AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PRIVACY AND CYBERCRIME ENFORCEMENT ACT OF 2007

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

ON

H.R. 4175

DECEMBER 18, 2007

Serial No. 110–128

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

39–708 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SANCHEZ, California
STEVE COHEN, Tennessee
HANK JOHNSON, Georgia
BETTY SUTTON, Ohio
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota

LAMAR SMITH, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

PERRY APELBAUM, *Staff Director and Chief Counsel*
JOSEPH GIBSON, *Minority Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

ROBERT C. "BOBBY" SCOTT, Virginia, *Chairman*

MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
JERROLD NADLER, New York
HANK JOHNSON, Georgia
ANTHONY D. WEINER, New York
SHEILA JACKSON LEE, Texas
ARTUR DAVIS, Alabama
TAMMY BALDWIN, Wisconsin
BETTY SUTTON, Ohio

LOUIE GOHMERT, Texas
J. RANDY FORGES, Virginia
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California

BOBBY VASSAR, *Chief Counsel*
MICHAEL VOLKOV, *Minority Counsel*

CONTENTS

DECEMBER 18, 2007

Page

TEXT OF THE BILL

H.R. 4175, the "Privacy and Cybercrime Enforcement Act of 2007" 3

OPENING STATEMENT

The Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security 1

The Honorable Louie Gohmert, a Representative in Congress from the State of Texas, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 13

WITNESSES

Mr. Andrew Lourie, acting Principal Deputy Assistant Attorney General and Chief of Staff to the Criminal Division, U.S. Department of Justice, Washington, DC

Oral Testimony 20

Prepared Statement 22

Mr. Craig Magaw, Special Agent, Criminal Investigative Division, U.S. Secret Service, U.S. Department of Homeland Security, Washington, DC

Oral Testimony 43

Prepared Statement 44

Mr. Joel Winston, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, Washington, DC

Oral Testimony 48

Prepared Statement 50

Ms. Jaimee Napp, Executive Director, Identity Theft Action Council of Nebraska, OMAHA, NE

Oral Testimony 71

Prepared Statement 72

Mr. Robert W. Holleyman, II, President and CEO, Business Software Alliance, Washington, DC

Oral Testimony 76

Prepared Statement 79

Ms. Lillie Coney, Associate Director, Electronic Privacy Information Center, Washington, DC

Oral Testimony 85

Prepared Statement 87

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Prepared Statement of the Honorable Louie Gohmert, a Representative in Congress from the State of Texas, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 14

Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Chairman, Committee on the Judiciary 16

Page

APPENDIX

Material Submitted for the Hearing Record 113

PRIVACY AND CYBERCRIME ENFORCEMENT ACT OF 2007

TUESDAY, DECEMBER 18, 2007

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 3 p.m., in room 2141, Rayburn House Office Building, the Honorable Robert C. "Bobby" Scott (Chairman of the Subcommittee) presiding.

Present: Representatives Scott, Jackson Lee, Gohmert, Coble, Chabot, Lungren and Conyers *(ex officio)*.

Staff Present: Bobby Vassar, Subcommittee Chief Counsel; Ameer Gopalani, Majority Counsel; Michael Volkov, Minority Counsel; and Veronica Eligan, Majority Professional Staff Member.

Mr. SCOTT. I am pleased to welcome you to the hearing of the Subcommittee on Crime, Terrorism, and Homeland Security on H.R. 4175, the "Privacy and Cybercrime Enforcement Act of 2007."

I would like to thank the Chairman of the full Committee, Mr. Conyers, for introducing the bill with bipartisan support. The bill was introduced at the time by the Chairman and Ranking Member of the Committee and the Subcommittee, and I am pleased to have been working with Mr. Conyers in drafting it to provide effective tools for Federal prosecutors and State and local law enforcement agencies to combat identity theft and other cybercrimes.

The Act takes several important steps to protect American consumers from the dangers of identity theft. First, our bill provides for the victims of identity theft, provides them with the ability to seek restitution in Federal court for the loss of time and money spent restoring their credit. Under current law, restitution to the victims is only available to recover the direct financial cost of identity theft offenses, such as recovering funds from unauthorized credit card charges.

