

FEDERAL AGENCY PROTECTION OF PRIVACY ACT OF 2004

JULY 7, 2004.—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

[To accompany H.R. 338]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 338) 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 .....	1
Purpose and Summary .....	5
Background and Need for the Legislation .....	6
Hearings .....	10
Committee Consideration .....	11
Vote of the Committee .....	11
Committee Oversight Findings .....	11
New Budget Authority and Tax Expenditures .....	11
Congressional Budget Office Cost Estimate .....	11
Performance Goals and Objectives .....	12
Constitutional Authority Statement .....	12
Section-by-Section Analysis and Discussion .....	13
Changes in Existing Law Made by the Bill, as Reported .....	15
Markup Transcript .....	21

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 2004”.

**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 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.

“(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 objec-

tives 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.

“(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.”.

### PURPOSE AND SUMMARY

H.R. 338, the “Federal Agency Protection of Privacy Act of 2004,” preserves and promotes the privacy rights of all Americans by requiring Federal agencies to assess and mitigate the adverse privacy impact of certain rules noticed for public comment pursuant to the Administrative Procedure Act (APA).<sup>1</sup> The bill 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. 338 makes no substantive demands on 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<sup>2</sup> and the E-Government Act of 2002.<sup>3</sup>

Specifically, H.R. 338 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. H.R. 338, as reported, includes a limited waiver from certain requirements for na-

<sup>1</sup> 5 U.S.C. § 551 *et seq.* (2002).

<sup>2</sup> Pub. L. No. 96–354, 94 Stat. 1164 (codified at 5 U.S.C. §§ 601 *et seq.* (2002)). 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, § 242, Pub. L. No. 104–121, 110 Stat. 857 (1996) (codified in scattered sections of the U.S.C.), subjects the regulatory flexibility analysis to judicial review. 5 U.S.C. § 611 (2002).

<sup>3</sup> Pub. L. No. 107–347, § 208, 116 Stat. 2899, 2921 (2002) (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).

tional security reasons or to prevent the disclosure of other sensitive information.

## BACKGROUND AND NEED FOR THE LEGISLATION

### PRIVACY IN THE HANDS OF THE FEDERAL GOVERNMENT

#### *In General*

The Federal Government collects vast amounts of personally identifiable information on every American—from birth until death—and uses this information for any number of reasons, such as law enforcement, national security, tax collection, and benefits eligibility determinations.<sup>4</sup> Under certain circumstances, this information may be disseminated to various agencies within the Federal Government and shared with state and local governments.<sup>5</sup> Some governmental entities, such as the Federal bankruptcy court system, are required by law to provide public access to case files,<sup>6</sup> which contain a plethora of personally identifiable information about a debtor, including the names and ages of the debtor’s dependent children.<sup>7</sup>

Pursuant to the Privacy Act of 1974,<sup>8</sup> however, executive branch Federal agencies are generally prohibited from disclosing personally identifiable information to other Federal or state agencies or to any other person,<sup>9</sup> subject to certain specified exceptions.<sup>10</sup> An agency that releases such information in violation of the Privacy Act is liable for damages sustained by an individual as a result of such violation under certain circumstances.<sup>11</sup> In addition, the Privacy Act grants individuals the right to have agency records maintained on themselves corrected upon a showing that such records are inaccurate, irrelevant, out-of-date, or incomplete.<sup>12</sup>

<sup>4</sup> See, e.g., Gun Control Act of 1968, 18 U.S.C. §§ 921 *et seq.* (2002) (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.* (2002) (requiring financial institutions to maintain records of personal financial transactions that “have a high degree of usefulness in criminal, tax and regulatory investigations and proceedings”); 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).

<sup>5</sup> 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. James Harper, *Government Exchange and Merger of Citizens’ Personal Information is Systematic and Routine* (Mar. 2001), at <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 their intention to exchange personal data and combine it into their own databases. *Id.*

<sup>6</sup> 11 U.S.C. § 107 (2002).

<sup>7</sup> See Official Bankr. Form No. 6. Rule 9009 of the Federal Rules of Bankruptcy Procedure mandates the use of Official Bankruptcy Forms as prescribed by the Judicial Conference of the United States. Fed. R. Bankr. P. 9009.

<sup>8</sup> 5 U.S.C. § 552a (2002). 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 CONFERENCE OF THE UNITED STATES, FEDERAL ADMINISTRATIVE PROCEDURE SOURCEBOOK—STATUTES AND RELATED MATERIALS 863 (2d ed. 1992).

<sup>9</sup> 5 U.S.C. § 552a(b) (2002). The types of information that may not be disclosed include medical, educational, criminal, financial, and employment records. 5 U.S.C. § 552a(a)(4) (2002).

<sup>10</sup> 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(a)(7), (b)(3) (2002). 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) (2002).

<sup>11</sup> 5 U.S.C. § 552a(g)(4) (2002).

<sup>12</sup> 5 U.S.C. § 552a(d)(2) (2002).

Last year, however, the General Accounting Office (GAO), while noting that agency compliance with the Privacy Act is “generally high in many areas,” reported that such compliance is “uneven across the Federal Government.”<sup>13</sup> As technological developments increasingly facilitate the collection and dissemination of personally identifiable information, the potential for misuse of such information increases. The GAO has observed:

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.<sup>14</sup>

The misuse of personally identifiable information in the hands of the Federal Government presents several concerns. One pertains to the problems raised by potentially unrestricted access to such information by unscrupulous individuals who use this information for various fraudulent activities. The other relates to the potential for the government to use this information to invade the privacy of innocent Americans. A third concern pertains to the adverse consequences that individuals may encounter when the government relies on inaccurate information.

*Potential for Misuse of Personally Identifiable Information in the Government’s Hands*

Identity theft,<sup>15</sup> for example, illustrates a major aspect of the first concern. Thanks to the largely unfettered use of Social Security numbers<sup>16</sup> and the availability of other personally identifiable information through technological advances, identity theft has swiftly evolved into one of the most prolific crimes in the United States. The Federal Trade Commission (FTC), for instance, reported that the number of identity theft complaints it received in 2002 nearly doubled over the number it received the previous year and that identity theft is the Commission’s “most widely reported consumer crime since the agency started issuing reports 3 years

<sup>13</sup>U.S. General Accounting Office, Privacy Act: OMB Leadership Needed To Improve Agency Compliance, GAO-03-304, at 3 (June 2003).

<sup>14</sup>U.S. General Accounting Office, Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information, GAO-01-126SP, at 1 (Apr. 2001).

