signed by the senior agency official with primary responsibility for privacy policy and published in the Federal Register at the time of the publication of a general notice of proposed rulemaking for the rule.

New section 553a(a)(2) requires the following matters to be set forth in the assessment: (1) a description and analysis of the extent to which the proposed rule will impact the privacy interests of individuals, including the extent to which the proposed rule provides notice that personally identifiable information is being collected, what information is to be collected, and how such information will be collected, maintained, used, and disclosed; (2) the extent to which a person to whom the information pertains has access to such information and whether he or she will have an opportunity to correct inaccuracies; and (3) the extent to which the rule prevents such information, which is collected for one purpose, from being used for another purpose.

In addition, the assessment must describe the extent to which such information is protected, including the provision of written notice to any individual, within 14 days of the date of compromise, whose privacy interests are compromised by the unauthorized release of personally identifiable information as a result of a breach of security at or by the agency. Further, the assessment must describe any significant alternatives to the proposed rule that accomplish the stated objectives of applicable statutes and that minimize any significant privacy impact of the proposed rule.

New section 553a(b) imposes similar requirements for a final rule that pertains to the collection, maintenance, use, or disclosure of personally identifiable information from ten or more individuals, other than agencies, instrumentalities, or employees of the Federal Government. As with a proposed rule, the assessment for a final rule noticed for proposed rulemaking must be signed by the senior agency official with primary responsibility for privacy policy. In addition, the assessment (or summary thereof) must be published in the Federal Register at the time of the publication of a general notice of proposed rulemaking for the final rule, pursuant to new section 553a(b).

Pursuant to new section 553a(b)(2), the following matters must be set forth in the assessment: (1) a description and analysis of the extent to which the final rule will impact the privacy interests of individuals, including the extent to which the proposed rule provides notice that personally identifiable information is being collected, what information is to be collected, and how such information will be collected, maintained, used, and disclosed; (2) the extent to which a person to whom the information pertains has access to such information and whether he or she will have an opportunity to correct inaccuracies; and (3) the extent to which the rule prevents such information, which is collected for one purpose, from being used for another purpose. In addition, the assessment must describe the extent to which such information is protected, including the provision of written notice to any individual, within 14 days of the date of compromise, whose privacy interests are compromised by the unauthorized release of personally identifiable information as a result of a breach of security at or by the agency.

The assessment must also include a summary of any significant issues raised by the public comments in response to the initial privacy impact assessment, a summary of the agency's analysis of such issues, and a statement of any changes made to the final rule as a result of such issues. Further, the assessment must describe the agency's efforts to minimize the significant privacy impact on individuals consistent with the objective of the rules and applicable statutes, including an analysis of other alternatives that may have a less adverse impact on privacy. The agency must make copies of the final privacy impact assessment available to the public and publish the assessment (or a summary thereof) in the Federal Register.

New section 553a(c) contains two waivers. Section 553a(c)(1) permits an agency head to waive or delay the completion of some or all of the requirements set forth for proposed and final rules to the same extent as permitted under section 608 of title 5 of the United States Code (with respect to sections 603 and 604 of that title). Section 608, as part of the Regulatory Flexibility Act, permits an agency head to waive or delay the completion of some or all of the requirements for notice and public comment by publishing in the Federal Register a written finding, with reasons therefor, that the final rule is being promulgated in response to an emergency that makes compliance or timely compliance with such requirements impracticable.

Section 553a(c)(2) permits an agency head to waive or delay certain requirements for national security reasons or to protect from disclosure classified information, confidential commercial informa-

tion, or information—the disclosure of which—may adversely affect a law enforcement effort. With respect to proposed rules, this waiver pertains to the requirement to make the initial privacy impact assessment available for public comment and to have the assessment published in the Federal Register. For final rules, the waiver pertains to the requirement to make the final privacy impact assessment available to the public and to the publication of such assessment in the Federal Register.

In any instance where new section 553a(c)(2) applies, the assessment must be made available in classified form to the Committees on the Judiciary of the House of Representatives and the Senate, in lieu of making such assessment available to the public or publishing such assessment in the Federal Register.

New section 553a(d) sets forth the procedures for gathering public comments. For any rule that may have a significant privacy impact on individuals or a privacy impact on a substantial number of individuals, the provision requires the agency head (or agency official with statutory responsibility for the rule's promulgation) to assure that individuals are given an opportunity to participate in the rulemaking process through various techniques.

New section 553a(e) requires each agency to conduct a periodic review of its rules having a significant privacy impact on individuals or a privacy impact on a substantial number of individuals to determine whether they should be amended or rescinded in a manner that minimizes any such impact while remaining in accordance with applicable law. In making this determination, the agency must consider: (1) whether there is a continuing need for the rule; (2) the nature of complaints or comments received from the public concerning the rule; (3) the rule's complexity; (4) the extent to which the rule overlaps, duplicates, or conflicts with other federal, state and local governmental rules; (5) the length of time since the rule was last reviewed under this provision; and (6) whether technological, economic conditions, or other factors have changed in the area affected by the rule since it was last reviewed under this provision.

The periodic review must be conducted in accordance with a plan published by the agency in the Federal Register. The plan must provide that each rule promulgated by the agency be reviewed no later than 10 years after it was published as a final rule and thereafter no later than 10 years after the date on which it was last reviewed. In addition, the agency must annually publish a list of rules to be reviewed in compliance with this provision.

New section 553a(f)(1) permits an individual adversely affected or aggrieved by final agency action to seek judicial review of an agency's compliance with the requirements applicable to final privacy impact assessments (as set forth in new section 553a(b)) and with respect to the waiver provision (as set forth in new section 553a(c)). Agency compliance with new section 553a(d) (concerning public participation) is judicially reviewable in connection with judicial review of new section 553a(b) (dealing with final privacy impact assessments).

New section 553a(f)(2) specifies the jurisdictional and time limits applicable to judicial review. Judicial review, pursuant to new section 553a(f)(3), must be sought within 1 year from the date of final agency action, or within any shorter period of time required under

applicable law. If the agency delays the issuance of a final privacy impact assessment, the action for judicial review must be filed within 1 year from the date the assessment is made public, or within any shorter period of time required under applicable law.

Pursuant to new section 553a(f)(4), a court may order the agency to take corrective action, including remanding the rule to the agency or deferring its enforcement. New section 553a(f)(5) provides that this provision may not be construed to limit a court's authority to stay the effective date of a rule under any other law or to grant other relief.

New section 553a(f)(6), (7) and (8) detail what constitutes the record of agency action and the exclusivity of judicial review as well as specify that the provision does not bar judicial review of any other assessment if such review is otherwise permitted by law.

New section 553a(g) defines "personally identifiable information" as information that can be used to identify an individual, including such individual's name, address, telephone number, photograph, Social Security number, or other identifying information, including medical or financial information.

Section 2(b) of the Act requires an agency to publish the plan required under new section 553a(e) within 180 days from the date of the Act's enactment. For a rule promulgated prior to the enactment of this Act, the plan must provide for the periodic review of such rule within 10 years from the Act's enactment date. This 10-year period may be extended for additional one-year periods, under certain circumstances. In no event, however, may the overall period exceed 15 years.

Section 2(c) of H.R. 2840 amends section 801(a)(1)(B) of title 5 of the United States Code to provide for Congressional review of an agency's actions relevant to new section 553a, as added by this Act.

Section 2(d) of the bill amends the table of sections for chapter 5 of the United States Code to include a reference to section 553a, as added by this Act.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, existing law in which no change is proposed is shown in roman):

TITLE 5, UNITED STATES CODE

* * * * * * *

PART I—THE AGENCIES GENERALLY

* * * * * * *

CHAPTER 5—ADMINISTRATIVE PROCEDURE

SUBCHAPTER I—GENERAL PROVISIONS

Sec.
500. Administrative practice; general provisions.

* * * * * * *

SUBCHAPTER II—ADMINISTRATIVE PROCEDURE

* * * * * * *

553. Rule making.
553a. Privacy impact assessment in rulemaking.

* * * * * * *

SUBCHAPTER II—ADMINISTRATIVE PROCEDURE

* * * * * * *

§ 553a. Privacy impact assessment in rulemaking

(a) INITIAL PRIVACY IMPACT ASSESSMENT.—

(1) IN GENERAL.—Whenever an agency is required by section 553 of this title, or any other law, to publish a general notice of proposed rulemaking for a proposed rule, or publishes a notice of proposed rulemaking for an interpretative rule involving the internal revenue laws of the United States, and such rule or proposed rulemaking pertains to the collection, maintenance, use, or disclosure of personally identifiable information from 10 or more individuals, other than agencies, instrumentalities, or employees of the Federal government, the agency shall prepare and make available for public comment an initial privacy impact assessment that describes the impact of the proposed rule on the privacy of individuals. Such assessment or a summary thereof shall be signed by the senior agency official with primary responsibility for privacy policy and be published in the Federal Register at the time of the publication of a general notice of proposed rulemaking for the rule.

(2) CONTENTS.—Each initial privacy impact assessment required under this subsection shall contain the following:

(A) A description and analysis of the extent to which the proposed rule will impact the privacy interests of individuals, including the extent to which the proposed rule—

(i) provides notice of the collection of personally identifiable information, and specifies what personally identifiable information is to be collected and how it is to be collected, maintained, used, and disclosed;

(ii) allows access to such information by the person to whom the personally identifiable information pertains and provides an opportunity to correct inaccuracies;

(iii) prevents such information, which is collected for one purpose, from being used for another purpose; and

(iv) provides security for such information, including the provision of written notice to any individual, within 14 days of the date of compromise, whose privacy interests are compromised by the unauthorized release of personally identifiable information as a result of a breach of security at or by the agency.

(B) A description of any significant alternatives to the proposed rule which accomplish the stated objectives of applicable statutes and which minimize any significant privacy impact of the proposed rule on individuals.

(b) FINAL PRIVACY IMPACT ASSESSMENT.—

(1) IN GENERAL.—Whenever an agency promulgates a final rule under section 553 of this title, after being required by that section or any other law to publish a general notice of proposed rulemaking, or promulgates a final interpretative rule involving the internal revenue laws of the United States, and such rule or proposed rulemaking pertains to the collection, maintenance, use, or disclosure of personally identifiable information from 10 or more individuals, other than agencies, instrumentalities, or employees of the Federal government, the agency shall prepare a final privacy impact assessment, signed by the senior agency official with primary responsibility for privacy policy.

(2) CONTENTS.—Each final privacy impact assessment required under this subsection shall contain the following:

(A) A description and analysis of the extent to which the final rule will impact the privacy interests of individuals, including the extent to which such rule—

(i) provides notice of the collection of personally identifiable information, and specifies what personally identifiable information is to be collected and how it is to be collected, maintained, used, and disclosed;

(ii) allows access to such information by the person to whom the personally identifiable information pertains and provides an opportunity to correct inaccuracies;

(iii) prevents such information, which is collected for one purpose, from being used for another purpose; and

(iv) provides security for such information, including the provision of written notice to any individual, within 14 days of the date of compromise, whose privacy interests are compromised by the unauthorized release of personally identifiable information as a result of a breach of security at or by the agency.

(B) A summary of any significant issues raised by the public comments in response to the initial privacy impact assessment, a summary of the analysis of the agency of such issues, and a statement of any changes made in such rule as a result of such issues.

(C) A description of the steps the agency has taken to minimize the significant privacy impact on individuals consistent with the stated objectives of applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the privacy interests of individuals was rejected.

(3) AVAILABILITY TO PUBLIC.—The agency shall make copies of the final privacy impact assessment available to members of the public and shall publish in the Federal Register such assessment or a summary thereof.

(c) WAIVERS.—

(1) EMERGENCIES.—An agency head may waive or delay the completion of some or all of the requirements of subsections (a) and (b) to the same extent as the agency head may, under section 608, waive or delay the completion of some or all of the requirements of sections 603 and 604, respectively.

(2) NATIONAL SECURITY.—An agency head may, for national security reasons, or to protect from disclosure classified information, confidential commercial information, or information the disclosure of which may adversely affect a law enforcement effort, waive or delay the completion of some or all of the following requirements:

(A) The requirement of subsection (a)(1) to make an assessment available for public comment, provided that such assessment is made available, in classified form, to the Committees on the Judiciary of the House of Representatives and the Senate, in lieu of making such assessment available to the public.

(B) The requirement of subsection (a)(1) to have an assessment or summary thereof published in the Federal Register, provided that such assessment or summary is made available, in classified form, to the Committees on the Judiciary of the House of Representatives and the Senate, in lieu of publishing such assessment or summary in the Federal Register.