But many identity theft victims incur other indirect costs, such as loss of wages due to time taken off from work to resolve credit disputes. Our bill amends the present law to make it clear that restitution orders may include an amount equal to the value of the victim's time spent addressing the actual or intended harm of the identity theft.

Second, the bill addresses urgent needs for agencies and companies to provide appropriate notification when they experience major breaches. The problem of data breaches remains a persistent and

dangerous threat to Americans' privacy. For example, in 2006, there was a disclosure that a company had suffered a major computer breach involving up to 45 million credit and debit card records. While the company knew about the breach, none of its customers were told about it until a month later. And we are all aware of the identity theft from 26 million of our veterans and active duty personnel from the Department of Veterans' Affairs last year.

Although up to 39 States have laws pertaining to data breaches, there is no Federal standard or regulation to provide notice. Our bill would require rapid notice of breaches to the FBI and Secret Service, and this notice is critical to the successful investigation and prosecution of any criminal activity associated with the breach. The FBI and Secret Service would then publish the list of reported breaches in the Federal Register so the public would be aware of where and to what extent major data breaches are occurring.

Finally, the bill makes it a crime punishable by up to 5 years in prison for knowingly failing to report major breaches to the appropriate authorities.

Lastly, this bill provides much needed tools to Federal and State law enforcement agents. The bill adds Section 1030 to the Computer Fraud and Abuse Act to the RICO statute which will provide the Department of Justice with a much-needed tool to investigate and prosecute organized crime syndicates which use sophisticated cyber schemes to commit criminal acts.

The bill also authorizes $25 million for each of the fiscal years from 2008 to 2010 to establish State grant programs with enforcement of cybercrimes. State and local law enforcement resources need to be strengthened to attack the low lying identity theft that Federal prosecutors fail to go after.

We heard the last Congress had a Subcommittee hearing about the incident involving Senator Dominici where some $800 in merchandise was charged to a stolen credit card. We found that the crime was not being prosecuted.

So thieves are left with the knowledge that if they don't steal too much, they can do so with impunity. The credit card company will cancel the debt, write off the loss, and there will be no criminal investigation, and so the thieves can keep the bounty of their crimes without worrying about prosecution.

I believe that the Secret Service working in partnership with State law enforcement could quickly reverse this expectation that thieves have in this front. H.R. 4175 is a comprehensive bill. It not only deals with the need to provide law enforcement notice to law enforcement when innocent consumers have their data briefed, it also deals with the underlying problems of lack of accountability to deter crimes from occurring in the first place.

Our privacy in cybercrimes lag behind both capabilities of our technology and the sophistication of identity thieves, and this legislation will close that gap.

[The text of the bill, H.R. 4175, follows:]

I

110TH CONGRESS
1ST SESSION

H. R. 4175

To amend title 18, United States Code, with respect to data privacy and security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 14, 2007

Mr. CONYERS (for himself, Mr. SMITH of Texas, Mr. SCOTT of Virginia, Mr. FORBES, Ms. LINDA T. SÁNCHEZ of California, Mr. DAVIS of Alabama, and Ms. JACKSON-LEE of Texas) introduced the following bill; which was referred to the Committee on the Judiciary

A BILL

To amend title 18, United States Code, with respect to data privacy and security, and for other purposes.

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

SECTION 1. SHORT TITLE.

(a) SHORT TITLE.—This Act may be cited as the "Privacy and Cybercrime Enforcement Act of 2007".

(b) TABLE OF CONTENTS.—The title of contents for this Act is as follows:

Sec. 1. Short title.

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

Sec. 101. Organized criminal activity.
Sec. 102. Failure to provide notice of security breaches involving sensitive personally identifiable information.
Sec. 103. Use of full interstate and foreign commerce power for criminal penalties.
Sec. 104. Cyber-extortion.
Sec. 105. Conspiracy to commit cyber-crimes.
Sec. 106. Penalties for section 1030 violations.
Sec. 107. Additional funding for resources to investigate and prosecute criminal activity involving computers.
Sec. 108. Criminal restitution.
Sec. 109. Review and amendment of Federal sentencing guidelines related to fraudulent access to or misuse of digitized or electronic personally identifiable information.