<sup>15</sup>As explained by one academic:

An identity thief begins by discovering the name and Social Security number of a potential victim and using it to open credit accounts in that person’s name. The creditors accept the thief’s assertion of identity principally because the thief knows the victim’s number. In this transaction, the Social Security number serves as a password—knowledge of the number is accepted as proof of identity.

Lynn M. LoPucki, *Better Way To Stop A(n Identity) Thief*, JEWISH WORLD REV. , Sept. 5, 2001, available at <http://www.jewishworldreview.com/0901/catch.thief.asp>

Another form of identity theft involves a situation where the thief gains access to a person’s existing account and makes fraudulent charges. *The Fair Credit Reporting Act—How It Functions for Consumers and the Economy: Hearing Before the Subcomm. on Financial Institutions and Consumer Credit of the House Comm. on Financial Services*, 108th Cong. 315 (2003) (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Group).

<sup>16</sup>Social Security numbers, for example, are widely used by the government and private industry as a standard identifier in connection with verifying credit and other commercial transactions, the collection of taxes by Federal and state governments, administration of various governmental benefits, and student identification numbers, among other purposes. See *Use and Misuse of Social Security Numbers: Hearing Before the Subcomm. on Social Security of the House Comm. on Ways and Means*, 108th Cong. 2 (2003) (noting that Social Security numbers are “an invaluable tool for identity thieves”).

ago.”<sup>17</sup> In 2003, identity theft again represented one of the primary sources of complaints received by the FTC.<sup>18</sup> A survey conducted last year estimates that at least 13 million Americans have been victims of identity theft since 2001.<sup>19</sup> Although the Identity Theft and Assumption Deterrence Act of 1998<sup>20</sup> was enacted to address this problem, concerns persist.<sup>21</sup> Congress has recently responded again to this problem by passing the “Identity Theft Penalty Enhancement Act.”

Unrestricted access to personally identifiable information in public records can also lead to more serious crimes. For example, the Driver’s Privacy Protection Act of 1994<sup>22</sup> was enacted in response to the murder of actress Rebecca Shaeffer whose assailant obtained her address from state driving records.

Notwithstanding the serious consequences that can result when personally identifiable information is accessible by unscrupulous individuals, a series of GAO reports over the past several years highlights the vulnerability of personal data maintained by the Federal Government. In one report, 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.”<sup>23</sup> The study found that “information security weaknesses place enormous amounts of confidential data, ranging from personal and tax data to proprietary business information, at risk of inappropriate disclosure.”<sup>24</sup> Agencies cited in this highly critical report included the Treasury Department,<sup>25</sup> the Department of Health and Human Services,<sup>26</sup> and the Social Security Administration.<sup>27</sup>

In another report, the GAO found that eight Federal Government web sites had “persistent cookies” (user information collecting devices) and that four of these web sites failed to alert users about their existence.<sup>28</sup> Pursuant to a July 2000 survey that the GAO conducted of 65 Federal web sites, the GAO found that only 3 percent of these sites adhered to the principles of notice, choice, access, and security that the Federal Trade Commission specifies for

<sup>17</sup> Jennifer S. Lee, *Identity Theft Complaints Double in '02*, N.Y. TIMES, Jan. 23, 2003, at A18. See Federal Trade Commission Report: Overview of the Identity Theft Program October 1998–September 2003 at 1 (Sept. 2003).

<sup>18</sup> Maudlyne Ihejirika, *Identity Theft Is Tops Among Consumer Complaints*, CHI. SUN-TIMES, Jan. 23, 2004, at 16 (noting that of 516,740 complaints received by the FTC, 42% involved identity theft).

<sup>19</sup> Vivian Marino, *Identity Theft Thriving, and Proving Expensive*, N.Y. TIMES, Aug. 3, 2003, at 8.

<sup>20</sup> Pub. L. No. 105–318, 112 Stat. 3007 (1998) (codified in scattered sections of the U.S.C.).

<sup>21</sup> See, e.g., U.S. General Accounting Office, *Security: Counterfeit Identification and Identification Fraud Raise Security Concerns*, GAO–03–1147T (Sept. 9, 2003); Kathleen Swendiman, *The Social Security Number: Legal Developments Affecting Its Collection, Disclosure and Confidentiality*, Congressional Research Service Report, RL30318 (Apr. 25, 2003).

<sup>22</sup> 18 U.S.C. §§ 2721 *et seq.* (2002).

<sup>23</sup> U.S. General Accounting Office, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD–00–295, at 2 (Sept. 2000).

<sup>24</sup> *Id.*

<sup>25</sup> *Id.* at 9 (noting, for example, that the IRS computer security controls “continued to place taxpayer and other data in IRS’ automated systems at serious risk of unauthorized disclosure, modification, or destruction”).

<sup>26</sup> *Id.* at 12–13 (noting that the “[m]ost 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).

<sup>27</sup> *Id.* at 13–15 (noting that such weaknesses “might allow an individual or group to fraudulently obtain [Social Security] payments by creating fictitious beneficiaries or increasing payment amounts”).

<sup>28</sup> U.S. General Accounting Office, *Internet Privacy: Implementation of Federal Guidance for Agency Use of “Cookies,”* GAO–01–424, at 2 (Apr. 2001).

private-sector web sites.<sup>29</sup> In 2001, the General Services Administration Inspector General identified an Internet site managed by a private contractor who was given ownership of all user data collected by a persistent cookie installed by the contractor into the government website.<sup>30</sup> In 2002, computer equipment containing the personal information of approximately 562,000 people was stolen from a Pentagon medical claims contractor.<sup>31</sup>

*Issues Presented by the Government's Developing Surveillance Technologies and Reliance on Inaccurate Personal Data*

Increasingly, local jurisdictions are installing surveillance cameras for law enforcement purposes, such as photographing motorists to identify alleged speed-limit violators. In the borough of Manhattan in New York City alone, for example, 2,397 surveillance cameras have been installed.<sup>32</sup> Facial recognition systems are rapidly becoming another form of government surveillance technology. In Tampa, Florida, for example, facial recognition technology was used during the 2001 Super Bowl to photograph attendees' faces and compare them with those of suspects.<sup>33</sup> Much like a virtual "police line-up," the faces of thousands of sports fans attending the game were photographed digitally so that they could be compared with a database of criminals' faces. The technology was not used at the 2002 Super Bowl because, according to a local law enforcement official, "It doesn't work."<sup>34</sup>

In addition to these technologies, the Federal Government is currently exploring the terrorist detection capabilities of data mining, a system that utilizes sophisticated data analysis tools to scan large databases to identify "valid patterns and relationships."<sup>35</sup> In private industry, data mining has been used to detect fraud, assess risk, as well as conduct product and medical research.<sup>36</sup> Data mining is used by the Justice Department to assess crime patterns and adjust resource allotments and by the Veterans Administration to predict demographic changes in the constituency it serves for budgetary purposes.<sup>37</sup>

The Congressional Research Service has observed that data mining presents certain issues pertaining to data quality and privacy

<sup>29</sup> *Recent Developments in Privacy Protections for Consumers: Hearing Before the Subcomm. on Telecommunications, Trade, and Consumer Protection of the House Comm. on Commerce*, 106th Cong. 26 (2000).