(C) The requirements of subsection (b)(3), provided that the final privacy impact assessment is made available, in classified form, to the Committees on the Judiciary of the House of Representatives and the Senate, in lieu of making such assessment available to the public and publishing such assessment in the Federal Register.

(d) PROCEDURES FOR GATHERING COMMENTS.—When any rule is promulgated which may have a significant privacy impact on individuals, or a privacy impact on a substantial number of individuals, the head of the agency promulgating the rule or the official of the agency with statutory responsibility for the promulgation of the rule shall assure that individuals have been given an opportunity to participate in the rulemaking for the rule through techniques such as—

(1) the inclusion in an advance notice of proposed rulemaking, if issued, of a statement that the proposed rule may have a significant privacy impact on individuals, or a privacy impact on a substantial number of individuals;

(2) the publication of a general notice of proposed rulemaking in publications of national circulation likely to be obtained by individuals;

(3) the direct notification of interested individuals;

(4) the conduct of open conferences or public hearings concerning the rule for individuals, including soliciting and receiving comments over computer networks; and

(5) the adoption or modification of agency procedural rules to reduce the cost or complexity of participation in the rulemaking by individuals.

(e) PERIODIC REVIEW OF RULES.—

(1) IN GENERAL.—Each agency shall carry out a periodic review of the rules promulgated by the agency that have a signifi-

cant privacy impact on individuals, or a privacy impact on a substantial number of individuals. Under such periodic review, the agency shall determine, for each such rule, whether the rule can be amended or rescinded in a manner that minimizes any such impact while remaining in accordance with applicable statutes. For each such determination, the agency shall consider the following factors:

(A) The continued need for the rule.

(B) The nature of complaints or comments received from the public concerning the rule.

(C) The complexity of the rule.

(D) The extent to which the rule overlaps, duplicates, or conflicts with other Federal rules, and, to the extent feasible, with State and local governmental rules.

(E) The length of time since the rule was last reviewed under this subsection.

(F) The degree to which technology, economic conditions, or other factors have changed in the area affected by the rule since the rule was last reviewed under this subsection.

(2) PLAN REQUIRED.—Each agency shall carry out the periodic review required by paragraph (1) in accordance with a plan published by such agency in the Federal Register. Each such plan shall provide for the review under this subsection of each rule promulgated by the agency not later than 10 years after the date on which such rule was published as the final rule and, thereafter, not later than 10 years after the date on which such rule was last reviewed under this subsection. The agency may amend such plan at any time by publishing the revision in the Federal Register.

(3) ANNUAL PUBLICATION.—Each year, each agency shall publish in the Federal Register a list of the rules to be reviewed by such agency under this subsection during the following year. The list shall include a brief description of each such rule and the need for and legal basis of such rule and shall invite public comment upon the determination to be made under this subsection with respect to such rule.

(f) JUDICIAL REVIEW.—

(1) IN GENERAL.—For any rule subject to this section, an individual who is adversely affected or aggrieved by final agency action is entitled to judicial review of agency compliance with the requirements of subsections (b) and (c) in accordance with chapter 7. Agency compliance with subsection (d) shall be judicially reviewable in connection with judicial review of subsection (b).

(2) JURISDICTION.—Each court having jurisdiction to review such rule for compliance with section 553, or under any other provision of law, shall have jurisdiction to review any claims of noncompliance with subsections (b) and (c) in accordance with chapter 7. Agency compliance with subsection (d) shall be judicially reviewable in connection with judicial review of subsection (b).

(3) LIMITATIONS.—

(A) An individual may seek such review during the period beginning on the date of final agency action and ending 1 year later, except that where a provision of law re-

quires that an action challenging a final agency action be commenced before the expiration of 1 year, such lesser period shall apply to an action for judicial review under this subsection.

(B) In the case where an agency delays the issuance of a final privacy impact assessment pursuant to subsection (c), an action for judicial review under this section shall be filed not later than—

(i) 1 year after the date the assessment is made available to the public; or

(ii) where a provision of law requires that an action challenging a final agency regulation be commenced before the expiration of the 1-year period, the number of days specified in such provision of law that is after the date the assessment is made available to the public.

(4) RELIEF.—In granting any relief in an action under this subsection, the court shall order the agency to take corrective action consistent with this section and chapter 7, including, but not limited to—

(A) remanding the rule to the agency; and

(B) deferring the enforcement of the rule against individuals, unless the court finds that continued enforcement of the rule is in the public interest.

(5) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit the authority of any court to stay the effective date of any rule or provision thereof under any other provision of law or to grant any other relief in addition to the requirements of this subsection.

(6) RECORD OF AGENCY ACTION.—In an action for the judicial review of a rule, the privacy impact assessment for such rule, including an assessment prepared or corrected pursuant to paragraph (4), shall constitute part of the entire record of agency action in connection with such review.

(7) EXCLUSIVITY.—Compliance or noncompliance by an agency with the provisions of this section shall be subject to judicial review only in accordance with this subsection.

(8) SAVINGS CLAUSE.—Nothing in this subsection bars judicial review of any other impact statement or similar assessment required by any other law if judicial review of such statement or assessment is otherwise permitted by law.

(g) DEFINITION.—For purposes of this section, the term "personally identifiable information" means information that can be used to identify an individual, including such individual's name, address, telephone number, photograph, social security number or other identifying information. It includes information about such individual's medical or financial condition.

* * * * * * *

CHAPTER 8—CONGRESSIONAL REVIEW OF AGENCY RULEMAKING

* * * * * * *

§ 801. Congressional review

(a)(1)(A) * * *

(B) On the date of the submission of the report under subparagraph (A), the Federal agency promulgating the rule shall submit to the Comptroller General and make available to each House of Congress—

(i) * * *

* * * * * * *

(iii) the agency's actions relevant to section 553a;

[(iii)**]** *(iv)* the agency's actions relevant to sections 202, 203, 204, and 205 of the Unfunded Mandates Reform Act of 1995; and

[(iv)**]** *(v)* any other relevant information or requirements under any other Act and any relevant Executive orders.

* * * * * * *

MARKUP TRANSCRIPT

BUSINESS MEETING

WEDNESDAY, JUNE 7, 2006

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 1:10 p.m., in Room 2141, Rayburn House Office Building, the Honorable F. James Sensenbrenner, Jr. (Chairman of the Committee) presiding.

[Intervening business.]

Chairman SENSENBRENNER. The next item on the agenda is the adoption of H.R. 2840, the Federal Agency Protection of Privacy Act of 2005. The Chair recognizes the gentleman from Utah, Mr. Cannon, the chair of the Subcommittee on Commercial and Administrative Law for a motion.

Mr. CANNON. Thank you, Mr. Chairman. The Subcommittee on Commercial and Administrative Law reports favorably the bill H.R. 2840 and moves its favorable recommendation to the full House.

[The bill, H.R. 2840, follows:]

I

109TH CONGRESS
1ST SESSION

H. R. 2840

To amend title 5, United States Code, to require that agencies, in promulgating rules, take into consideration the impact of such rules on the privacy of individuals, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 9, 2005

Mr. CHABOT (for himself, Mr. NADLER, Mr. CANNON, and Mr. DELAHUNT) introduced the following bill; which was referred to the Committee on the Judiciary

---

A BILL

To amend title 5, United States Code, to require that agencies, in promulgating rules, take into consideration the impact of such rules on the privacy of individuals, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Federal Agency Protection of Privacy Act of 2005".

SEC. 2. REQUIREMENT THAT AGENCY RULEMAKING TAKE INTO CONSIDERATION IMPACTS ON INDIVIDUAL PRIVACY.

(a) IN GENERAL.—Title 5, United States Code, is amended by adding after section 553 the following new section:

"§ 553a. Privacy impact assessment in rulemaking

"(a) INITIAL PRIVACY IMPACT ASSESSMENT.—

"(1) IN GENERAL.—Whenever an agency is required by section 553 of this title, or any other law, to publish a general notice of proposed rulemaking for a proposed rule, or publishes a notice of proposed rulemaking for an interpretative rule involving the internal revenue laws of the United States, and such rule or proposed rulemaking pertains to the collection, maintenance, use, or disclosure of personally identifiable information from 10 or more individuals, other than agencies, instrumentalities, or employees of the Federal Government, the agency shall prepare and make available for public comment an initial privacy impact assessment that describes the impact of the proposed rule on the privacy of individuals. Such assessment or a summary thereof shall be signed by the senior agency official with primary responsibility for privacy policy and be published in the Federal Register at the time of the

publication of a general notice of proposed rulemaking for the rule.

"(2) CONTENTS.—Each initial privacy impact assessment required under this subsection shall contain the following:

"(A) A description and analysis of the extent to which the proposed rule will impact the privacy interests of individuals, including the extent to which the proposed rule—

"(i) provides notice of the collection of personally identifiable information, and specifies what personally identifiable information is to be collected and how it is to be collected, maintained, used, and disclosed;

"(ii) allows access to such information by the person to whom the personally identifiable information pertains and provides an opportunity to correct inaccuracies;

"(iii) prevents such information, which is collected for one purpose, from being used for another purpose; and

"(iv) provides security for such information.

"(B) A description of any significant alternatives to the proposed rule which accomplish the stated objectives of applicable statutes and which minimize any significant privacy impact of the proposed rule on individuals.

"(b) FINAL PRIVACY IMPACT ASSESSMENT.—

"(1) IN GENERAL.—Whenever an agency promulgates a final rule under section 553 of this title, after being required by that section or any other law to publish a general notice of proposed rulemaking, or promulgates a final interpretative rule involving the internal revenue laws of the United States, and such rule or proposed rulemaking pertains to the collection, maintenance, use, or disclosure of personally identifiable information from 10 or more individuals, other than agencies, instrumentalities, or employees of the Federal Government, the agency shall prepare a final privacy impact assessment, signed by the senior agency official with primary responsibility for privacy policy.

"(2) CONTENTS.—Each final privacy impact assessment required under this subsection shall contain the following:

"(A) A description and analysis of the extent to which the final rule will impact the pri-

vacy interests of individuals, including the extent to which such rule—

"(i) provides notice of the collection of personally identifiable information, and specifies what personally identifiable information is to be collected and how it is to be collected, maintained, used, and disclosed;

"(ii) allows access to such information by the person to whom the personally identifiable information pertains and provides an opportunity to correct inaccuracies;

"(iii) prevents such information, which is collected for one purpose, from being used for another purpose; and

"(iv) provides security for such information.

"(B) A summary of any significant issues raised by the public comments in response to the initial privacy impact assessment, a summary of the analysis of the agency of such issues, and a statement of any changes made in such rule as a result of such issues.

"(C) A description of the steps the agency has taken to minimize the significant privacy

impact on individuals consistent with the stated objectives of applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the privacy interests of individuals was rejected.

"(3) AVAILABILITY TO PUBLIC.—The agency shall make copies of the final privacy impact assessment available to members of the public and shall publish in the Federal Register such assessment or a summary thereof.

"(c) WAIVERS.—

"(1) EMERGENCIES.—An agency head may waive or delay the completion of some or all of the requirements of subsections (a) and (b) to the same extent as the agency head may, under section 608, waive or delay the completion of some or all of the requirements of sections 603 and 604, respectively.

"(2) NATIONAL SECURITY.—An agency head may, for national security reasons, or to protect from disclosure classified information, confidential commercial information, or information the disclosure of which may adversely affect a law enforce-

ment effort, waive or delay the completion of some or all of the following requirements:

"(A) The requirement of subsection (a)(1) to make an assessment available for public comment.

"(B) The requirement of subsection (a)(1) to have an assessment or summary thereof published in the Federal Register.

"(C) The requirements of subsection (b)(3).

"(d) PROCEDURES FOR GATHERING COMMENTS.—When any rule is promulgated which may have a significant privacy impact on individuals, or a privacy impact on a substantial number of individuals, the head of the agency promulgating the rule or the official of the agency with statutory responsibility for the promulgation of the rule shall assure that individuals have been given an opportunity to participate in the rulemaking for the rule through techniques such as—

"(1) the inclusion in an advance notice of proposed rulemaking, if issued, of a statement that the proposed rule may have a significant privacy impact on individuals, or a privacy impact on a substantial number of individuals;

"(2) the publication of a general notice of proposed rulemaking in publications of national circulation likely to be obtained by individuals;

"(3) the direct notification of interested individuals;

"(4) the conduct of open conferences or public hearings concerning the rule for individuals, including soliciting and receiving comments over computer networks; and

"(5) the adoption or modification of agency procedural rules to reduce the cost or complexity of participation in the rulemaking by individuals.