TITLE II—NON-CRIMINAL PRIVACY ENFORCEMENT AND PRIVACY IMPACT STATEMENTS

Sec. 201. Enforcement by Attorney General and State authorities.
Sec. 202. Coordination of State and Federal efforts.
Sec. 203. Requirement that agency rulemaking take into consideration impacts on individual privacy.

TITLE III—ASSISTANCE FOR STATE AND LOCAL LAW ENFORCEMENT TO COMBAT FRAUDULENT, UNAUTHORIZED, OR OTHER CRIMINAL USE OF PERSONALLY IDENTIFIABLE INFORMATION

Sec. 301. Grants for State and local law enforcement.
Sec. 302. Authorization of appropriations.

TITLE IV—NATIONAL WHITE COLLAR CRIME CENTER GRANTS

Sec. 401. Authorization and Expansion of National White Collar Crime Center.

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

SEC. 101. ORGANIZED CRIMINAL ACTIVITY.

Section 1961(1) of title 18, United States Code, is amended by inserting "section 1030 (relating to certain frauds and related activities in connection with computers)".

SEC. 102. FAILURE TO PROVIDE NOTICE OF SECURITY BREACHES INVOLVING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

"§ 1040. Failure to provide notice of security breaches involving sensitive personally identifiable information

"(a) Whoever, having a covered obligation to provide notice of a security breach involving sensitive personally identifiable information, knowingly fails to do so, shall be fined under this title or imprisoned not more than 5 years, or both.

"(b) As used in this section—

"(1) the term 'covered obligation', with respect to providing notice of a security breach, means an obligation under Federal law or, if the breach is in or affects interstate or foreign commerce, under State law;

"(2) the term 'sensitive personally identifiable information' means any electronic or digital information that includes—

"(A) an individual's first and last name, or first initial and last name, or address or phone number in combination with any 1 of the following data elements where the data elements are not protected by a technology protection measure that renders the data element indecipherable—

"(i) a nontruncated social security number, driver's license number, state resident identification number, passport number, or alien registration number;

"(ii) both of the following—

"(I) mother's maiden name, if identified as such; and

"(II) month, day, and year of birth; and

"(iii) unique biometric data such as a finger print, voice print, a retina or iris image; or

"(B) a financial account number or credit or debit card number in combination with any security code, access code or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction by means of such number;

"(3) the term 'security breach' means a compromise of the security, confidentiality, or integrity of computerized data that there is reason to believe has resulted in improper access to sensitive personally identifiable information; and

"(4) the term 'improper access' means access without authorization or in excess of authorization.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 47 of title 18, United States Code, is amended by adding at the end the following:

"1040. Concealment of security breaches involving personally identifiable information.".

(c) OBLIGATION TO REPORT.—

(1) IN GENERAL.—A person who owns or possesses data in electronic form containing a means of identification and has knowledge of a major security breach of the system containing such data maintained by such person, must provide prompt notice of such breach to the United States Secret Service or Federal Bureau of Investigation.

(2) PUBLICATION OF LIST OF NOTIFICATIONS.—The Secret Service and the Federal Bureau of Investigation shall annually publish in the Federal Register a list of all notifications submitted the previous calendar year and the identity of each entity with respect to which the major security breach occurred.

(3) DEFINITION.—In this subsection—

(A) the term "major security breach" means any security breach involving—

(i) means of identification pertaining to 10,000 or more individuals is, or is reasonably believed to have been acquired;

(ii) databases owned by the Federal Government; or

(iii) means of identification of Federal Government employees or contractors involved in national security matters or law enforcement; and

(B) the term "means of identification" has the meaning given that term in section 1028 of title 18, United States Code.

SEC. 103. USE OF FULL INTERSTATE AND FOREIGN COMMERCE POWER FOR CRIMINAL PENALTIES.

(a) BROADENING OF SCOPE.—Section 1030(e)(2)(B) of title 18, United States Code, is amended by inserting "or affecting" after "which is used in".

(b) ELIMINATION OF REQUIREMENT OF AN INTERSTATE OR FOREIGN COMMUNICATION FOR CERTAIN OFFENSES INVOLVING PROTECTED COMPUTERS.—Section 1030(a)(2)(C) of title 18, United States Code, is amended by striking "if the conduct involved an interstate or foreign communication".