<sup>30</sup> Press Statement, *Thompson: Preliminary Reports Reveal Continued Agency Violations of Administration Privacy Policies*, U.S. Senate Committee on Governmental Affairs (Apr. 16, 2001).

<sup>31</sup> Jennifer S. Lee, *Identity Theft Complaints Double in '02*, N.Y. TIMES, Jan. 23, 2003, at A18.

<sup>32</sup> NYC Surveillance Camera Project Summary, at <http://www.mediaeater.com/cameras/summary.html> (visited June 29, 2004).

<sup>33</sup> Dennis O'Brien, *Biometrics: Fraud, Terror Attacks and Privacy Laws Have Many Seeking Foolproof Ways to Identify People*, BALTIMORE SUN, May 5, 2003, at 8A.

<sup>34</sup> *Id.* (quoting William Mahew, Assistant Police Chief, San Diego, California).

<sup>35</sup> Jeffrey W. Seifert, *Data Mining: An Overview*, Congressional Research Service Report for Congress, RL31798, at 1 (May 3, 2004). Data mining applications include:

association (patterns where one event is connected to another event, such as purchasing a pen and purchasing paper), sequence or path analysis (patterns where one event leads to another event, such as the birth of a child and purchasing diapers), classification (identification of new patterns, such as coincidences between duct tape purchases and plastic sheeting purchases), clustering (finding and visually documenting groups of previously unknown facts, such as geographic location and brand preferences), and forecasting (discovering patterns from which one can make reasonable predictions regarding future activities, such as the prediction that people who join an athletic club may take exercise classes).

*Id.*

<sup>36</sup> *Id.* at 3-4.

<sup>37</sup> *Id.* at 4.

that may warrant scrutiny.<sup>38</sup> The data quality issues relate to the accuracy and completeness of the data being analyzed, while the privacy implications of data mining concern the propriety of Federal agencies using and mixing “commercial data with government data, whether data sources are being used for purposes other than those for which they were originally designed, and possible application of the Privacy Act to these initiatives.”<sup>39</sup>

To the extent Federal agencies use data collected from a “wide range of commercial and governmental sources, such as credit card records, motor vehicle and property records, license records, marriage and divorce data, bankruptcy and other court databases, product warranty registrations, loan applications and other sources”<sup>40</sup> for law enforcement or security purposes, the accuracy of the data being collected—or data quality—becomes critically important. If a database contains inaccurate information, “innocent people could be branded security risks on the basis of flawed data and without any meaningful way to challenge the government’s determination.”<sup>41</sup>

An example of how the Federal Government’s use of inaccurate data can affect citizens in their daily lives was experienced by various airline passengers named “David Nelson.” Passengers sharing this name were singled out for heightened security,<sup>42</sup> even though they had no idea why they were being scrutinized and had no effective way to correct the apparently erroneous information causing the recurrent security advisory.<sup>43</sup>

#### HEARINGS

The Committee’s Subcommittee on Commercial and Administrative Law and the Subcommittee on the Constitution held one hearing on H.R. 338 on July 22, 2003.<sup>44</sup> Testimony was received from United States Senator Charles E. Grassley (R-IA), former Con-

<sup>38</sup>*Id.* at 2.

<sup>39</sup>*Id.* at 7.

<sup>40</sup>William Matthews, *Commercial Database Use Flagged*, FEDERAL COMPUTER WEEK, Jan. 16, 2002, available at <http://www.fcw.com/fcw/articles/2002/0114/web-epic-01-16-02.asp>. Among the agencies that apparently purchase these data are the Federal Bureau of Investigation, the Drug Enforcement Administration, the U.S. Marshals Service, the Internal Revenue Service, the Immigration and Naturalization Service, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives. *Id.*

<sup>41</sup>Letter to Rep. Christopher Cox, Chair, & Rep. Jim Turner, Ranking Member, House Select Committee on Homeland Security, from Privacy Coalition (Mar. 25, 2003), available at <http://www.eff.org/Privacy/TIA/20030324-capps-letter.php>. Members of the Privacy Coalition represent a broad political spectrum ranging from the American Civil Liberties Union to the American Conservative Union. Other members include Americans for Tax Reform, the Christian Coalition, the Eagle Forum, and the People for the American Way.

<sup>42</sup>See, e.g., Rex W. Huppke, *Name Can Set Off Bells with Airport Security; David Nelsons Need Extra Time, Patience at U.S. Checkpoints*, CHI. TRIB., June 29, 2003, at 1C (reporting on the similar experiences of four David Nelsons); Joe Kennedy, *It’s a Tough Time To Be David Nelson*, ROANOKE TIMES & WORLD NEWS, June 28, 2003, at B1 (reporting on one David Nelson, among others, who “had been taken out of line every time he has traveled since the terrorist attacks on the World Trade Center—even though he works on Capitol Hill and often flies on tickets bought by the government”); Tom Ramstack & Patrick Badgely, *Name Won’t Fly If You Are David Nelson*, WASHINGTON TIMES, June 17, 2003, at A1.

<sup>43</sup>One David Nelson, who was detained at least 15 times for heightened security analysis when he checked in at different airports over a period of several months, contacted the TSA to try to have the agency address this problem on several occasions, but to no avail. Telephone interview by Susan Jensen, Counsel, Subcommittee on Commercial and Administrative Law of the House Committee on the Judiciary, with David Nelson of McLean, Virginia (July 9, 2003); Tom Ramstack & Patrick Badgely, *Name Won’t Fly If You Are David Nelson*, WASHINGTON TIMES, June 17, 2003, at A1.

<sup>44</sup>*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 House Comm. on the Judiciary*, 108th Cong. (2003).

gressman Bob Barr (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 February 10, 2004, the Subcommittee on Commercial and Administrative Law met in open session and ordered favorably reported the bill, H.R. 338, as amended, by voice vote, a quorum being present. On June 23, 2004, the Committee met in open session and ordered favorably reported the bill, H.R. 338, 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 there were no recorded votes during the Committee consideration of H.R. 338.

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. 338, 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, July 2, 2004.*

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. 338, the Federal Agency Protection of Privacy Act of 2004.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Matthew Pickford.