"(e) PERIODIC REVIEW OF RULES.—

"(1) IN GENERAL.—Each agency shall carry out a periodic review of the rules promulgated by the agency that have a significant privacy impact on individuals, or a privacy impact on a substantial number of individuals. Under such periodic review, the agency shall determine, for each such rule, whether the rule can be amended or rescinded in a manner that minimizes any such impact while remaining in accordance with applicable statutes. For each such determination, the agency shall consider the following factors:

"(A) The continued need for the rule.

"(B) The nature of complaints or comments received from the public concerning the rule.

"(C) The complexity of the rule.

"(D) The extent to which the rule overlaps, duplicates, or conflicts with other Federal rules, and, to the extent feasible, with State and local governmental rules.

"(E) The length of time since the rule was last reviewed under this subsection.

"(F) The degree to which technology, economic conditions, or other factors have changed in the area affected by the rule since the rule was last reviewed under this subsection.

"(2) PLAN REQUIRED.—Each agency shall carry out the periodic review required by paragraph (1) in accordance with a plan published by such agency in the Federal Register. Each such plan shall provide for the review under this subsection of each rule promulgated by the agency not later than 10 years after the date on which such rule was published as the final rule and, thereafter, not later than 10 years after the date on which such rule was last reviewed under this subsection. The agency may

amend such plan at any time by publishing the revision in the Federal Register.

"(3) ANNUAL PUBLICATION.—Each year, each agency shall publish in the Federal Register a list of the rules to be reviewed by such agency under this subsection during the following year. The list shall include a brief description of each such rule and the need for and legal basis of such rule and shall invite public comment upon the determination to be made under this subsection with respect to such rule.

"(f) JUDICIAL REVIEW.—

"(1) IN GENERAL.—For any rule subject to this section, an individual who is adversely affected or aggrieved by final agency action is entitled to judicial review of agency compliance with the requirements of subsections (b) and (c) in accordance with chapter 7. Agency compliance with subsection (d) shall be judicially reviewable in connection with judicial review of subsection (b).

"(2) JURISDICTION.—Each court having jurisdiction to review such rule for compliance with section 553, or under any other provision of law, shall have jurisdiction to review any claims of noncompliance with subsections (b) and (c) in accordance with chapter 7. Agency compliance with subsection (d)

shall be judicially reviewable in connection with judicial review of subsection (b).

"(3) LIMITATIONS.—

"(A) An individual may seek such review during the period beginning on the date of final agency action and ending 1 year later, except that where a provision of law requires that an action challenging a final agency action be commenced before the expiration of 1 year, such lesser period shall apply to an action for judicial review under this subsection.

"(B) In the case where an agency delays the issuance of a final privacy impact assessment pursuant to subsection (c), an action for judicial review under this section shall be filed not later than—

"(i) 1 year after the date the assessment is made available to the public; or

"(ii) where a provision of law requires that an action challenging a final agency regulation be commenced before the expiration of the 1-year period, the number of days specified in such provision of law that is after the date the assessment is made available to the public.

"(4) RELIEF.—In granting any relief in an action under this subsection, the court shall order the agency to take corrective action consistent with this section and chapter 7, including, but not limited to—

"(A) remanding the rule to the agency; and

"(B) deferring the enforcement of the rule against individuals, unless the court finds that continued enforcement of the rule is in the public interest.

"(5) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit the authority of any court to stay the effective date of any rule or provision thereof under any other provision of law or to grant any other relief in addition to the requirements of this subsection.

"(6) RECORD OF AGENCY ACTION.—In an action for the judicial review of a rule, the privacy impact assessment for such rule, including an assessment prepared or corrected pursuant to paragraph (4), shall constitute part of the entire record of agency action in connection with such review.

"(7) EXCLUSIVITY.—Compliance or noncompliance by an agency with the provisions of this section

shall be subject to judicial review only in accordance with this subsection.

"(8) SAVINGS CLAUSE.—Nothing in this subsection bars judicial review of any other impact statement or similar assessment required by any other law if judicial review of such statement or assessment is otherwise permitted by law.

"(g) DEFINITION.—For purposes of this section, the term 'personally identifiable information' means information that can be used to identify an individual, including such individual's name, address, telephone number, photograph, social security number or other identifying information. It includes information about such individual's medical or financial condition.".

(b) PERIODIC REVIEW TRANSITION PROVISIONS.—

(1) INITIAL PLAN.—For each agency, the plan required by subsection (e) of section 553a of title 5, United States Code (as added by subsection (a)), shall be published not later than 180 days after the date of the enactment of this Act.

(2) In the case of a rule promulgated by an agency before the date of the enactment of this Act, such plan shall provide for the periodic review of such rule before the expiration of the 10-year period beginning on the date of the enactment of this Act.

For any such rule, the head of the agency may provide for a 1-year extension of such period if the head of the agency, before the expiration of the period, certifies in a statement published in the Federal Register that reviewing such rule before the expiration of the period is not feasible. The head of the agency may provide for additional 1-year extensions of the period pursuant to the preceding sentence, but in no event may the period exceed 15 years.

(c) CONGRESSIONAL REVIEW.—Section 801(a)(1)(B) of title 5, United States Code, is amended—

(1) by redesignating clauses (iii) and (iv) as clauses (iv) and (v), respectively; and

(2) by inserting after clause (ii) the following new clause:

"(iii) the agency's actions relevant to section 553a;".

(d) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 5 of title 5, United States Code, is amended by adding after the item relating to section 553 the following new item:

"553a. Privacy impact assessment in rulemaking.".

○

Chairman SENSENBRENNER. Without objection, H.R. 2840 will be considered as read and open for amendment at any point. The Chair recognizes the gentleman from Utah, Mr. Cannon, to strike the last word.

Mr. CANNON. Thank you, Mr. Chairman.

Today's markup of H.R. 2840, the "Federal Agency Protection of Privacy Act," cannot be more timely. Just last month, personal information—including Social Security numbers and birth dates belonging to more than 26 million military veterans—was stolen from the residence of a Department of Veterans Affairs employee. This deplorable loss of personal information held by the Federal Government is exactly the type of problem this legislation is intended to address.

I commend my colleague from the State of Ohio, Mr. Chabot, for his leadership on this much-needed bipartisan measure. I also commend the Chairman for scheduling this bill for markup today on such a timely basis.

As you probably know, the Subcommittee on Commercial and Administrative Law reported H.R. 2840 last month by voice vote, without amendment. I accordingly urge my colleagues to do the same. And to the extent that I have time remaining, however fast the clock may be moving, I would yield to my colleague from Ohio, the bill's distinguished author, Mr. Chabot, and ask my detailed written statement be included in the record.

[The statement of Mr. Cannon follows:]

PREPARED STATEMENT OF THE HONORABLE CHRIS CANNON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF UTAH, AND CHAIRMAN, SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

Today's markup of H.R. 2840, the "Federal Agency Protection of Privacy Act," could not be more timely. Just last month, personal information—including Social Security numbers and birth dates—belonging to more than 26 million military veterans was stolen from the residence of a Department of Veterans Affairs employee. This deplorable loss of personal information held by the Federal government is exactly the type of problem this legislation is intended to address.

This incident highlights the fact that the government's collection, use, dissemination, and protection of personally identifiable information presents far-reaching regulatory issues. Especially in these days, there is an increasingly critical need to balance law enforcement initiatives designed to preemptively detect and deter terrorist attacks and other crimes with the need to protect the privacy of innocent Americans from potentially unwarranted governmental intrusion.

H.R. 2840, I believe, strikes that important balance. It imposes a modest, though meaningful, requirement that a federal agency prepare a privacy impact analysis for proposed and final rules noticed for public comment. H.R. 2840 is intended to ensure that individual privacy rights are safeguarded by requiring federal agencies to consider the privacy implications presented by the collection, use, and dissemination of personally identifiable information.

On the other hand, H.R. 2840 will not overly burden the work of these agencies. In fact, its analysis requirement is similar to other analyses that agencies currently conduct, such as those required by the Regulatory Flexibility Act and the E-Government Act of 2002. And, the Congressional Budget Office has concluded—with respect to H.R. 2840's predecessor in the 108th Congress—that implementation of this measure will "have *no significant effect on Federal spending*." I am proud to be an original cosponsor of this bill along with my Subcommittee colleagues from New York (Mr. Nadler) and Massachusetts (Mr. Delahunt).

At least with respect to the regulatory aspects of privacy in the hands of the government, H.R. 2840 offers a simple, noncontroversial solution that requires federal agencies to consider the privacy ramifications of proposed and final rules as they are formulated.

I commend my colleague from the State of Ohio for his leadership on this very much needed bipartisan measure. I also commend the Chairman for scheduling this bill for markup today on such a timely basis. As you probably know, the Sub-

committee on Commercial and Administrative Law reported H.R. 2840 last month by voice vote without amendment. I accordingly urge my colleagues to do the same.

Mr. CHABOT. I thank the gentleman for yielding and I want to take this opportunity to thank Mr. Nadler, as well as Mr. Cannon and Mr. Delahunt, who are cosponsors of this important legislation. They have supported it both in our Subcommittee and in hearings and previous markup.

This legislation is an appropriate remedy to address citizens' privacy concerns over the use of their personal information by the Federal Government. The Federal Agency Privacy Protection Act would require that all Federal agencies conduct privacy impact assessments when issuing a notice regarding a new or interpretative rule relating to the collection of personally identifiable information on citizens, as well as when final rules are promulgated.

It would also require agencies to perform a periodic review every 10 years of rules having a significant impact on individuals' privacy.

Furthermore, if a person is adversely affected or aggrieved by a final agency action, they may seek judicial review of the agency's compliance with the requirements.

At the very least, Federal agencies must be held accountable for the personal information they collect, maintain, protect and share. The bill passed the House in the 107th Congress, and the Judiciary Committee reported the bill favorably in the 108th Congress and it was included in the House-passed version of the legislation to create the Office of the National Intelligence Director.

But it never was accepted by the Senate.

Yet, as we have learned in the 109th Congress, there is still a need for this type of legislation. In April, the Subcommittee on the Constitution, which I chair, and the

Subcommittee on Commercial and Administrative Law held a hearing to discuss a GAO report that identified several areas that need improvement among agencies about information acquired and maintained by the Federal Government.

In May, we learned in our hearing about agency privacy officers and the importance of creating a culture among agencies to protect the privacy of citizens.

The markup is even more timely in light of news that a government laptop containing personal information, including Social Security numbers of over 26 million veterans, was stolen from the home of a Veterans Affairs employee. Just today, there are reports that additional information of enlisted soldiers may also have been compromised.

This legislation is yet another measure to keep Big Brother at bay, and I would encourage Members of the Committee to support this passage. And I would again thank Mr. Nadler and Mr. Delahunt and Mr. Cannon for their leadership on this issue.

I yield back.

Chairman SENSENBRENNER. In the absence of the gentleman from North Carolina on the Democratic side, the gentleman from New York, Mr. Nadler.

For what purpose do you seek recognition?

Mr. NADLER. To strike the last word.

Chairman SENSENBRENNER. The gentleman is recognized for 5 minutes.

Mr. NADLER. Thank you, Mr. Chairman.

I want to join my colleagues, the gentleman from Ohio and the gentleman from Utah, in urging the Members of this Committee to support this bipartisan legislation.

This bill would require simply that Federal agencies conduct a privacy impact analysis as part of their rulemaking. This is not a radical proposal. Section 208 of the E-Government Act, which we passed in 2003, requires a privacy impact assessment for any information technology, "that collects, maintains or disseminates information that is an identifiable form."

This bill mirrors the language in the E-Government Act. There have been too many examples of the misuse of personally identifiable information. The recent case involving records of millions of veterans is just the latest example.

With each passing day the news brings greater and greater challenges to individual privacy at the hands of the government. While many of those important concerns may not be addressed by this bill, it is nonetheless an important step toward making our government consider the privacy implications of its actions, something that has been woefully lacking, especially in recent years.

Just recently the Subcommittee on Commercial and Administrative Law of this Committee held a hearing on privacy in the hands of government. At that hearing, the GAO testified that, "privacy officers need to be vigilant to ensure that agency officials are continually mindful of their privacy responsibilities."

Fortunately, tools are available, including the requirement for PIAs and Privacy Act public notices that can help ensure that the right operational decisions are made about the acquisition, use and storage of personal information. By using these tools effectively, agencies have the opportunity to gain greater public confidence that their actions are in the best interest of all Americans.