SEC. 104. CYBER-EXTORTION.

Section 1030(a)(7) of title 18, United States Code, is amended by inserting ", or to access without authorization or exceed authorized access to a protected computer" after "cause damage to a protected computer".

SEC. 105. CONSPIRACY TO COMMIT CYBER-CRIMES.

Section 1030(b) of title 18, United States Code, is amended by inserting "or conspires" after "attempts".

SEC. 106. PENALTIES FOR SECTION 1030 VIOLATIONS.

Subsection (c) of section 1030 of title 18, United States Code, is amended to read as follows:

"(c)(1) The punishment for an offense under subsection (a) or (b) is a fine under this title or imprisonment for not more than 20 years, or both, but if the offender in the course of a violation of subsection (a)(5)(A)(i) knowingly or recklessly causes or attempts to cause death, such offender shall be fined under this title or imprisoned for any term of years or for life, or both.

"(2) The court, in imposing sentence for an offense under subsection (a) or (b), may, in addition to any other sentence imposed and irrespective of any provision of State law, order that the person forfeit to the United States—

"(A) the person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of the offense; and

"(B) any property, real or personal, constituting or derived from, any proceeds the person obtained, directly or indirectly, as a result of the offense.".

SEC. 107. ADDITIONAL FUNDING FOR RESOURCES TO INVESTIGATE AND PROSECUTE CRIMINAL ACTIVITY INVOLVING COMPUTERS.

(a) ADDITIONAL FUNDING FOR RESOURCES.—

(1) AUTHORIZATION.—In addition to amounts otherwise authorized for resources to investigate and prosecute criminal activity involving computers, there are authorized to be appropriated for each of the fiscal years 2008 through 2012—

(A) $10,000,000 to the Director of the United States Secret Service;

(B) $10,000,000 to the Attorney General for the Criminal Division of the Department of Justice; and

(C) $10,000,000 to the Director of the Federal Bureau of Investigation.

(2) AVAILABILITY.—Any amounts appropriated under paragraph (1) shall remain available until expended.

(b) USE OF ADDITIONAL FUNDING.—Funds made available under subsection (a) shall be used by the Director of the United States Secret Service, the Director of the Federal Bureau of Investigation, and the Attorney General, for the United States Secret Service, the Federal Bureau of Investigation, and the criminal division of the Department of Justice, respectively, to—

(1) hire and train law enforcement officers to—

(A) investigate crimes committed through the use of computers and other information technology, including through the use of the Internet; and

(B) assist in the prosecution of such crimes; and

(2) procure advanced tools of forensic science to investigate, prosecute, and study such crimes.

SEC. 108. CRIMINAL RESTITUTION.

Section 3663(b) of title 18, United States Code, is amended—

(1) by striking "and" at the end of paragraph (4);

(2) by striking the period at the end of paragraph (5) and inserting "; and" and

(3) by adding at the end the following:

"(6) in the case of an offense under section 1028(a)(7), 1028A(a), or 1030(a)(2), pay an amount equal to the value of the victim's time reasonably spent to remediate actual harm resulting from the offense.".

SEC. 109. REVIEW AND AMENDMENT OF FEDERAL SENTENCING GUIDELINES RELATED TO FRAUDULENT ACCESS TO OR MISUSE OF DIGITIZED OR ELECTRONIC PERSONALLY IDENTIFIABLE INFORMATION.

The United States Sentencing Commission, pursuant to its authority under section 994 of title 28, United States Code, and in accordance with this section, shall review and, if appropriate, amend the Federal sentencing guidelines (including its policy statements) applicable to persons convicted of using fraud to access, or misuse of, digitized or electronic personally identifiable information, including identity theft or any offense under—

(1) sections 1028, 1028A, 1030, 1030A, 2511, and 2701 of title 18, United States Code; and

(2) any other relevant provision.

TITLE II—NON-CRIMINAL PRIVACY ENFORCEMENT AND PRIVACY IMPACT STATEMENTS

SEC. 201. ENFORCEMENT BY ATTORNEY GENERAL AND STATE AUTHORITIES.