Sincerely,

DOUGLAS HOLTZ-EAKIN, *Director.*

Enclosure

*H.R. 338—Federal Agency Protection of Privacy Act of 2004*

H.R. 338 would require Federal agencies to assess proposed regulations to determine the impact on the privacy of individuals. The legislation would exclude any agency rule that does not have an impact on personally identifiable information. H.R. 338 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. Finally, agencies would have to review existing rules to consider impacts on the privacy of individuals at least every 10 years.

CBO estimates that implementing H.R. 338 would have no significant effect on Federal spending. Based on a review on the number and types of agency rules published in recent years, we expect that the collection, maintenance, use, or disclosure of personally identifiable information is a concern for a small percentage of the rules published annually. H.R. 338 would add to the existing regulatory procedures for considering impacts 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 current Office of Management and Budget requirements concerning information collected from the public. Based on information from some agencies that would be affected by the bill, we expect that implementing this bill would not require significant additional efforts by rulemaking agencies. Thus, its implementation would not have a significant cost.

H.R. 338 also could affect direct spending by increasing the administrative costs of rulemaking agencies that receive no annual appropriations. However, CBO estimates that any increase in direct spending would not be significant. The bill contains no inter-governmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of State, local, or tribal governments.

The CBO staff contact for this estimate is Matthew Pickford. This estimate was approved by Peter H. Fontaine, Deputy 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. 338, protects the privacy rights of all Americans by requiring that Federal agencies assess, consider, and inform the public about the privacy impact of certain rules noticed for public comment under the Administrative Procedure 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 I, section 8, and the Fourth Amendment of the Constitution.

## SECTION-BY-SECTION ANALYSIS AND DISCUSSION

*Section 1. Short Title*

Section 1 sets forth the title of the bill as the “Federal Agency Protection of Privacy Act of 2004.”

*Section 2. Requirement That Agency Rulemaking Take Into Consideration Impacts on Individual Privacy*

*Initial Privacy Impact Assessment.* Subsection 2(a) of H.R. 338 amends title 5 of the United States Code to require 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.

Pursuant to new subsection 553a(a), the assessment 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 rule. The following matters must be set forth in the assessment: (1) a description of the rule’s impact on the privacy of individuals, including an explanation of what personally identifiable information is being 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 may correct any inaccuracies; (3) the extent to which the rule prevents such information, which is collected for one purpose, from being used for another purpose; (4) the extent to which such information is protected; and (5) a description of 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.

*Final Privacy Impact Assessment.* Subsection 2(a) of the bill 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 subsection 553a(b). The following matters must be set forth in the assessment: (1) a description of the rule’s impact on the privacy of individuals, including an explanation of what personally identifiable information is being 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 may correct any inaccuracies; (3) the extent to which the rule prevents such information, which is collected for one purpose, from being used for another purpose; and (4) the extent to which such information is protected. In addition, the assessment

must: (1) summarize any significant issues raised by public comments received in response to the initial privacy assessment; (2) include the agency's analysis of such issues; and (3) identify any changes made in 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.

*Waivers.* New subsection 553a(c) contains two waivers. One 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).

The second waiver permits an agency head to waive or delay certain requirements 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. For a proposed or final rule, the provision permits the waiver or delay of the requirements to make the assessment available for public comment and to publish the assessment in the Federal Register.

*Public Participation.* New subsection 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.

*Periodic Review.* New subsection 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) the 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) the impact of technological, economic, or other factors on the rule. These periodic reviews are required to be conducted in accordance with a plan published 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.

*Judicial Review.* New subsection 553a(f) 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 subsection 553a(b)) and with respect to the waiver provision (as set forth in new subsection 553a(c)). Agency compliance with new sub-

section 553a(d) (concerning public participation) is judicially reviewable in connection with judicial review of new subsection 553a(b). New subsection 553a(f) specifies the jurisdictional and time limits applicable to judicial review. Judicial review 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. A court may order the agency to take corrective action, including remanding the rule to the agency or deferring enforcement of the rule. 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.

*Definition of Personally Identifiable Information.* New subsection 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.

*Periodic Review Transition Provisions.* Subsection 2(b) of H.R. 338 requires an agency to publish the plan required under new subsection 553a(e) within 180 days from the date of enactment of this Act. 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 1 year, under certain circumstances. In no event, however, may the period exceed 15 years.

*Congressional Review.* Subsection 2(c) of H.R. 338 amends subsection 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.

*Clerical Amendment.* Subsection 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.	*	*	*	*	*
553a.	<i>Privacy impact assessment in rulemaking.</i>	*	*	*	*	*

**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.*

(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.

(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.*

(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.*

\* \* \* \* \*

**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 23, 2004**

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

The Committee met, pursuant to notice, at 10:09 a.m., in Room 2141, Rayburn House Office Building, Hon. F. James Sensenbrenner, Jr. [Chairman of the Committee] presiding.

[Intervening business.]

Chairman SENSENBRENNER. The next item on the agenda is H.R. 338, the "Defense of Privacy Act."

The Chair recognizes the gentleman from Utah, Mr. Cannon, winner and still champ in Utah's 3rd district. Congratulations. The Chairman of the Subcommittee on Commercial and Administrative Law.

Mr. CANNON. I thank the Chairman for acknowledging that. A little scary last night, because only a third of the people voted in our Republican primary since we closed the primary and made it registered Republicans only. So it is harder to predict a small turnout like that, but it worked very well, thank you.

And, Mr. Chairman, the Subcommittee on Commercial and Administrative Law reports favorably the bill H.R. 338 with a single amendment in the nature of a substitute, and I move its favorable recommendation to the full House.

Chairman SENSENBRENNER. Without objection, the bill will be considered as read and open for amendment at any point, and the Subcommittee amendment in the nature of a substitute which the Members have before them will be considered as read, considered as the original text for purposes of amendment and open for amendment at any point.

The Chair recognizes the gentleman from Utah, Mr. Cannon, to strike the last word.

[The Subcommittee Amendment in the Nature of a Substitute to H.R. 338 follows:]

**SUBCOMMITTEE AMENDMENT IN THE NATURE OF  
A SUBSTITUTE TO H.R. 338  
(AS ORDERED REPORTED BY THE SUBCOMMITTEE  
ON COMMERCIAL AND ADMINISTRATIVE LAW  
ON FEBRUARY 10, 2004)**

Strike all after the enacting clause and insert the following:

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Federal Agency Pro-  
3 tection of Privacy Act of 2004”.