This bill would do just that, and at a critical time. It will take vigorous oversight by the Congress and the courts to deal with the abuses of power and willful lawlessness we have seen exhibited by the current Administration. But requiring agencies to consider and to receive public comment on the protection of privacy can help to prevent problems, if only by requiring agencies to think through the implications of their policies and their actions.

As the Committee that has created the only statutory privacy officer in the Federal Government at the Department of Homeland Security, we know that the protection of privacy is not in conflict with the mission of even our government's most sensitive agencies. Perhaps one day the Administration will understand that, too.

The constitutional right to privacy should not be a partisan issue. The right to be let alone is a cherished American value. A formal and legally mandated review procedure will greatly improve the workings of our government and protect the privacy rights of all Americans.

Thank you, Mr. Chairman. I yield back the balance of my time.

Chairman SENSENBRENNER. Without objection, all Members may put opening statements in the record at this point.

Are there amendments?

Mr. DELAHUNT. Mr. Chairman.

Chairman SENSENBRENNER. For what purpose does the gentleman from Massachusetts seek recognition?

Mr. DELAHUNT. I will be brief.

I want to commend my colleagues on both sides. I think this is a good piece of legislation, and I think it is an important step. But I want to express my own concern with the language that provides for an exception for national security reasons.

Clearly, taken on its face, that should not cause any of us any concern. However, given the interpretation of national security that seems to be in current vogue with this Administration, I do have serious concerns about the efficacy of what we are intending to do, and I think this goes to the whole issue of the abuse and misuse of the classification process.

I haven't prepared an amendment, I don't intend to offer one at this point in time, but I plan——

Mr. SCHIFF. Will the gentleman yield?

Mr. DELAHUNT. I yield to Mr. Schiff.

Mr. SCHIFF. I appreciate the gentleman's comments, and it is a concern that I share and I actually do have an amendment to propose, that I would love to have you support for, that would require simply that in those cases where the agency decides that national security requires a waiver, that there be disclosure in classified form to the Judiciary Committee of the House and Senate, so we can make sure the exception doesn't become the rule and that there is a substantial justification for that decision.

I yield back to the gentleman.

Mr. DELAHUNT. Reclaiming my time, obviously I haven't had an opportunity to review the amendment and I have not——

Mr. CHABOT. Would the gentleman yield?

Mr. DELAHUNT. I yield.

Mr. CHABOT. We are in a position to accept this helpful amendment.

Mr. DELAHUNT. If that is the case, then should I yield back, Mr. Chairman?

Chairman SENSENBRENNER. You can do whatever you want to.

Mr. DELAHUNT. Thank you for the permission.

I think then I will yield to Mr. Schiff.

Mr. CANNON. Mr. Chairman, point of order.

Chairman SENSENBRENNER. There is no amendment pending.

The gentleman from Massachusetts controls the time. I believe he has yielded to the gentleman from California.

Mr. SCHIFF. Mr. Chairman, I have an amendment at the desk.

Mr. DELAHUNT. Reclaiming my time, I yield back.

Chairman SENSENBRENNER. Are there amendments?

The gentleman from California, Mr. Schiff.

Mr. SCHIFF. Mr. Chairman, I have an amendment at the desk.

[The amendment follows:]

AMENDMENT TO H.R. 2840

OFFERED BY MR. SCHIFF OF CALIFORNIA

Page 7, line 5, after "comment" insert the following: ", provided that such assessment is made available, in classified form, to the Committees on the Judiciary of the House of Representatives and the Senate, in lieu of making such assessment available to the public".

Page 7, line 8, after "Register" insert the following: ", provided that such assessment or summary is made available, in classified form, to the Committees on the Judiciary of the House of Representatives and the Senate, in lieu of publishing such assessment or summary in the Federal Register".

Page 7, line 10, after "(b)(3)" insert the following: ", provided that the final privacy impact assessment is made available, in classified form, to the Committees on the Judiciary of the House of Representatives and the Senate, in lieu of making such assessment available to the public and publishing such assessment in the Federal Register".

Chairman SENSENBRENNER. The clerk will report the amendment.

The CLERK. Amendment to H.R. 2840, offered by Mr. Schiff of California. Page 7, line 5, after comment——

Mr. CANNON. Reserving the point of order, Mr. Chairman.

Chairman SENSENBRENNER. The point of order is reserved. The clerk will continue to read.

The CLERK. Comma—provided that such assessment is made available in classified form to the Committee on the Judiciary of the House of Representatives and the Senate in lieu of making——

Chairman SENSENBRENNER. Without objection, the amendment is considered as read.

The gentleman from California will be recognized for 5 minutes.

Mr. SCHIFF. I thank the Chairman.

Did I understand the gentleman is willing to accept the amendment?

Chairman SENSENBRENNER. I would suggest the gentleman from California keep on talking for a bit.

Mr. SCHIFF. Well, thank you, Mr. Chairman.

I appreciate the initial indication that the gentleman may be willing to accept the amendment. It is narrowly crafted; it addresses a concern raised by my colleague from Massachusetts.

In light of the concerns that have been raised about the potential overuse of a national—claim of national security waiver, and given this Committee is the Committee that has jurisdiction over privacy issues, it seems to me that when an agency that is engaged in rulemaking decides that it cannot make disclosure, rather than keeping that report internal as the bill contemplates and not disclosing it to anyone outside the agency, it ought to be shared with this Committee and its Senate counterpart in classified form so that we can ensure that the waiver is made for good cause or, if the waiver isn't, then Congress can take subsequent action.

It doesn't give us the power to overturn that.

Mr. CANNON. Would the gentleman yield?

Mr. SCHIFF. Yes.

Mr. CANNON. We apologize on this side. I apologize, at least.

This is a new amendment. I think what you are articulating is certainly desirable. I would like to see something like this in the bill. I just don't know that we have the ability right now to deal with—it is a little complex because of reasons of germaneness and other issues.

If the gentleman would withdraw, I would be happy to work with him to come up with something that I believe would actually work. I just don't have enough information and ability to deal with it right now, to agree to its inclusion, but I am very much in concert with the gentleman in his desire.

So if you would be willing to withdraw it, I think we can probably work something out between now and the floor to meet on the idea that you have here.

Mr. SCHIFF. Reclaiming my time, I can't imagine there would be a germaneness issue, given that it requires disclosure to the Judiciary Committee. The Judiciary Committee has jurisdiction or we wouldn't have the bill, and that is all that the bill—the amendment requires.

But if the gentleman is committed to including this in a manager's amendment in some form, then I am happy to work with him on that.

Mr. CANNON. I thank the gentleman and I assure him I will do so.

Mr. DELAHUNT. Will the gentleman yield?

Mr. SCHIFF. I would be happy to yield to my colleague from Massachusetts.

Mr. DELAHUNT. I think we should note, too, that the language is more expansive than simply for national security reasons. It includes confidential commercial information, or information the disclosure of which may adversely affect a law enforcement effort, waive or delay the completion of some or all of the following requirements.

This is a very, very expansive exception, and I welcome the willingness of the Subcommittee chair and the author of the legislation, the gentleman from Ohio. I think this is an amendment that makes eminent good sense, particularly when it is considered in the context that this Administration has a history of overclassification—in fact, declassifying, allowing into the public domain information and then reclassifying that same information. So this is a question that I have grave concerns about.

I have reservations as to whether we can rely on the Administration not simply to overuse this exception and other exceptions. And I daresay the gentleman should submit in conjunction with those of us who share these concerns similar amendments in additional legislation that we may consider during the remainder of this term.

With that, I yield back to the gentleman.

Mr. SCHIFF. If I can follow up with my colleague, if you like, there may be another amendment. If you would like time to review it, I am happy to hold off until the end of consideration of the bill.

Do you need a little more time to look at it?

Mr. CANNON. I don't think that we can do it in the time frame, and staff has raised a couple of concerns that I think we are going to have to work through. I am not expressing objections; this is just a bit of a complicated issue and it is in an area we have been working on openly for a long period of time.

I agree with the Ranking Member: This is not a partisan issue and not an issue that we want to be gaming. It is just, I think we need to take a little bit of time to look at it and make sure that it fits in with where we are headed.

Mr. SCHIFF. I know I am running out of time; if I might be permitted one other follow-up question.

Chairman SENSENBRENNER. Without objection, the gentleman is given an additional minute.

Mr. SCHIFF. Thank you, Mr. Chairman.

I just want to make sure that you are committed to offering this as a part of a manager's amendment, the only limitation being working out any germaneness consideration.

If not, I really would like to offer the amendment here.

Mr. CANNON. Mr. Chairman, I move to strike the last word, requisite number of words.

Chairman SENSENBRENNER. Well, does the gentleman from Ohio insist on his point of order?

Mr. CHABOT. At this time I do, yes, Mr. Chairman.

Chairman SENSENBRENNER. The gentleman will state his point of order.

Mr. CHABOT. In the spirit of—I think we have basically an agreement on the policy here. I think the gentleman has offered a good amendment.

I think there may well be a germaneness issue relative——

Chairman SENSENBRENNER. Does the gentleman make the point of order the amendment is not germane, and if so, state why.

Mr. CHABOT. It is inconsistent with the subject matter under consideration.

Chairman SENSENBRENNER. Does the gentleman from California wish to respond?

Mr. SCHIFF. It seems to me, Mr. Chairman, if the goal of this bill, the subject matter of this bill, is to ensure the privacy of Americans in the rulemaking process, and there was a provision for a waiver, and this bill has been referred to this Committee, that the requirement of a classified report to this Committee on the very privacy issues implicated in the bill can't help but be not only germane, but at the heart of the bill.

Chairman SENSENBRENNER. The Chair is prepared to rule.

The gentleman from Ohio Mr. Chabot makes a point of order that the amendment offered by the gentleman from California Mr. Schiff to H.R. 2840 is not germane. The rule of germaneness requires that the bill be within the jurisdiction of the Committee that is considering it and relate to the subject matter of the bill.

The three paragraphs of the amendment offered by the gentleman from California seek a limitation on the assessments that are being made, or the summaries that are being made, pursuant to the provisions of the bill and requires a report to this Committee which is the Committee of jurisdiction. Because of that, the Chair feels that the amendment is germane and overrules the point of order.

The question is on agreeing to the amendment offered by the gentleman from California, Mr. Schiff. Those in favor will say aye.

Opposed, no.

Mr. CANNON. No.

Chairman SENSENBRENNER. The ayes appear to have it. The ayes have it and the amendment is agreed to.

Are there further amendments?

Mr. CONYERS. Mr. Chairman.

Chairman SENSENBRENNER. The gentleman from Michigan.

Mr. CONYERS. I have an amendment at the desk.

[The amendment follows:]

AMENDMENT TO H.R. 2840
OFFERED BY MR. Conyers

At the end of the bill, insert the following new section:

Sec. 3 Additional Protections

The requirements of section 553a of title 5, United States Code, (as amended by section 2 of this Act) relating to privacy impact assessments shall, subject to any restrictions herein, apply with respect to the collection, maintenance, use, or disclosure of personally identifiable information, including any action or authorization relating to the wiretapping or other electronic surveillance of communications by citizens of the United States, and the acquisition or compilation of call records, unless such actions are conducted pursuant to a court order or warrant.

Chairman SENSENBRENNER. The Clerk will report the amendment.

The CLERK. Amendment to H.R. 2840, offered by Mr. Conyers. At the end of the bill insert the following new section. Section 3, Additional Protections. The requirements of section 553a of title 5, United States Code, as amended by section 2 of this Act——

Chairman SENSENBRENNER. Without objection, the amendment is considered as read.

The gentleman from Michigan is recognized for 5 minutes.

Mr. CONYERS. Mr. Chairman, I appreciate the fact that the gentleman from California offered an amendment that improves this.

My amendment requires that—we don't have the measure before us. Well, we do have a broad national security waiver allowing unfettered discretion to an agency to determine when to make privacy impact assessments available to the public.

The problem is that the intrusions of NSA prove that under this broad cloak of national security that sometimes people go to no end, even if it involves mining through the most sensitive personal information. So what we are proposing here is to protect the privacy of American citizens, but to also take into consideration the current threats and assaults to our privacy rights.

I don't see how the bill could contain such a broad national security waiver, and so what we are doing here is making sure that we include this and incorporate it to cover the NSA warrantless wiretapping exceptions which have just been revealed, as well as the data mining that has also recently been disclosed.

What we are saying is that we need a little bit more privacy here, and privacy protection; and the only way we can do it is through this amendment, which would include—would be subject to any restrictions that would apply with respect to the collection, maintenance, use or disclosure of personally identifiable information, including any action or authorization relating to the wire-

tapping or other electronic surveillance of communications by citizens of the United States, and the acquisition or compilation of call records unless such actions are conducted pursuant to a court order or warrant.