(a) DEFINITION OF "AUTHORIZED ENTITY".—As used in this section, the term "authorized entity" means the Attorney General, with respect to any conduct constituting a violation of a Federal law enacted after the date of the enactment of this Act relating to data security and engaged in by a business entity, and a State Attorney General with respect to that conduct to the extent the conduct adversely affects an interest of the residents of a State.

(b) CIVIL PENALTY.—

(1) GENERALLY.—An authorized entity may in a civil action obtain a civil penalty of not more than $500,000 from any business entity that engages in conduct constituting a violation of a Federal law enacted after the date of the enactment of this Act relating to data security.

(2) SPECIAL RULE FOR INTENTIONAL VIOLATION.—If the violation described in subsection (a) is intentional, the maximum civil penalty is $1,000,000.

(c) INJUNCTIVE RELIEF.—An authorized entity may, in a civil action against a business entity that has engaged, or is engaged, in any conduct constituting a violation of a Federal law enacted after the date of the enactment of this Act relating data security, obtain an order—

(1) enjoining such act or practice; or

(2) enforcing compliance with that law.

(d) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section do not affect any other rights and remedies available under Federal or State law.

SEC. 202. COORDINATION OF STATE AND FEDERAL EFFORTS.

(a) NOTICE.—

(1) IN GENERAL.—A State consumer protection attorney may not bring an action under section 201, until the attorney general of the State involved provides to the Attorney General of the United States—

(A) written notice of the action; and

(B) a copy of the complaint for the action.

(2) EXCEPTION.—Paragraph (1) does not apply with respect to the filing of an action by an attorney general of a State under this section if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action, in such a case the State attorney general shall provide notice and a copy of the complaint to the Attorney General at the time the State attorney general files the action.

(b) FEDERAL PROCEEDINGS.—The Attorney General may—

(1) move to stay any non Federal action under section 201, pending the final disposition of a pending Federal action under that section;

(2) initiate an action in an appropriate United States district court and move to consolidate all pending actions under section 201, including State actions, in that court; and

(3) intervene in a State action under section 201.

(c) PENDING PROCEEDINGS.—If the Attorney General institutes a proceeding or action for a violation of a Federal law enacted after the date of the enactment of this Act relating data security, no authority of a State may, during the pendency of such proceeding or action, bring an action under this section against any defendant named in such criminal proceeding or a civil action against any defendant for any violation that is alleged in that proceeding or action.

(d) DEFINITION.—As used in this section, the term "State consumer protection attorney" means the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law.

SEC. 203. REQUIREMENT THAT AGENCY RULEMAKING TAKE INTO CONSIDERATION IMPACTS ON INDIVIDUAL PRIVACY.

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

"§ 553a. Privacy impact assessment in rulemaking

"(a) INITIAL PRIVACY IMPACT ASSESSMENT.—

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

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

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

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

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

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

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

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

"(b) FINAL PRIVACY IMPACT ASSESSMENT.—

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

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

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

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

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

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

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

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

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

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

"(c) WAIVERS.—

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

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

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

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

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

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

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

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

"(3) the direct notification of interested individuals;

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

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

"(e) PERIODIC REVIEW OF RULES.—

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

"(A) The continued need for the rule.

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

"(C) The complexity of the rule.

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

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

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

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

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

"(f) JUDICIAL REVIEW.—

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

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

"(3) LIMITATIONS.—

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

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

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

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

"(4) RELIEF.—In granting any relief in an action under this subsection, the court shall order the agency to take corrective action consistent with this section and chapter 7, and may—

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

"(B) defer 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 limits the authority of any court to stay the effective date of any rule or provision thereof under any other provision of law or to grant any other relief in addition to the requirements of this subsection.

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

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

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

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

(b) PERIODIC REVIEW TRANSITION PROVISIONS.—

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

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

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

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

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

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

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

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

TITLE III—ASSISTANCE FOR STATE AND LOCAL LAW ENFORCEMENT TO COMBAT FRAUDULENT, UNAUTHORIZED, OR OTHER CRIMINAL USE OF PERSONALLY IDENTIFIABLE INFORMATION

SEC. 301. GRANTS FOR STATE AND LOCAL LAW ENFORCEMENT.