4 **SEC. 2. REQUIREMENT THAT AGENCY RULEMAKING TAKE  
5 INTO CONSIDERATION IMPACTS ON INDI-  
6 VIDUAL PRIVACY.**

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

10 **“§ 553a. Privacy impact analysis in rulemaking**

11 (a) INITIAL PRIVACY IMPACT ANALYSIS.—

12 “(1) IN GENERAL.—Whenever an agency is re-  
13 quired by section 553 of this title, or any other law,  
14 to publish a general notice of proposed rulemaking  
15 for any proposed rule, or publishes a notice of pro-

1 posed rulemaking for an interpretative rule involving  
2 the internal revenue laws of the United States, the  
3 agency shall prepare and make available for public  
4 comment an initial privacy impact analysis that de-  
5 scribes the impact of the proposed rule on the pri-  
6 vacy of individuals. Such analysis or a summary  
7 thereof shall be signed by the senior agency official  
8 with primary responsibility for privacy policy and be  
9 published in the Federal Register at the time of the  
10 publication of a general notice of proposed rule-  
11 making for the rule.

12 “(2) CONTENTS.—Each initial privacy impact  
13 analysis required under this subsection shall contain  
14 the following:

15 “(A) A description and assessment of the  
16 extent to which the proposed rule will impact  
17 the privacy interests of individuals, including  
18 the extent to which the proposed rule—

19 “(i) provides notice of the collection of  
20 personally identifiable information, and  
21 specifies what personally identifiable infor-  
22 mation is to be collected and how it is to  
23 be collected, maintained, used, and dis-  
24 closed;

1           “(ii) allows access to such information  
2           by the person to whom the personally iden-  
3           tifiable information pertains and provides  
4           an opportunity to correct inaccuracies;

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

8           “(iv) provides security for such infor-  
9           mation.

10          “(B) A description of any significant alter-  
11          natives to the proposed rule which accomplish  
12          the stated objectives of applicable statutes and  
13          which minimize any significant privacy impact  
14          of the proposed rule on individuals.

15          “(b) FINAL PRIVACY IMPACT ANALYSIS.—

16          “(1) IN GENERAL.—Whenever an agency pro-  
17          mulgates a final rule under section 553 of this title,  
18          after being required by that section or any other law  
19          to publish a general notice of proposed rulemaking,  
20          or promulgates a final interpretative rule involving  
21          the internal revenue laws of the United States, the  
22          agency shall prepare a final privacy impact analysis,  
23          signed by the senior agency official with primary re-  
24          sponsibility for privacy policy.

1           “(2) CONTENTS.—Each final privacy impact  
2 analysis required under this subsection shall contain  
3 the following:

4           “(A) A description and assessment of the  
5 extent to which the final rule will impact the  
6 privacy interests of individuals, including the  
7 extent to which such rule—

8           “(i) provides notice of the collection of  
9 personally identifiable information, and  
10 specifies what personally identifiable infor-  
11 mation is to be collected and how it is to  
12 be collected, maintained, used, and dis-  
13 closed;

14           “(ii) allows access to such information  
15 by the person to whom the personally iden-  
16 tifiable information pertains and provides  
17 an opportunity to correct inaccuracies;

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

21           “(iv) provides security for such infor-  
22 mation.

23           “(B) A summary of any significant issues  
24 raised by the public comments in response to  
25 the initial privacy impact analysis, a summary

1 of the assessment of the agency of such issues,  
2 and a statement of any changes made in such  
3 rule as a result of such issues.

4 “(C) A description of the steps the agency  
5 has taken to minimize the significant privacy  
6 impact on individuals consistent with the stated  
7 objectives of applicable statutes, including a  
8 statement of the factual, policy, and legal rea-  
9 sons for selecting the alternative adopted in the  
10 final rule and why each one of the other signifi-  
11 cant alternatives to the rule considered by the  
12 agency which affect the privacy interests of in-  
13 dividuals was rejected.

14 “(3) AVAILABILITY TO PUBLIC.—The agency  
15 shall make copies of the final privacy impact anal-  
16 ysis available to members of the public and shall  
17 publish in the Federal Register such analysis or a  
18 summary thereof.

19 “(c) PROCEDURE FOR WAIVER OR DELAY OF COM-  
20 PLETION.—An agency head may waive or delay the com-  
21 pletion of some or all of the requirements of subsections  
22 (a) and (b) to the same extent as the agency head may,  
23 under section 608, waive or delay the completion of some  
24 or all of the requirements of sections 603 and 604, respec-  
25 tively.

1       “(d) PROCEDURES FOR GATHERING COMMENTS.—  
2 When any rule is promulgated which may have a signifi-  
3 cant privacy impact on individuals, or a privacy impact  
4 on a substantial number of individuals, the head of the  
5 agency promulgating the rule or the official of the agency  
6 with statutory responsibility for the promulgation of the  
7 rule shall assure that individuals have been given an op-  
8 portunity to participate in the rulemaking for the rule  
9 through techniques such as—

10           “(1) the inclusion in an advance notice of pro-  
11 posed rulemaking, if issued, of a statement that the  
12 proposed rule may have a significant privacy impact  
13 on individuals, or a privacy impact on a substantial  
14 number of individuals;

15           “(2) the publication of a general notice of pro-  
16 posed rulemaking in publications of national circula-  
17 tion likely to be obtained by individuals;

18           “(3) the direct notification of interested individ-  
19 uals;

20           “(4) the conduct of open conferences or public  
21 hearings concerning the rule for individuals, includ-  
22 ing soliciting and receiving comments over computer  
23 networks; and

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

4           “(e) PERIODIC REVIEW OF RULES.—

5           “(1) IN GENERAL.—Each agency shall carry  
6 out a periodic review of the rules promulgated by the  
7 agency that have a significant privacy impact on in-  
8 dividuals, or a privacy impact on a substantial num-  
9 ber of individuals. Under such periodic review, the  
10 agency shall determine, for each such rule, whether  
11 the rule can be amended or rescinded in a manner  
12 that minimizes any such impact while remaining in  
13 accordance with applicable statutes. For each such  
14 determination, the agency shall consider the fol-  
15 lowing factors:

16           “(A) The continued need for the rule.

17           “(B) The nature of complaints or com-  
18 ments received from the public concerning the  
19 rule.

20           “(C) The complexity of the rule.

21           “(D) The extent to which the rule over-  
22 laps, duplicates, or conflicts with other Federal  
23 rules, and, to the extent feasible, with State and  
24 local governmental rules.

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

3           “(F) The degree to which technology, eco-  
4           nomic conditions, or other factors have changed  
5           in the area affected by the rule since the rule  
6           was last reviewed under this subsection.