For those reasons, we are clarifying just how much Federal agency protection privacy that we are accorded and would strip this wide, broad, national security waiver that is currently in the bill so that we can get the protection to cover the very incidents that we are talking about.

For that reason, I urge the consideration, favorably, of this amendment.

Mr. CANNON. Would the gentleman yield?

Mr. CONYERS. Yes.

Mr. CANNON. Just for clarification, you talked about data mining in general. Your amendment deals with call records in particular. Are you intending that this amendment go beyond the government's actions in comparing records of phone calls?

Mr. CONYERS. Yes, we have got to include them as well. That would be my intention, yes, sir.

Mr. CANNON. Thank you. I would oppose this amendment and yield back to the gentleman.

Mr. CHABOT. Mr. Chairman.

Mr. CONYERS. I return my time.

Chairman SENSENBRENNER. For what purpose does the gentleman from Ohio seek recognition?

Mr. CHABOT. Move to strike the last word.

Chairman SENSENBRENNER. The gentleman is recognized for 5 minutes.

Mr. CHABOT. Thank you, Mr. Chairman. I won't take that much time, but I would just note several things.

First of all, this has been a very bipartisan bill and I want to thank my colleagues on the other side for having participated in that process on this bill. It has passed this Committee and the House a number of times already. It has been much vetted; and this particular amendment, we believe, would undercut the national security exception that is also in the bill, and these are issues really which could have been raised, I think, at an earlier time and we would have had more time to consider this.

So I would strongly oppose this and yield back.

Mr. CONYERS. Would the gentleman yield briefly?

Mr. CHABOT. Yes. I would be happy to yield. Reclaiming my time and yield back.

Mr. CONYERS. Thank you. The reason that we were all in support of the bill before is that the two incidents that we are talking about now hadn't occurred. All I am asking for is a bipartisan amendment to go along with your bipartisan bill.

Mr. CHABOT. Reclaiming my time, I think it goes far beyond that; and again I think this is a bill that could be very beneficial, that has been bipartisan. I would like to keep it that way if at all possible. It is amendments like this which will make it no longer bipartisan and are likely not to pass.

So I yield back.

Chairman SENSENBRENNER. For what purpose does the gentleman from New York seek recognition?

Mr. NADLER. To strike the last word as——

Chairman SENSENBRENNER. The gentleman is recognized for 5 minutes.

Mr. NADLER. Thank you, Mr. Chairman.

Mr. Chairman, I have been involved with this bill for at least 5 years now, and it has been a bipartisan bill and I appreciate the way it has been handled. I think this amendment by the gentleman from Michigan simply says that if you want to do wiretapping, et cetera, you ought to do it by court order or warrant, which is always the way we have done it.

The FISA Act, in fact, says you can only do it by court order or warrant, or in certain instances by order, secret order, of the FISA court.

There is a recent claim by the Administration of the power to go beyond that. Many of us don't believe there is any such power to go beyond that, but that is not at issue in this bill. But if they are going to go beyond that, they should at least have a privacy impact statement.

I would ask the gentleman from Michigan if he would agree to an amendment of his amendment, because within the FISA Act there are provisions for 72 hours to get—to be able to wiretap for up to 72 hours and then get a court order and so forth.

So I would simply urge that we add at the end of the amendment the words, "or the provisions of the FISA Act."

Mr. CONYERS. Yes. I agree, and if the gentleman would yield, ask unanimous consent that that amendment to the amendment be accepted.

Chairman SENSENBRENNER. Without objection, the amendment is modified.

The gentleman from New York.

Mr. NADLER. Thank you.

I hope with this amendment, with the second degree amendment—all this amendment is now saying is that wiretapping, if it is done, or data mining, if it is done, should be done in accordance with law; and if it is not, if it is not done by court order or by warrant or according to the provisions of the FISA Act, then there should be a privacy impact statement. Seems to me a simple thing.

I yield.

Mr. CHABOT. I thank the gentleman for yielding.

This bill deals with regulations. It deals with government agencies which are considering promulgating regulations which ultimately would impact the privacy of American citizens. We are not talking about data mining, we are not talking about the NSA's program, which has been very controversial. We are not—in fact, there is a specific exemption for things which have to do with national security and the rest.

I think also, the fact that the gentleman is amending the Ranking Member's amendment here today on the floor—I mean, this is something that has been considered long ago, and I think to be amending this right now in this manner——

Mr. NADLER. Reclaiming my time, I appreciate the comments of the distinguished Chairman of the Subcommittee. If we hadn't had these recent developments, we wouldn't have to have this amendment and—the bill was fine, and I think comprehensive and had a very broad, arguably overbroad, national security exemption.

But I think the recent developments do show the usefulness of this amendment and with the modification of the amendment, I don't see any objection.

Let me just say this, it would be proper—it would be proper for this or a future Administration to issue proposed regulations to deal with wiretapping or whatever with its own methodology and then this bill would apply.

I yield back.

Chairman SENSENBRENNER. The question—the gentleman from California, Mr. Lungren. For what purpose do you seek recognition?

Mr. LUNGREN. Strike the requisite number of words.

Chairman SENSENBRENNER. The gentleman is recognized for 5 minutes.

Mr. LUNGREN. Mr. Chairman, I rise in opposition to this amendment. I heard the word "recent" developments. I thought maybe the gentleman was going to talk about what happened in Toronto. That seems to be pretty recent. I guess terrorists beheading or attempting to behead or planning to behead a prime minister isn't as recent as what the gentleman is referring to. But it does suggest to us in the American public that the war on terrorism is real and the suggestion that—the implicit suggestion that the Administration wants to involve itself with our privacy for whatever reason whatsoever, I just think takes what they are doing out of context.

This is hardly the place, it seems to me on this particular bill, which is focused on Federal agency privacy protection, which we are talking in about—in the general category of information that the Federal Government gets is not the place, it seems to me, to be trying through one single amendment to deal with the question brought up about the NSA, about "data mining," about the activities of listening in on conversations between an al-Qaeda member on the outside and someone here in the United States. And the suggestion made by one of my colleagues that somehow this is something newly found by the Administration contradicts the record.

When the FISA law was presented to the Congress, it was a Democratic attorney general representing a Democratic Administration; his name was Griffin Bell. He stated for the record that the support of the FISA bill, which became the law, did not in any way suggest that it could impinge on the constitutional prerogatives of the President in these areas.

Now, this sleight of hand, this verbal sleight of hand to suggest that somehow the Administration does something that is against the law leaves out the fact that the Supreme Court is the supreme—I mean, that the Constitution is the supreme law of the land. And there is at least an arguable position the Administration has advanced that the category of authority given to the President under his commander-in-chief powers allows an Administration to operate in the areas the President has operated under.

Remember when General Hayden's nomination to be head of the CIA first came up, there was an uproar that he would have a difficult time because he had been in charge of these various programs, and once the Senators learned the details involved, they would reject his nomination.

I recall that he passed rather easily after sitting down and talking with Members on the other side of this Capitol about this very issue. Perhaps, perhaps they actually learned something by those presentations and learned that, in fact, this was constitutional under the authority that the President has and, number two, it was effective and may have protected us against some of these activities by terrorists.

In fact, in my conversations with General Hayden, he said very specifically that we have gained information that we could not have gained in any other way, in his judgment—admittedly it is his judgment, although I think that is a considered judgment.

So I just think we are playing—well, the gravity——

Mr. CONYERS. Would the gentleman yield?

Mr. LUNGREN. In just a moment.

The gravity of the situation with respect to the threat that we are facing, it seems to me, is not evidence in this particular amendment being considered under these circumstances on a bill that otherwise has tremendous bipartisan support and deals with areas of privacy protection about which there is no question whatsoever and for which we can advance protections by the adoption of this bill.

I would be happy to yield to my friend from Michigan.

Mr. CONYERS. I thank—did the gentleman yield?

Mr. LUNGREN. Yes.

Mr. CONYERS. Thank you very much.

All we are looking for is an impact statement. We are not trying to raise covertly any of the problems that——

Mr. LUNGREN. A covert impact statement?

Mr. CONYERS. I said you were talking about what we were trying to do covertly. All I am trying to do is put this in the record that we have a covert statement—have an impact statement on the wiretap——

Mr. LUNGREN. I understand. You have this as a covert impact statement or have it as a public impact statement?

Mr. CONYERS. How about the statement we got that has already been an amendment. It could be classified, if it would make you feel better. But we are not trying to solve the larger problem.

I just think that this unfettered discretion of a national security waiver without mentioning the two incidents that everybody keeps referring to, that happened before we had all the agreement, is a little bit naive.

Chairman SENSENBRENNER. The time has expired.

For what purpose does the gentleman from Massachusetts seek recognition?

Mr. DELAHUNT. Move to strike the requisite number of words.

Chairman SENSENBRENNER. The gentleman is recognized for 5 minutes.

Mr. DELAHUNT. I think my colleague from California has missed the mark.

I mean, we just passed the Schiff amendment which created an option which created or conferred upon the Judiciary Committee a report as to classified, and I had read earlier all of the various components that were implicated in the exception provision.

So we are not making this public. This is doing nothing other than conferring on the Judiciary Committee the appropriate information that we need to exercise our oversight.

The gentleman referred to the Senate, where they must have learned something from General Hayden. I have serious reservations as to whether they learned anything about the constitutionality of the Executive's position, but I know that we have not learned anything in terms of this particular program.

But having said all that, this is about this Committee as an institution within the House of Representatives, and this is not about partisan politics. This is about asserting the appropriate jurisdiction of this Committee, and we should have this information available to us in a classified forum.

I just can't simply——

Mr. CANNON. Would the gentleman yield?

As I read this, the second line, "relating to privacy impact assessments shall...apply with respect to the collection," et cetera, I don't think this is consistent with the nature of the underlying bill which is dealing with rulemakings, public rulemakings.

Are you suggesting by this amendment that any activity of the government which is data mining or collecting information electronically now has to become part of a public rulemaking?

Mr. DELAHUNT. Reclaiming my time. I believe that the Conyers amendment speaks for itself. It says, "including any action or authorization relating to the wiretapping or other electronic surveillance."

Mr. CANNON. Would the gentleman yield?

Mr. DELAHUNT. I yield.

Mr. CANNON. The underlying bill is about privacy impact statements relating to rulemakings. We are not doing rulemakings right now, whatever the legitimacy of the activity may be in these covert areas.

Mr. DELAHUNT. I understand. The statement was made earlier, I believe, by my friend from California is, Why now? I guess my response was, because there hasn't been an opportunity, nor do I see an opportunity, to establish and strengthen and enhance the role of this Committee in oversight.

Why now? Why not now?

Mr. CANNON. Would the gentleman yield?

Mr. CONYERS. Would the gentleman yield?

Mr. DELAHUNT. I yield to the gentleman from Michigan.

Mr. CONYERS. I want to thank the gentleman.

Line 2, "relating to privacy impact assessments shall, subject to any restrictions therein"——

Mr. DELAHUNT. Reclaiming my time for one moment. Given the amendment by the gentleman from California, Mr. Schiff, includes—implicates those restrictions in a classified form——

Mr. CONYERS. Exactly.

Mr. DELAHUNT. —available to this Committee, only this Committee.

Mr. CANNON. Would the gentleman yield?

Mr. CONYERS. If the gentleman will yield, that is "subject to any restrictions therein," and it is dealing only with rulemaking.

Ladies and gentlemen, we are not trying to go into the partisanship that was referred to by my friend from California. We are try-

ing to include this subject matter as part of the "relating to privacy impact assessments, subject to any restrictions therein," and it can be classified.

We are not——

Mr. CANNON. Would the gentleman yield? The issue is not whether the matter is classified or not; the issue is whether this bill is built to do that sort of thing.

This is the wrong idea in the wrong bill at the wrong time.

Now, I think it is appropriate for this Committee to be pursuing these activities and I would love to do so with the gentleman, the Ranking Member, because this is important to us, but this bill is about rulemakings, and we don't make rulemakings about how we do these clandestine activities. Those are not public.

Mr. DELAHUNT. Reclaiming my time, it is clear that this activity is being done subject to some rule. What the specific rule is is unavailable to me, but clearly it is done "with respect to the collection, maintenance, use or disclosure." so there is a rule in existence somewhere, and I believe that——

Chairman SENSENBRENNER. The time of the gentleman has expired.

The question is on the Conyers amendment.

Ms. JACKSON LEE. Mr. Chairman.

Chairman SENSENBRENNER. The gentlewoman from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. I thank the distinguished Chairman.