(a) IN GENERAL.—Subject to the availability of amounts provided in advance in appropriations Acts, the Assistant Attorney General for the Office of Justice Programs of the Department of Justice may award grants to States to establish and develop programs to increase and enhance enforcement against crimes related to fraudulent, unauthorized, or other criminal use of personally identifiable information.

(b) APPLICATION.—To be eligible for a grant under subsection (a), a State shall submit an application to the Assistant Attorney General for the Office of Justice

Programs of the Department of Justice at such time, in such manner, and containing such information, including as described in subsection (d), as the Assistant Attorney General may require.

(c) USE OF GRANT AMOUNTS.—A grant awarded to a State under subsection (a) shall be used by a State, in conjunction with units of local government within that State, State and local courts, other States, or combinations thereof, to establish and develop programs to—

(1) assist State and local law enforcement agencies in enforcing State and local criminal laws relating to crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information;

(2) assist State and local law enforcement agencies in educating the public to prevent and identify crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information;

(3) educate and train State and local law enforcement officers and prosecutors to conduct investigations and forensic analyses of evidence and prosecutions of crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information;

(4) assist State and local law enforcement officers and prosecutors in acquiring computer and other equipment to conduct investigations and forensic analysis of evidence of crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information; and

(5) facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information with State and local law enforcement officers and prosecutors, including the use of multi-jurisdictional task forces.

(d) ASSURANCES AND ELIGIBILITY.—To be eligible to receive a grant under subsection (a), a State shall provide assurances to the Attorney General that the State—

(1) has in effect laws that penalize crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information, such as penal laws prohibiting—

(A) fraudulent schemes executed to obtain personally identifiable information;

(B) schemes executed to sell or use fraudulently obtained personally identifiable information; and

(C) online sales of personally identifiable information obtained fraudulently or by other illegal means;

(2) will provide an assessment of the resource needs of the State and units of local government within that State, including criminal justice resources being devoted to the investigation and enforcement of laws related to crimes involving the fraudulent, unauthorized, or other criminal use of personally identifiable information;

(3) will develop a plan for coordinating the programs funded under this section with other federally funded technical assistant and training programs, including directly funded local programs such as the Local Law Enforcement Block Grant program (described under the heading "Violent Crime Reduction Programs, State and Local Law Enforcement Assistance" of the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 1998 (Public Law 105–119)); and

(4) will submit to the Assistant Attorney General for the Office of Justice Programs of the Department of Justice applicable reports in accordance with subsection (f).

(e) MATCHING FUNDS.—The Federal share of a grant received under this section may not exceed 90 percent of the total cost of a program or proposal funded under this section unless the Attorney General waives, wholly or in part, the requirements of this subsection.

(f) REPORTS.—For each year that a State receives a grant under subsection (a) for a program, the State shall submit to the Assistant Attorney General for the Office of Justice Programs of the Department of Justice a report on the results, including the effectiveness, of such program during such year.

SEC. 302. AUTHORIZATION OF APPROPRIATIONS.

(a) IN GENERAL.—There is authorized to be appropriated to carry out this title $25,000,000 for each of fiscal years 2008 through 2010.

(b) LIMITATIONS.—Of the amount made available to carry out this title in any fiscal year not more than 3 percent may be used by the Attorney General for salaries and administrative expenses.

(c) MINIMUM AMOUNT.—Unless all eligible applications submitted by a State or units of local government within a State for a grant under this title have been funded, the State, together with grantees within the State (other than Indian tribes), shall be allocated in each fiscal year under this title not less than 0.75 percent of the total amount appropriated in the fiscal year for grants pursuant to this title, except that the United States Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands each shall be allocated 0.25 percent.

(d) GRANTS TO INDIAN TRIBES.—Notwithstanding any other provision of this title, the Attorney General may use amounts made available under this title to make grants to Indian tribes for use in accordance with this title.

TITLE IV—NATIONAL WHITE COLLAR CRIME CENTER GRANTS

SEC. 401. AUTHORIZATION AND EXPANSION OF NATIONAL WHITE COLLAR CRIME CENTER.