7           “(2) PLAN REQUIRED.—Each agency shall  
8           carry out the periodic review required by paragraph  
9           (1) in accordance with a plan published by such  
10          agency in the Federal Register. Each such plan shall  
11          provide for the review under this subsection of each  
12          rule promulgated by the agency not later than 10  
13          years after the date on which such rule was pub-  
14          lished as the final rule and, thereafter, not later  
15          than 10 years after the date on which such rule was  
16          last reviewed under this subsection. The agency may  
17          amend such plan at any time by publishing the revi-  
18          sion in the Federal Register.

19          “(3) ANNUAL PUBLICATION.—Each year, each  
20          agency shall publish in the Federal Register a list of  
21          the rules to be reviewed by such agency under this  
22          subsection during the following year. The list shall  
23          include a brief description of each such rule and the  
24          need for and legal basis of such rule and shall invite

1 public comment upon the determination to be made  
2 under this subsection with respect to such rule.

3 “(f) JUDICIAL REVIEW.—

4 “(1) IN GENERAL.—For any rule subject to this  
5 section, an individual who is adversely affected or  
6 aggrieved by final agency action is entitled to judi-  
7 cial review of agency compliance with the require-  
8 ments of subsections (b) and (c) in accordance with  
9 chapter 7. Agency compliance with subsection (d)  
10 shall be judicially reviewable in connection with judi-  
11 cial review of subsection (b).

12 “(2) JURISDICTION.—Each court having juris-  
13 diction to review such rule for compliance with sec-  
14 tion 553, or under any other provision of law, shall  
15 have jurisdiction to review any claims of noncompli-  
16 ance with subsections (b) and (c) in accordance with  
17 chapter 7. Agency compliance with subsection (d)  
18 shall be judicially reviewable in connection with judi-  
19 cial review of subsection (b).

20 “(3) LIMITATIONS.—

21 “(A) An individual may seek such review  
22 during the period beginning on the date of final  
23 agency action and ending 1 year later, except  
24 that where a provision of law requires that an  
25 action challenging a final agency action be com-

1 commenced before the expiration of 1 year, such  
2 lesser period shall apply to an action for judicial  
3 review under this subsection.

4 “(B) In the case where an agency delays  
5 the issuance of a final privacy impact analysis  
6 pursuant to subsection (c), an action for judi-  
7 cial review under this section shall be filed not  
8 later than—

9 “(i) 1 year after the date the analysis  
10 is made available to the public; or

11 “(ii) where a provision of law requires  
12 that an action challenging a final agency  
13 regulation be commenced before the expi-  
14 ration of the 1-year period, the number of  
15 days specified in such provision of law that  
16 is after the date the analysis is made avail-  
17 able to the public.

18 “(4) RELIEF.—In granting any relief in an ac-  
19 tion under this subsection, the court shall order the  
20 agency to take corrective action consistent with this  
21 section and chapter 7, including, but not limited  
22 to—

23 “(A) remanding the rule to the agency;  
24 and

1           “(B) deferring the enforcement of the rule  
2           against individuals, unless the court finds that  
3           continued enforcement of the rule is in the pub-  
4           lic interest.

5           “(5) RULE OF CONSTRUCTION.—Nothing in  
6           this subsection shall be construed to limit the au-  
7           thority of any court to stay the effective date of any  
8           rule or provision thereof under any other provision  
9           of law or to grant any other relief in addition to the  
10          requirements of this subsection.

11          “(6) RECORD OF AGENCY ACTION.—In an ac-  
12          tion for the judicial review of a rule, the privacy im-  
13          pact analysis for such rule, including an analysis  
14          prepared or corrected pursuant to paragraph (4),  
15          shall constitute part of the entire record of agency  
16          action in connection with such review.

17          “(7) EXCLUSIVITY.—Compliance or noncompli-  
18          ance by an agency with the provisions of this section  
19          shall be subject to judicial review only in accordance  
20          with this subsection.

21          “(8) SAVINGS CLAUSE.—Nothing in this sub-  
22          section bars judicial review of any other impact  
23          statement or similar analysis required by any other  
24          law if judicial review of such statement or analysis  
25          is otherwise permitted by law.

1       “(g) DEFINITION.—For purposes of this section, the  
2 term ‘personally identifiable information’ means informa-  
3 tion that can be used to identify an individual, including  
4 such individual’s name, address, telephone number, photo-  
5 graph, social security number or other identifying infor-  
6 mation. It includes information about such individual’s  
7 medical or financial condition.”.

8       (b) PERIODIC REVIEW TRANSITION PROVISIONS.—

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

14           (2) In the case of a rule promulgated by an  
15 agency before the date of the enactment of this Act,  
16 such plan shall provide for the periodic review of  
17 such rule before the expiration of the 10-year period  
18 beginning on the date of the enactment of this Act.  
19 For any such rule, the head of the agency may pro-  
20 vide for a 1-year extension of such period if the head  
21 of the agency, before the expiration of the period,  
22 certifies in a statement published in the Federal  
23 Register that reviewing such rule before the expira-  
24 tion of the period is not feasible. The head of the  
25 agency may provide for additional 1-year extensions

1 of the period pursuant to the preceding sentence,  
2 but in no event may the period exceed 15 years.

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

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

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

9 “(iii) the agency’s actions relevant to section  
10 553a;”.

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

“553a. Privacy impact analysis in rulemaking.”.

Mr. CANNON. Thank you, Mr. Chairman.

The Government's collection, use, dissemination, and protection of personally identifiable information presents far-reaching regulatory issues. Especially 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 Government intrusion.

H.R. 338, I believe, strikes that important balance, and I thank my colleague from the State of Ohio, Mr. Chabot, for taking the initiative to reintroduce the bill in the 108th Congress. H.R. 338 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. 338 is intended to ensure that individual privacy rights are safeguarded by requiring Federal agencies to consider privacy implications presented by the collection, use and dissemination of personally identifiable information. On the other hand, H.R. 338 will not overly burden the work of these agencies. In fact, its analysis requirement is similar to other analyses 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. 338's predecessor in the 107th Congress—that implementation of this measure will not entail "significant costs."

As technological developments increasingly facilitate the collection and dissemination of personally identifiable information, the potential for misuse of such information grows. The General Accounting Office has warned that our nation's increasing ability to accumulate, store, retrieve, cross-reference, analyze and link vast numbers of electronic records produces substantial Federal information benefits as well as increases responsibilities and concerns.

The misuse of personally identifiable information by the Federal Government presents two major concerns. One is the potential for fraud presented by unrestricted access to such information by unscrupulous individuals such as identity thieves. According to the Federal Trade Commission, identity theft has become one of the most widely-reported consumer crimes in recent years. In fact, a study released last year estimates that at least 13 million Americans have been victims of identity theft since 2001.

The other concern relates to those instances when the Government relies on inaccurate personally identifiable information. The Congressional Research Service, for instance, noted that if a database contains inaccurate information, "innocent people could be branded security risks on the basis of flawed data and without any meaningful way to challenge the Government's determination."