Chairman SENSENBRENNER. The gentlewoman is recognized for 5 minutes.

Ms. JACKSON LEE. I rise to support the Conyers amendment. And I am probably going to go across the lot and beyond, but I rise to support the particular amendment because I think this is an opportunity to discuss overall the undermining of privacy of individual Americans and, as well, the seemingly burned firewall between the judiciary, the executive and the legislature.

Frankly, we have got to get a grip on the issue of privacy. The violations are enormous. I think the Conyers amendment goes to the frustration of many who have watched warrantless searches, many who are absolutely confused as to how an employee of the Veterans Department can just randomly take home millions and millions of data names to their personal home and then be violated by an alleged burglary or breaking and entry, of which those unfortunate souls have had their privacy violated.

I would also suggest that it goes to the overall insult of a lack of respect of the new technology that generates confusion between technology and privacy. To the extent that my young college student son received a letter from a university he had applied to, apologizing for the fact that his personal data had mistakenly been either lost and/or abused by a hacker—and, again, this particular amendment does not cover the gamut, but frankly, I think additional protections in this legislation are needed.

I would hope that besides the passage of Mr. Conyers' amendment that we would also have the hearings that we are, I believe, obligated to have expansively on this question of the overall violation of America's privacy.

So I would hope that this amendment would be passed so that we can begin to make a statement about unauthorized wiretapping, electronic surveillance——

Mr. CONYERS. Would the gentlelady yield?

Ms. JACKSON LEE. I would be happy to yield.

I believe this amendment speaks to the broader question, Mr. Conyers; and I hope we will be able to have a long history on this question because people are being violated.

I yield to the gentleman.

Mr. CONYERS. At this moment, we are only discussing the privacy impact assessments subject to any restrictions therein. So I want to allay—we are not having a hearing on the deeper and more complex question.

This bill should contain a less broad national security waiver that allows unfettered discretion to an agency to determine when to make privacy impact assessments available to the public.

The intrusions of the NSA prove that under the broad cloak of national security this Administration has to—if we want to be bipartisan, let's include in the Federal Agency Protection of Privacy Act the considerations not of what happened in Canada, but what happened in the U.S. in terms of the warrantless wiretap and the data mining that goes on.

We just want a privacy impact assessment of those rules, and no more, no less. And we want it included in this Protection of Privacy Act bill that has enjoyed so much bipartisanship.

Ms. JACKSON LEE. Reclaiming my time, let me say to Congressman Conyers, you are right, your amendment is narrowly drawn.

I associate myself with your words of support and articulation of its purpose and believe that it is an appropriate amendment for this bill and would not associate my broad conversation about security violations or privacy violations to your amendment.

I support your amendment and I hope we can support a narrowly drawn amendment, thoughtfully done, as the one you have offered today.

I yield back.

Mr. KING. Mr. Chairman.

Chairman SENSENBRENNER. For what purpose does the gentleman from Iowa seek recognition?

Mr. KING. Mr. Chairman, I move to strike the last word.

Chairman SENSENBRENNER. The gentleman is recognized for 5 minutes.

Mr. KING. Thank you, Mr. Chairman. I would be happy to yield to the gentleman from Ohio, Mr. Chabot.

Mr. CHABOT. I thank the gentleman for yielding, and I will be relatively brief here. I just want to get back to what this bill is about.

Again, this is about rulemaking, it is not about communications between al-Qaeda terrorists in a cell over here in the United States. It is not about data mining or anything of that nature.

I think my friends on the other side raise some issues which it is certainly appropriate to debate. They are issues that have been debated in the public sector. This is just not the bill, in my view, in which they are really relevant.

We are trying to do something here, which we have a chance to have an impact on future information-gathering at Federal agen-

cies, those agencies who may be able to get personal information from American citizens; and we have the ability to protect Americans privacy rights in this particular bill.

It has passed a number of times before. Now, these incidences arguably have come up since then, but they are, in my view and in most of the folks' views over here, irrelevant to what is at hand here.

This is rulemaking, not communications being intercepted between Pakistan or Saudi Arabia or Afghanistan and some al-Qaeda terrorist-connected person here in this country. That is a debate that ought to be had, but not relative to this bill.

I thank the gentleman for yielding.

Mr. KING. Reclaiming my time and yielding to the gentleman from Utah, Mr. Cannon.

Mr. CANNON. Thank you.

Just two points: First of all, we have had a discussion during the debate on this amendment about whether it means data mining or limited to other forms. There is no definition by which you can say this is a narrowly drafted amendment.

Secondly, we have an ongoing project in the Subcommittee on Commercial and Administrative Law which is a review of the Administrative Procedure Act. We are looking at how it is operating and how it ought to be changed. I suspect we will have some significant changes, given just the changes in society since the last time this has happened.

What is happening with the programs that this amendment deals with is unrelated to the APA. Those clandestine activities are controlled by law, and they have reporting processes; but those are not processes that are done under the APA unless we want to change the Administrative Procedure Act, in which case, I invite everyone interested in the subject to join the process.

These programs are not subject to results and therefore not relevant to the underlying bill, which deals only with privacy impact statements relating to rulemakings in other public processes.

And with that summary statement, I yield back.

Mr. KING. Reclaiming my time, I would state that I appreciate the opposition's remarks with regard to the periphery issues, that may also have a flavor of politics to it. But I associate with the remarks of Mr. Cannon and Mr. Chabot, and I would urge that position to be adopted here by this Committee and yield back the balance of my time.

Chairman SENSENBRENNER. The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Strike the last word.

Chairman SENSENBRENNER. The gentleman is recognized for 5 minutes.

Mr. SCOTT. Yield to Mr. Nadler.

Mr. NADLER. I thank the gentleman for yielding. I have two comments.

First, with respect to what Mr. Lungren said before, we all understand that we are engaged in a very serious war against the Islamic terrorists—not against terrorism, against the Islamic terrorists. We understand we are going to be involved in this war for a long time to come, and we have to protect ourselves.

Having said that, that is not a blank check for the Executive doing whatever the heck the President, or this President, the next President, may think he wants to do regardless of constitutional and legal processes.

The underlying bill says that there should be a privacy impact statement when there is a rule to do something new, in effect, or change the way something old is being done. The amendment says, or the amendment we are discussing, Mr. Conyers' amendment, that with respect to—that there should be a similar statement relating to privacy impact statements, that this should apply to any restrictions with respect to the collection, maintenance, et cetera, of personally identifiable data.

You might say that before the Executive decided suddenly to undertake a program like this, they should have done a rule. But we are not asking that.

We are saying that whether they do a rule or not, they have got to look at the privacy impacts, and pursuant to Mr. Schiff's amendment combined with Mr. Conyers' amendment, at least tell this Committee in secret so that we can assess the implications that the Executive is not alone, we have a Congress here, too; that Mr. Lungren says we have a Supreme Court that will decide the constitutionality, at least until the next bill which says they will not.

Mr. CANNON. Will the gentleman yield?

Mr. NADLER. Not for the moment.

As of now, the Supreme Court is supposed to adjudicate the constitutionality of anything the Executive or the Congress does that is challenged of which it is aware, and what this amendment does is say that before the Executive in the name of the war on terrorism, or anything else, undertakes a perhaps justified, a perhaps worthwhile—or maybe not—program that implicates personally identifiable data, is has got to inform this Committee. That is all it says.

That, I think, belongs in this bill. I agree it would be nice if we had the opportunity to consider this in greater detail in other bills. We have not. If there are further hearings or processes before Mr. Cannon's Subcommittee, that is very good.

This is a good amendment for this bill.

Mr. CANNON. Would the gentleman yield?

Mr. SCOTT. Would the gentleman yield?

Mr. CANNON. I think I heard you say, Mr. Nadler, that the purpose of this amendment is to take privacy statements, impact statements, beyond rulemakings and into every activity, clandestine or otherwise of the Administration.

Mr. NADLER. No, no, no. Whether I said it or not, that is not what I meant to say.

Mr. CANNON. That is the core point. What does this amendment do?

Mr. NADLER. It is for rulemaking.

I might add, we ought to do a rule.

Mr. CANNON. If the gentleman would continue to yield, in a case where clandestine activity is covered by other laws other than the APA, are you suggesting by this amendment we need to assert ourselves?

Mr. NADLER. No.

It does not say that. It is subject to all the restrictions of the overall bill.

Mr. CANNON. Then what does it do, if it does not do that; if it does not extend privacy impact statements?

Mr. NADLER. In any case where there is a rule, or perhaps somebody might sue if they knew about it and they say there ought to be a rule, it makes this applicable whether there is a privacy implication with respect to wiretapping and so forth. It is a strictly an amendment to the APA.

Mr. CANNON. I thank the gentleman for yielding.

Chairman SENSENBRENNER. The question is on the Conyers amendment, as modified

All those in favor, signify by saying aye.

Opposed, no.

And the noes appear to have it.

A record vote is requested. Those in favor of the Conyers amendment, as modified, will say aye.

Those opposed, no.

The clerk will call the roll. Before the Clerk starts calling the roll, a reporting quorum will be present for this rollcall. I ask the Members to stick around so we can report out the two bills that we have already finished.

The Clerk will call the roll.

The CLERK. Mr. Hyde.

[No response.]

The CLERK. Mr. Coble.

[No response.]

The CLERK. Mr. Smith.

[No response.]

The CLERK. Mr. Gallegly.

[No response.]

The CLERK. Mr. Goodlatte.

[No response.]

The CLERK. Mr. Chabot.

Mr. CHABOT. No.

The CLERK. Mr. Chabot, no.

Mr. Lungren.

Mr. LUNGREN. No.

The CLERK. Mr. Lungren, no.

The CLERK. Mr. Jenkins.

Mr. JENKINS. No.

The CLERK. Mr. Jenkins, no.

Mr. Cannon.

Mr. CANNON. No.

The CLERK. Mr. Cannon, no.

Mr. Bachus.

[No response.]

The CLERK. Mr. Inglis.

[No response.]

The CLERK. Mr. Hostettler.

[No response.]

The CLERK. Mr. Green.

Mr. GREEN. No.

The CLERK. Mr. Green, no.

Mr. Keller.

Mr. KELLER. No.
The CLERK. Mr. Keller no.
Mr. Issa.
[No response.]
The CLERK. Mr. Flake.
[No response.]
The CLERK. Mr. Pence.
[No response.]
The CLERK. Mr. Forbes.
Mr. FORBES. No.
The CLERK. Mr. Forbes, no.
Mr. King.
Mr. KING. No.
The CLERK. Mr. King, no.
Mr. Feeney.
Mr. FEENEY. No.
The CLERK. Mr. Feeney, no.
Mr. Franks.
Mr. FRANKS. No.
The CLERK. Mr. Franks, no.
Mr. Gohmert.
[No response.]
The CLERK. Mr. Conyers.
Mr. CONYERS. Aye.
The CLERK. Mr. Conyers, aye.
Mr. Berman.
[No response.]
The CLERK. Mr. Boucher.
[No response.]
The CLERK. Mr. Nadler.
Mr. NADLER. Aye.
The CLERK. Mr. Nadler, aye.
Mr. Scott.
Mr. SCOTT. Aye.
The CLERK. Mr. Scott, aye.
Mr. Watt.
[No response.]
The CLERK. Ms. Lofgren.
[No response.]
The CLERK. Ms. Jackson Lee.
Ms. JACKSON LEE. Aye.
The CLERK. Ms. Jackson Lee, aye.
Ms. Waters.
[No response.]
The CLERK. Mr. Meehan.
[No response.]
The CLERK. Mr. Delahunt.
Mr. DELAHUNT. Aye.
The CLERK. Mr. Delahunt, aye.
Mr. Wexler.
Mr. WEXLER. Aye.
The CLERK. Mr. Wexler, aye.
Mr. Weiner.
Mr. WEINER. Aye.
The CLERK. Mr. Weiner, aye.