At least in response to the regulatory aspects of privacy in the hands of Government, H.R. 338 offers a simple, noncontroversial solution that requires Federal agencies to consider the privacy ramifications with respect to proposed and final rules. As some of you may recall, bipartisan legislation similar to H.R. 338 was introduced by Mr. Chabot in the 106th Congress, and a bill virtually identical to H.R. 338 was introduced by my predecessor, Congressman Bob Barr, in the 107th Congress.

In the last Congress, my Subcommittee held a hearing on legislation substantially identical to H.R. 338, in which a broad political spectrum of witnesses testified in strong support of the legislation. The bill was ordered favorably reported by the Subcommittee as well as by the full Committee without amendment by voice vote. Thereafter, the House, under suspension of the rules, passed the bill without amendment by voice vote.

Unfortunately, the Senate did not consider the bill prior to the conclusion of the 107th Congress. Last year, my Subcommittee, in conjunction with the Subcommittee on the Constitution, held a joint hearing on H.R. 338. Again, broad bipartisan support was expressed for this legislation. On February 10, 2004, my Subcommittee reported the bill as an amendment in the nature of a substitute by voice vote. The revisions to the bill consist simply in revising its title and making certain minor technical corrections.

I urge my colleagues to support H.R. 338 favorably. I report favorably. Thank you, Mr. Chairman. I yield back.

Mr. NADLER. Mr. Chairman?

Chairman SENSENBRENNER. I understand the gentleman from New York, Mr. Nadler, is going to give the Democratic opening statement and is recognized for 5 minutes.

Mr. NADLER. Thank you, Mr. Chairman.

Mr. Chairman, I was pleased to sponsor this bill last Congress with Congressman Barr—two Congresses ago, I suppose, and this Congress with the gentleman from Ohio. And I want to join him 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 2 years ago, requires a privacy impact assessment for any information technology that collects, maintains or disseminates information that is in an identifiable form, close quote.

This legislation and the substitute that we will consider later on mirrors the language in the E-Government Act. An example of the need for a formal requirement can be found in the implementation of the U.S. VISIT Program, which in its original form did not provide for a redress policy. The privacy officer for DHS, an office that this Committee established, did a privacy impact analysis of that program, even though one was not required by law, which gave privacy advocates the opportunity to raise their concerns.

While many of us still have serious concerns about the U.S. VISIT Program, the analysis and the dialogue that it prompted brought that problem to light. By looking at privacy interests in advance, we will have the opportunity to address concerns before problems arise rather than after they become institutionalized, and the agency is on the defensive.

It will also protect agencies from themselves by forcing them to consider these vital privacy issues before they become problems. It will help Government get it the first time. The amendment we will consider will make a few important changes. Each of these changes brings this bill in line with the language of the E-Government Act. The minority witness at our hearing, Sally Katzen, recommended that we avoid overlap, and I believe that this change will help accomplish that end.

It will also narrow the mandate to avoid application to many rulemakings that do not have privacy implications, such as the rules setting the dates for duck hunting season. While every concern may not be addressed by this bill and by the amendment that will be offered, this bill is an important step toward making our Government consider the privacy implications of its actions, something that has been woefully lacking, especially in recent years.

We have also checked with the Center for Democracy and Technology concerning this change. I am confident this legislation will be a step in the right direction, and we should move it forward with the amendment that has been offered.

Privacy is not 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. I urge the passage of this bill with the amendment, and I yield back the balance of my time.

Chairman SENSENBRENNER. Without objection, all Members' opening statements will be included in the record at this point.

[The prepared statement of Ms. Jackson Lee follows:]

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS, AND RANKING MEMBER, SUBCOMMITTEE ON IMMIGRATION, BORDER SECURITY, AND CLAIMS

I thank Chairman Sensenbrenner and Ranking Member Conyers for holding today's markup of H.R. 338, the Defense of Privacy Act. This bill, that the Subcommittee on Commercial and Administrative Law reported favorably, requires federal agencies to (1) analyze the impact of proposed rules and regulations on privacy rights, (2) examine what personal information will be collected, maintained, and disclosed by the federal government, (3) disclose how personally identifiable information will be used by the federal government, and (4) specify whether and under what circumstances personal information will be disseminated among federal and state governmental agencies.

Given the government's wide variety of justifications for its access to personal information that include tax assessment, doling out benefits, and protecting our national security, it is vital that adequate checks be put into place to provide the necessary buffer for individual privacy. I am pleased with this bill's method of protecting individual privacy—by establishing legal boundaries for the beginning of the regulatory process.

Justice Thomas Cooley in his treatise on torts defined the notion of "privacy" as the inalienable and natural "right to be let alone." With this legislation as amended, we will be able to keep a protective veil over personal information.

A September 5, 2000 Government Accounting Office study found that 23 of the 70 Federal agencies surveyed had taken personal information from their websites and shared it with third parties (mostly government agencies). Four agencies had shared the information with non-governmental entities. Subsequently, another GAO study concluded that the "information security weaknesses [of Federal government agencies] place enormous amounts of confidential data, ranging from personal and tax to proprietary business information, at risk of inappropriate disclosure."

Given recent legislation that expands law enforcement and governmental information-gathering ability such as the PATRIOT Act and the rising concern for "national security," a foundation must be established to set the threshold for the governmental reach into individual spheres of privacy.

Chairman Sensenbrenner and Ranking Member Conyers, I support this legislation and urge my colleagues to do the same. Thank you.

Chairman SENSENBRENNER. Are there amendments?

And the Chair recognizes the gentleman from Utah, Mr. Cannon, for purposes of offering a manager's amendment.

Mr. CANNON. Thank you, Mr. Chairman. I believe my amendment is an excellent example of the benefits associated with the legislative process.

Chairman SENSENBRENNER. The clerk will report the amendment.

Mr. CANNON. Oh, pardon me.

The CLERK. Amendment to the amendment in the nature of a substitute to H.R. 338, offered by Mr. Cannon.

Chairman SENSENBRENNER. Without objection, the amendment is considered as read, and the gentleman from Utah is recognized for 5 minutes.

[The amendment follows:]

**AMENDMENT TO H.R. 338**  
**OFFERED BY MR. CANNON**

**(Page and line numbers refer to Subcommittee Amendment in  
the Nature of a Substitute)**

Page 1, line 10, strike “analysis” and insert “assessment”.

Page 1, line 11, strike “ANALYSIS” and insert “ASSESSMENT”.

Page 1, line 15, strike “any” and insert “a”.

Page 2, line 2, insert after “United States,” the following: “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,”.