Mr. Schiff.
Mr. SCHIFF. Aye.
The CLERK. Mr. Schiff, aye.
Ms. Sanchez.
Ms. SANCHEZ. Aye.
The CLERK. Ms. Sanchez, aye.
Mr. Van Hollen.
Mr. VAN HOLLEN. Aye.
The CLERK. Mr. Van Hollen, aye.
Ms. Wasserman Schultz.
Ms. WASSERMAN SCHULTZ. Aye.
The CLERK. Ms. Wasserman Schultz, aye.
Mr. Chairman.
Chairman SENSENBRENNER. No.
The CLERK. Mr. Chairman, no.
Chairman SENSENBRENNER. Are there any Members in the chamber who wish to change their vote? The gentleman from Massachusetts, Mr. Meehan.
Mr. MEEHAN. Aye.
The CLERK. Mr. Meehan, aye.
Chairman SENSENBRENNER. The gentleman from North Carolina, Mr. Coble.
Mr. COBLE. No.
The CLERK. Mr. Coble, no.
Chairman SENSENBRENNER. The gentleman from Indiana, Mr. Hostettler.
Mr. HOSTETTLER. No.
The CLERK. Mr. Hostettler, no.
Chairman SENSENBRENNER. Further Members who wish to cast or change their votes? The gentleman from Virginia, Mr. Goodlatte.
Mr. GOODLATTE. No.
The CLERK. Mr. Goodlatte, no.
Chairman SENSENBRENNER. The Clerk will report.
The CLERK. Mr. Chairman, there were 12 ayes and 14 nays.
Chairman SENSENBRENNER. And the amendment is not agreed to.
[Intervening business.]
Chairman SENSENBRENNER. We will now return to consideration of the bill H.R. 2840. When the Committee moved to deal with the unfinished business, the question before the Committee was on the motion to report the bill favorably to the House, as amended.
Are there any further amendments? The gentleman from Florida, Mr. Wexler.
Mr. WEXLER. Mr. Chairman, I have an amendment at the desk.
[The amendment follows:]

AMENDMENT TO H.R. 2840

OFFERED BY MR. WEXLER

At the end of the bill, add the following new section:

1 **SEC. 3. NOTIFICATION OF BREACH OF PRIVACY.**

2 (a) NOTIFICATION.—Whenever an agency of the
3 United States is responsible for the collection, mainte-
4 nance, use, or disclosure of personally identifiable informa-
5 tion from 10 or more individuals, other than agencies, in-
6 strumentalities, or employees of the Federal Government,
7 and the privacy of any individual is compromised by the
8 unauthorized release of such personally identifiable infor-
9 mation as a result of a breach of security at or by such
10 agency, the agency shall notify each such individual whose
11 privacy was compromised, in writing, of such compromise
12 as soon as practicable, but not later than 14 days after
13 the date of the compromise, or 14 days after the date of
14 the enactment of this Act, whichever is later.

15 (b) CERTIFICATION.—The head of an agency of the
16 United States subject to subsection (a) shall certify, in
17 writing, to the Committees on the Judiciary of the House
18 of Representatives and the Senate that the agency has
19 complied with the notification requirements of such sub-
20 section.

1 (c) APPLICABILITY.—The notification requirement
2 under subsection (a) and the certification requirement
3 under subsection (b) shall apply with respect to any com-
4 promise of personally identifiable information that—
5 (1) occurs on or after the date of the enactment
6 of this Act; or
7 (2) occurred during the one year period before
8 the date of the enactment of this Act, including the
9 compromise of personally identifiable information re-
10 sulting from the theft of data from an employee of
11 the Department of Veterans Affairs on or around
12 May 3, 2006.
13 (d) DEFINITION.—For purposes of this section, the
14 term "personally identifiable information" means informa-
15 tion that can be used to identify an individual, including
16 such individual's name, address, telephone number, photo-
17 graph, social security number, or other identifying infor-
18 mation, and includes such individual's medical or financial
19 condition.

Chairman SENSENBRENNER. The Clerk will report the amendment.

Mr. CANNON. Mr. Chairman, I reserve a point of order.

Chairman SENSENBRENNER. A point of order is reserved. The Clerk will report the amendment.

The CLERK. Amendment to H.R. 2840 offered by Mr. Wexler. At the end of the bill, add the following new section: Section 3——

Chairman SENSENBRENNER. Without objection, the amendment is considered as read. And the gentleman from Florida, Mr. Wexler, will be recognized for 5 minutes.

Mr. WEXLER. Thank you, Mr. Chairman. This amendment is similar to two amendments that the Chairman graciously accepted last week from Mr. Scott and myself in the context of reviewing what happened with the Veterans Administration and the breach of security for 26-plus-million American veterans that found their personal information stolen and then possibly disseminated.

The amendments that the Chairman graciously accepted last week provided that in the future a Federal agency would have to notify law enforcement officials under a due period of time. What this amendment simply says is under those same circumstances where Americans have had their privacy violated by a Federal agency, that within 14 days after the compromise of the breach of security, that those Americans be notified of the breach. It is as simple as that.

I agree that this is a very good bill; and I would hope that with the adoption, hopefully voluntarily of this amendment, we could extend protection of Americans' privacy rights in an addition to this bill in a very comprehensive way.

Chairman SENSENBRENNER. Does the gentleman yield back?

Mr. WEXLER. Yes.

Chairman SENSENBRENNER. Does the gentleman from Utah insist upon his point of order?

Mr. CANNON. Yes, Mr. Chairman, I do.

Chairman SENSENBRENNER. The gentleman will state his point of order.

Mr. CANNON. Thank you. This amendment establishes a governmentwide obligation for Federal agencies to notify individuals if personally identifiable information is compromised. This legislation pertains to the preparation and publication of privacy impact analyses by Federal agencies. As such, the amendment is nongermane because it contains provisions outside the scope and subject matter of the legislation under consideration.

Chairman SENSENBRENNER. Does the gentleman from Florida wish to be heard in opposition to the point of order?

Mr. WEXLER. I do, Mr. Chairman.

Chairman SENSENBRENNER. The gentleman is recognized.

Mr. WEXLER. Quickly, with Mr. Cannon, is it the scope of the amendment that Mr. Cannon finds objection with? Or is it the substance?

Mr. CANNON. It is the scope and subject matter, because we are going beyond the jurisdiction of this Committee.

Chairman SENSENBRENNER. The gentleman from Florida is recognized on the point of order. The Chair heard the gentleman from Utah state what the point of order is and the Chair, under the

rules, is required to rule on the point of order as stated by the gentleman from Florida.

Mr. WEXLER. I would defer to the Chairman to use his discretion. He has been very fair thus far.

Chairman SENSENBRENNER. Okay. In the opinion of the Chair, the amendment offered by the gentleman from Florida, Mr. Wexler, goes far beyond the scope of the legislation which has been introduced. The title of the bill, as introduced, amends Title 5 United States Code to require that agencies in promulgating rules take into consideration the impact of such rules on the privacy of individuals. In other words, this is a factor that the agencies have to take into consideration should this bill be enacted into law.

On the other hand, the amendment offered by the gentleman from Florida, Mr. Wexler, requires the agency to go beyond taking into consideration the factors contained in the title of the bill in making notifications to people whose privacy was potentially violated by the agency and, as such, it goes far beyond the scope of the bill as introduced.

For this reason, the Chair sustains the point of order of the gentleman from Utah that the amendment is not germane.

Are there further amendments?

Mr. WEXLER. Mr. Chairman.

Chairman SENSENBRENNER. The gentleman from Florida, Mr. Wexler.

Mr. WEXLER. In light of the Chairman's ruling, which I respect, I have another amendment at the desk which I think reflects the Chairman's sentiments.

Chairman SENSENBRENNER. The Clerk will report the amendment.

The CLERK. Amendment to H.R. 2840 offered by Mr. Wexler.

Mr. CANNON. Mr. Chairman, not having seen this yet, I would like to reserve a point of order.

Chairman SENSENBRENNER. A point of order is reserved. The Clerk will report the amendment.

The CLERK. Page 3, line 24, after "information" insert the following: including the provision of written notice to any individual within 14 days of the date of compromise, whose privacy——

Chairman SENSENBRENNER. Without objection, the amendment is considered as read and subject to the reserved point of order. The gentleman from Florida is recognized for 5 minutes.

[The amendment follows:]

AMENDMENT TO H.R. 2840

OFFERED BY MR. WEXLER

Page 3, line 24, after "information" insert the following: ", including the provision of written notice to any individual, within 14 days of the date of compromise, whose privacy interests are compromised by the unauthorized release of personally identifiable information as a result of a breach of security at or by the agency".

Page 5, line 17, after "information" insert the following: ", including the provision of written notice to any individual, within 14 days of the date of compromise, whose privacy interests are compromised by the unauthorized release of personally identifiable information as a result of a breach of security at or by the agency".

Mr. WEXLER. Thank you, Mr. Chairman. Respecting the objection that Mr. Cannon raised and that the Chairman acknowledged, this amendment substantively does the same thing, but is limited, exactly as Mr. Cannon said, to the terms of this bill to the rulemaking administrative process of the Federal agency. They then would be affected by the requirement to notify Americans if their privacy was breached in the context of what this bill is specifically about.

Chairman SENSENBRENNER. Does the gentleman yield back?

Mr. WEXLER. Yes.

Chairman SENSENBRENNER. Does the gentleman from Utah insist upon his point of order?

Mr. CANNON. Yes, Mr. Chairman, I do.

Chairman SENSENBRENNER. The gentleman will state his point of order.

Mr. CANNON. I believe this is—I don't see any difference between this amendment which puts the same obligation on agencies outside the scope of the title we are amending here with this bill. And, therefore, would just repeat the point of order as I made it against the privacy amendment.

Mr. Chairman, do I need to restate that point of order.

Chairman SENSENBRENNER. The gentleman can do whatever he wants to.

Mr. CANNON. Thank you. I will just repeat, then. This amendment establishes a governmentwide obligation of Federal agencies to notify individuals if personally identifiable information is compromised. This legislation pertains to the preparation and publication of privacy impact analyses by Federal agencies. As such, the amendment is nongermane because it contains provisions outside the scope and subject matter of the law under consideration before us today.

Chairman SENSENBRENNER. The gentleman from Florida, Mr. Wexler.

Mr. WEXLER. Thank you, Mr. Chairman. This objection I don't really understand, quite frankly. I understood the first one, but this one does not seem to make sense, unless there was a disagreement on the substance, which I can't imagine that anybody would disagree with. All this amendment does is say that in the context of the privacy impact assessment study, which is what this bill is requiring, that the issue of privacy will have to be respected by the Federal Government within the time period.

This does not require, for instance, that 26 million notices be sent out as to what would have been the case under the breach of the Veterans Administration, which is what I think should be done. And that is what my previous amendment would have done had it been in effect when the Veterans Administration had the problem that it does. But what this amendment simply relates to is the four corners of this bill and the requirements of this bill.

Mr. CANNON. Would the gentleman yield to help me understand a little bit better?

Mr. WEXLER. Yes, I will be happy to yield.

Chairman SENSENBRENNER. When there is a discussion on a point of order, I don't think that there can be yielding from one Member to the other. People give their position on the point of order. The Chair is limited to ruling on the point of order and not

on extraneous material that more properly fits into the debate of the amendment, should the amendment be further debated.

The gentleman from Florida has the floor.

Mr. WEXLER. I think I have stated my case, Mr. Chairman. If I could just respectfully suggest, there does not appear to be any substantive reason why this objection needs to be made. I do not believe in any way we are expanding the scope of the bill under this amendment. This is different than the first amendment. It is drafted entirely to the specific terms of this bill. And I would respectfully ask Mr. Cannon to consider accepting it.

Chairman SENSENBRENNER. The Chair is prepared to rule. The gentleman from Utah, Mr. Cannon, makes a point of order that the current amendment offered by the gentleman from Florida, Mr. Wexler, is nongermane. The title of the bill is to amend Title 5 United States Code to require that agencies in promulgating rules take into consideration the impact of such rules on the privacy of individuals, and for other purposes.

The amendment proposes to add further material to the contents of what the agencies are supposed to do on the bottom of page 3 and after line 17 of page 5 of the bill. The Chair believes that these are additional requirements as to the contents of what needs to be put into the rulemaking process under the Administrative Procedures Act and additional contents on what would be in the rule would be germane to this bill. Therefore, the Chair overrules the point of order and the question is on agreeing to the amendment offered by the gentleman from Florida, Mr. Wexler.

All those in favor, signify by saying aye.

Opposed, no.

The ayes appear to have it. The ayes have it. And the amendment by the gentleman from Florida is agreed to.

Are there further amendments to the bill? If there are no further amendments to the bill, a reporting quorum is present. The question is on reporting the bill H.R. 2840 favorably, as amended.

All those in favor, signify by saying aye.

Opposed, no.

The ayes appear to have it. The ayes have it. The motion to report favorably is agreed to.

Without objection, the bill will be reported favorably to the House in the form of a single amendment in the nature of a substitute incorporating the amendments adopted here today.

Without objection, the staff is directed to make any technical and conforming changes. And all Members will be given 2 days, as provided by House rules, in which to submit additional dissenting supplemental or minority views.

[Intervening business.]

[Whereupon, at 3:01 p.m., the Committee was adjourned.]

ADDITIONAL VIEWS

Although we support H.R. 2840, as amended in full committee markup, we offer these additional views to explain the importance of Democratic amendments made to the bill and to express disappointment with the majority's refusal to adopt a crucial amendment offered by Rep. Conyers.

H.R. 2840 amends the Administrative Procedure Act (APA) to require a federal agency to prepare a privacy impact analysis for proposed and final rules and to make available and publish such analyses in the Federal Register.[1] As a result, under the bill, federal agencies will be required to analyze and deeply consider how their rules will impact the privacy interests of individuals. The contents of the privacy impact assessments required under the bill are substantive.[2] In addition, the bill contains sensible provisions permitting judicial review of the adequacy of an agency's final privacy impact analysis and requiring agencies to periodically review rules that have a significant privacy impact on individuals. However, the bill contains some gaps and loopholes that were addressed by a number of Democratic amendments offered at the full committee markup.

First, H.R. 2840 contains a broad national security waiver which allows unfettered discretion to an agency to determine when to make privacy impact assessments available to the public.[3] To tighten this loophole and to prevent such abuses as overclassification, Rep. Schiff offered an amendment, agreed to by voice vote, which requires that when an agency decides that a waiver is warranted, it must disclose the requisite privacy impact assessment, in classified form, to the House and Senate Judiciary Committees.

Second, H.R. 2840, as introduced, did not explicitly address the obligations of government agencies after the discovery of data breaches, including the loss of personal information of 26 million veterans at the Department of Veterans Affairs. For example, the bill lacked a basic notification provision requiring government agencies to provide notice to consumers or to law enforcement officials in the event of a data breach. For this reason, Rep. Wexler offered an amendment that requires agencies to notify individuals,

[1] The bill was introduced on June 9, 2005 by Representative Steve Chabot with Representatives Chris Cannon, Jerrold Nadler, and William Delahunt as original cosponsors. H.R. 2840 has had a significant legislative history. Legislation substantially similar to H.R. 2840 was introduced in the prior three Congresses: H.R. 338 (108th Congress); H.R. 4561 (107th Congress); and H.R. 3307 (106th Congress).

[2] For example, the initial privacy impact assessment must contain, among other requirements, an analysis of the impact of proposed rules and regulations on privacy rights including what personal information will be collected, maintained and disclosed by the federal government and whether the rule prevents personal information, which is collected for one purpose, from being used for another purpose.

[3] The waiver reads, "[a]n agency head may, for national security reasons, or to protect from disclosure classified information, confidential commercial information, or information the disclosure of which may adversely affect a law enforcement effort, waive or delay the completion of some or all of the following requirements . . ."

as soon as practicable, in writing of a data breach. In addition, the amendment requires agency heads to certify to the House and Senate Judiciary Committees that the appropriate notification has in fact been given. The amendment applies to data breaches occurring after the date of the enactment of the Act and a one year period before the date of enactment, including "the compromise of personally identifiable information resulting from the theft of data from an employee of the Department of Veterans Affairs on or around May 3, 2006." Unfortunately, the amendment was ruled as non-germane by the Chair. However, Rep. Wexler introduced another amendment, agreed to by voice vote, requiring that the initial and final privacy impact assessments detailed in the bill contain an analysis of the extent to which the agency rule provides for the provision of written notice to an individual whose personal data has been compromised.

Finally, H.R. 2840 does not directly address the crucial privacy concerns of our time, including the compilation of millions of Americans' phone records into the largest known database in the world and the Administration's blatant violation of privacy rights by authorizing the NSA to engage in warrantless wiretapping. The disclosure of the warrantless wiretapping program on December 16, 2005, raised an obvious conflict with both the Foreign Intelligence Surveillance Act (FISA), which applies to the "interception of international wire communications to or from any person (whether or not a U.S. person) within the United States without the consent of at least one party"[4] and the Fourth Amendment.[5] Government sources have stated that pursuant to this program "the NSA eavesdrops without warrants on up to 500 people in the United States at any given time."[6]

---

[4] Foreign Intelligence Surveillance Act of 1978, Pub. L. 95–511, Title I, 92 Stat. 1796 (Oct. 25, 1978) codified as amended.

[5] The National Security Agency's (NSA) warrantless wiretapping activities were initially disclosed on December 16, 2005, by The New York Times. James Risen & Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, N.Y. TIMES, Dec. 16, 2005, at A1. The next day, the President publicly stated he "authorized the National Security Agency . . . to intercept the international communications of people with known links to al Qaeda and related terrorist organizations." President George W. Bush, President's Radio Address (Dec. 17, 2005), available at http://www.whitehouse.gov/news/releases/2005/12/print/20051217.html. The Attorney General acknowledged that the NSA surveillance is the "kind" that ordinarily "requires a court order before engaging in" it. Attorney General Alberto Gonzales and Principal Deputy Director for National Intelligence General Michael Hayden, Press Briefing (Dec. 19, 2005), available at www.whitehouse.gov/news/releases/2005/12/20051219-1.html. The domestic spying program has engendered widespread opposition, including from a number of Republicans, conservatives, and non-partisan groups. Those who have raised questions or challenged the legal and constitutional underpinnings of the NSA program include: Senate Judiciary Chairman Arlen Specter (R-PA), Senators Chuck Hagel (R-NE), Olympia Snowe (R-ME), Richard Lugar (R-IN), Susan Collins (R-ME), John Sununu (R-NH), Larry Craig (R-ID), Lindsey Graham (R-SC), and John McCain (R-AZ); former GOP Congressman Bob Barr; conservative activists Grover Norquist, David Keene, and Paul Weyrich; former Republican officials such as Judge and former Reagan FBI Director William Sessions, former Reagan Associate Deputy Attorney General Bruce Fein and former Nixon White House Counsel John Dean; conservative legal scholars such as CATO's Robert Levy and University of Chicago Professor Richard Epstein, noted conservative columnists William Safire, George Will, and Steve Chapman; the American Bar Association, the Congressional Research Service, and numerous current and former members of the Bush Administration. Among other things, Senator Specter stated that the Administration's legal interpretation "just defies logic and plain English."

[6] James Risen & Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, N.Y. Times, Dec. 16, 2005, at A1. James Risen's sources recounted in The New York Times, "roughly 500 people in the United States" were eavesdropped on "every day over the past three to four years." MSNBC.com: Interview by Andrea Mitchell with James Risen, (Jan. 3, 2006), available at http://www.msnbc.msn.com/it/10697484/page/4/print/1/displaymode/1098/. Some reports indicated that the total number of people monitored domestically has reached into the thousands, while others

On May 11, 2006, another aspect of the domestic spying scandal erupted. USA Today reported that according to individuals with first-hand knowledge, "[t]he NSA has been secretly collecting the phone call records of tens of millions of Americans."[7] The newspaper reported that "[t]he NSA program reaches into homes and businesses across the nation by amassing information about the calls of ordinary Americans—most of whom aren't suspected of any crime."[8] According to individuals familiar with the program, "[i]t's the largest database ever assembled in the world," and the NSA's goal is "to create a call of every call ever made" in the U.S.[9]

Due to the significant privacy breaches attendant to the Administration's warrantless surveillance and database collection programs, Rep. Conyers offered an amendment clarifying that actions or authorizations relating to the programs fall within the bill.[10] A debate ensued between the Democratic and Republican members of the committee on whether the amendment appropriately fit within the confines of H.R. 2840 and the APA. Since H.R. 2840 amends the APA, which applies to agency actions, the Conyers amendment would arguably bring in some presidential actions or authorizations that are not deemed agency actions subject to the APA. However, the Republican argument was misplaced since the Conyers amendment explicitly states that it is "subject to any restrictions herein." The amendment was ultimately defeated on a party-line vote of 14-12.

H.R. 2840 provides a useful and constructive procedure to protect personal privacy. The bill would, at a minimum, ensure that the public is aware of the potential implications of government regulations that may infringe upon privacy. The Democratic amendments reported out of full committee enhance the bill and address some of its shortcomings. However, considering the Administration's pursuit of warrantless wiretapping, and its massive collection of phone records, the Conyers amendment would have provided additional assurances that the Committee is taking all appropriate steps to halt the assault on the privacy of Americans.

---

have indicated that significantly more people have been spied upon. Eric Lichtblau & James Risen, Spy Agency Mined Vast Data Trove, Officials Report, N.Y. Times, Dec. 23, 2005, at A1.

[7] Leslie Cauley, NSA Has Massive Database of Americans' Phone Calls, USA Today, May 11, 2006 at A1. A number of prominent conservatives and Republicans have also expressed reservations about the NSA data base program. Former GOP Speaker Newt Gingrich declared, "I'm not going to defend the indefensible." Senator Charles Grassley (R-IA) asked "why are the telephone companies not protecting their customers privacy," and House Majority Leader John Boehner stated, ". . . I'm not sure why it would be necessary to keep and have that kind of information."

[8] Leslie Cauley, NSA Has Massive Database of Americans' Phone Calls, USA Today, May 11, 2006 at A1. This is a significant departure from previous practice under which, according to The Washington Post, "government agencies traditionally have been required to obtain a warrant before monitoring Americans conversations or call logs." Barton Gellman and Arshad Mohmmed, Data on Phone Calls Monitored: Extent of Administration's Domestic Surveillance Decried in Both Parties, Washington Post, May 12, 2006 at A1.

[9] *Id.*

[10] The amendment inserted a new section at the end of the bill that read: "The requirements of section 553a of title 5, United States Code, (as amended by section 2 of this Act) relating to privacy impact assessments shall, subject to any restrictions herein, apply with respect to the collection, maintenance, use, or disclosure of personally identifiable information, including any action or authorization relating to the wiretapping or other electronic surveillance of communications by citizens of the United States, and the acquisition or compilation of call records, unless such actions are conducted pursuant to a court order or warrant." The amendment was modified, without objection, to include Rep. Nadler's second-degree amendment that the actions mentioned be covered unless such actions are conducted pursuant to a court order or warrant "or the provisions of the FISA Act."

DESCRIPTION OF AMENDMENTS OFFERED BY DEMOCRATIC MEMBERS

During the full committee markup, there were 4 amendments offered by Democratic members. One amendment offered by Rep. Conyers, one by Rep. Schiff, and two by Rep.Wexler.

1. Schiff Amendment

Description of Amendment—Rep. Schiff offered an amendment which requires that when an agency decides that a national security waiver is warranted, it must disclose the requisite privacy impact assessment, in classified form, to the House and Senate Judiciary Committees.

Vote on Amendment: The amendment was agreed to on a voice vote.

*2. Conyers Amendment**

Description of Amendment—This amendment clarifies that the bill covers "any action or authorization relating to the wiretapping or other electronic surveillance of communications by citizens of the United States, and the acquisition or compilation of call records, unless such actions are conducted pursuant to a court order or warrant."

Vote on Amendment: The amendment was defeated by a party-line vote of 14-12. Ayes: Representatives Conyers, Delahunt, Jackson Lee, Meehan, Nadler, Sanchez, Schiff, Scott, Van Hollen, Wasserman Schultz, Weiner, Wexler; Nays: Representatives Coble, Goodlatte, Sensenbrenner, Jenkins, Chabot, Lungren, Cannon, Hostettler, Green, Keller, Forbes, Franks, Feeney, King.

*The Conyers Amendment was modified without objection by a second-degree amendment offered by Rep. Nadler that added to the end the following language: "or the provisions of the FISA Act."

3. Wexler Amendment

Description of Amendment—This Amendment requires agencies to notify individuals, as soon as practicable, in writing of a data breach. In addition, the amendment requires agency heads to certify to the House and Senate Judiciary Committees that the appropriate notification has in fact been given. The amendment applies to data breaches occurring after the date of the enactment of the Act and a one year period before the date of enactment, including "the compromise of personally identifiable information resulting from the theft of data from an employee of the Department of Veteran Affairs on or around May 3, 2006."

Vote on Amendment: The Amendment was ruled as not germane by the Chair.

4. Wexler Amendment

Description of Amendment—This Amendment requires that the initial and final privacy impact assessments detailed in the bill contain an analysis of the extent to which the agency rule provides for the provision of written notice to an individual, within 14 days of the date of compromise, whose personal data has been compromised.

Vote on Amendment: The Amendment was agreed to on a voice vote.

JOHN CONYERS, JR.
ZOE LOFGREN.
MAXINE WATERS.
MARTIN T. MEEHAN.
WILLIAM D. DELAHUNT.
ROBERT WEXLER.
ADAM B. SCHIFF.
LINDA T. SÁNCHEZ.
CHRIS VAN HOLLEN.

○