Page 2, line 4, strike “analysis” and insert “assessment”.

Page 2, line 6, strike “analysis” and insert “assessment”.

Page 2, line 13, strike “analysis” and insert “assessment”.

Page 2, line 15, strike “assessment” and insert “analysis”.

Page 3, line 5,

Page 3, line 15, strike “ANALYSIS” and insert “ASSESSMENT”.

Page 3, line 21, insert after “United States,” the following: “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,”.

Page 3, line 22, strike “analysis” and insert “assessment”.

Page 4, line 2, strike “analysis” and insert “assessment”.

Page 4, line 4, strike “assessment” and insert “analysis”.

Page 4, line 25, strike “analysis” and insert “assessment”.

Page 5, line 1, strike “assessment” and insert “analysis”.

Page 5, lines 15–16, strike “analysis” and insert “assessment”.

Page 5, line 17, strike “analysis” and insert “assessment”.

Page 5, lines 19–20, strike “(c) PROCEDURE FOR WAIVER OR DELAY OF COMPLETION.—” and insert the following:

1 (c) WAIVERS.—

2 (1) EMERGENCIES.—

Page 5, after line 25, insert the following:

3 (2) NATIONAL SECURITY.—An agency head  
4 may, for national security reasons, or to protect  
5 from disclosure classified information, confidential  
6 commercial information, or information the disclo-  
7 sure of which may adversely affect a law enforce-  
8 ment effort, waive or delay the completion of some  
9 or all of the following requirements:

10 (A) The requirement of subsection (a)(1)  
11 to make an assessment available for public com-  
12 ment.

13 (B) The requirement of subsection (a)(1)  
14 to have an assessment or summary thereof pub-  
15 lished in the Federal Register.

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

Page 10, line 5, strike “analysis” and insert “assessment”.

Page 10, line 9, strike “analysis” and insert “assessment”.

Page 10, line 16, strike “analysis” and insert “assessment”.

Page 11, line 13, strike “analysis” both places such term appears and insert “assessment”.

Page 11, line 23, strike “analysis” and insert “assessment”.

Page 11, line 24, strike “analysis” and insert “assessment”.

Page 13, after line 14, strike “analysis” in the item relating to section 553a and insert “assessment”.

Mr. CANNON. Thank you, Mr. Chairman.

I believe my amendment is an excellent example of the benefits associated with the legislative process. Last February, as many of you know, my Subcommittee held an oversight hearing on the Department of Homeland Security's privacy officer, which, by the way, is the first statutorily-created privacy officer position in the Federal Government. As that hearing was immediately followed by the Subcommittee's markup of H.R. 338, several of the witnesses commented about the bill and offered suggestions for improving it.

My amendment is prepared largely in response to these suggestions and other sources. Basically, the amendment consists of revisions intended to make the bill conform with the E-Government Act of 2002. To that end, the amendment imports the Act's waiver provisions dealing with national security matters and other types of sensitive information.

Specifically, the amendment waives the requirement to make the privacy impact assessment publicly available or to publish such assessment in the Federal Register 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. This revision ensures that the legislation does not undermine foreign intelligence, antiterrorism or law enforcement activities.

The second revision imports standardized terminology from the E-Government Act, and the third revision simply clarifies that the measure applies only to rules pertaining to the collection, maintenance, use or disclosure of personally-identifiable information from at least 10 or more individuals. Accordingly, I urge my colleagues to support my amendment and reserve the balance of my time.

Chairman SENSENBRENNER. The gentleman has to yield back.

Mr. CANNON. I yield back.

Chairman SENSENBRENNER. The gentleman from Ohio, Mr. Chabot.

Mr. CHABOT. I 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 the full 5 minutes. I want to thank you for holding this important markup today, and I want to thank Mr. Cannon for offering this amendment and also for shepherding this bill through his Committee. I also want to thank especially my colleagues Mr. Nadler and also Mr. Boucher for their leadership and support on this very important privacy bill and the amendment.

The privacy legislation that we are considering today is necessary because Federal agencies too often promulgate rules and dictate policy without consideration for the ultimate ramifications on the privacy of the American people. As my colleague Mr. Nadler mentioned, privacy is not and should not be a partisan issue. It is a value, as he stated.

Republicans and Democrats, liberal or conservative, it is important to all of us. It's an intrinsic American value. We're here today because we've witnessed attempt after attempt by Federal agencies to implement sometimes ominous regulations that allow the Government to invade the privacy of American citizens. From financial information to medical records, the Federal Government has sought

access to highly sensitive information, oftentimes without regard to privacy implications.

The Defense of Privacy Act provides a straightforward solution to this problem. The legislation would, for the first time, require Federal agencies to assess the privacy implications of the proposed rules and regulations. Through this process, we would shine a light on the potentially negative impact of Government regulations on personal privacy, at the same time encouraging Federal agencies to more fully consider the merits of each proposal and review less intrusive alternatives.

Congress and the Administration must work to protect the privacy rights of law-abiding Americans, especially where the collection and dissemination of personally identifiable information is concerned. Passing this commonsense legislation and this amendment is a good first step, and requiring all Federal agencies to assess privacy implications of proposed rules and regulations will elevate the issue and generate important debate strengthening the rights of every American.

I urge my colleagues to support the amendment and also to support the underlying bill, and I yield back the balance of my time.

Chairman SENSENBRENNER. The question is on the amendment.

The gentleman from North Carolina, Mr. Watt.

Mr. WATT. Thank you, Mr. Chairman. I move to strike the last word.

Chairman SENSENBRENNER. The gentleman is recognized for 5 minutes.

Mr. WATT. I won't take 5 minutes. I just wanted to thank Mr. Cannon for narrowing this amendment to take into account some concerns we had about it in the Subcommittee and to encourage my colleagues to support the amendment and the underlying bill. I yield back.

Mr. CANNON. Would the gentleman yield for the purpose of just thanking the gentleman for working closely with us on this bill and to Mr. Chabot, who I talked about earlier but who has shown great leadership on this issue. We appreciate that, and thank you.

Mr. WATT. I yield back.

Chairman SENSENBRENNER. The question is on the amendment offered by the gentleman from Utah, Mr. Cannon.

Those in favor will say aye.

Opposed no.

The ayes appear to have it. The ayes have it. The amendment is agreed to.

Are there further amendments?

If there are no further amendments, without objection, the Subcommittee amendment in the nature of a substitute laid down as the base text as amended as adopted.

A reporting quorum is present. The question occurs on the motion to report the bill H.R. 338 favorably as amended.

All those in favor will say aye.

Opposed, no.

The ayes appear to have it. The ayes have it, and 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 Chairman is authorized to move to go to conference pursuant to House rules.

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