(a) IN GENERAL.—Title I of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3711 et seq.) is amended—

(1) by redesignating part X, as added by section 623 of Public Law 109–248, as part JJ; and

(2) by adding at the end the following new part:

"PART KK—NATIONAL WHITE COLLAR CRIME CENTER GRANTS

"SEC. 3021. ESTABLISHMENT OF GRANTS PROGRAM.

"(a) AUTHORIZATION.—The Director of the Bureau of Justice Assistance is authorized to make grants and enter into contracts with State and local criminal justice agencies and nonprofit organizations for the purpose of improving the identification, investigation, and prosecution of certain criminal activities.

"(b) CERTAIN CRIMINAL ACTIVITIES DEFINED.—For purposes of this part, the term 'certain criminal activity' means a criminal conspiracy or activity or a terrorist conspiracy or activity that spans jurisdictional boundaries, including the following:

"(1) Terrorism.

"(2) Economic crime.

"(3) High-tech crime, also known as cyber crime or computer crime, including internet-based crime against children and child pornography.

"(c) CRIMINAL JUSTICE AGENCY DEFINED.—For purposes of this part, the term 'criminal justice agency', with respect to a State or a unit of local government within such State, includes a law enforcement agency, a State regulatory body with criminal investigative authority, and a State or local prosecution office to the extent that such agency, body, or office, respectively, is involved in the prevention, investigation, and prosecution of certain criminal activities.

"SEC. 3022. AUTHORIZED PROGRAMS.

"Grants and contracts awarded under this part may be made only for the following programs, with respect to the prevention, investigation, and prosecution of certain criminal activities:

"(1) Programs to provide a nationwide support system for State and local criminal justice agencies.

"(2) Programs to assist State and local criminal justice agencies to develop, establish, and maintain intelligence-focused policing strategies and related information sharing.

"(3) Programs to provide training and investigative support services to State and local criminal justice agencies to provide such agencies with skills and resources needed to investigate and prosecute such criminal activities and related criminal activities.

"(4) Programs to provide research support, to establish partnerships, and to provide other resources to aid State and local criminal justice agencies to prevent, investigate, and prosecute such criminal activities and related problems.

"(5) Programs to provide information and research to the general public to facilitate the prevention of such criminal activities.

"(6) Programs to establish National training and research centers regionally, including within Virginia, Texas, and Michigan, to provide training and research services for State and local criminal justice agencies.

"(7) Any other programs specified by the Attorney General as furthering the purposes of this part.

"SEC. 3023. APPLICATION.

"To be eligible for an award of a grant or contract under this part, an entity shall submit to the Director of the Bureau of Justice Assistance an application in such form and manner, and containing such information, as required by the Director.

"SEC. 3024. RULES AND REGULATIONS.

"Not later than 180 days after the date of the enactment of this part, the Director of the Bureau of Justice Assistance shall promulgate such rules and regulations as are necessary to carry out the this part, including rules and regulations for submitting and reviewing applications under section 3023.".

(b) AUTHORIZATION OF APPROPRIATION.—Section 1001(a) of such Act (42 U.S.C. 3793) is amended by adding at the end the following new paragraph:

"(26) There is authorized to be appropriated to carry out part KK—

"(A) $25,000,000 for fiscal year 2008;

"(B) $28,000,000 for fiscal year 2009;

"(C) $31,000,000 for fiscal year 2010;

"(D) $34,000,000 for fiscal year 2011;

"(E) $37,000,000 for fiscal year 2012; and

"(F) $40,000,000 for fiscal year 2013.".

○

Mr. SCOTT. It is now my pleasure to recognize our new Ranking Member of the Subcommittee, the gentleman from Texas, Judge Gohmert.

Mr. GOHMERT. Thank you, Chairman Scott. Thank you to the witnesses. I stayed until 1:30, when it was apparent we were going to be a while, and I ran over to the Capitol, but because the hour is so much later, I have an opening statement, but I would ask unanimous consent simply to submit it for the record. Unless you all want me to read my opening statement, I will. But otherwise, we will submit that.

H.R. 4175 was introduced by Chairman Conyers, Ranking Member Smith, Subcommittee Member Scott and then-Ranking Member Forbes. A bipartisan proposal, I think, represents a good first step in tackling the difficult problem of identity theft and cybercrime.

And so I will look forward to hearing the witnesses and working with my colleagues on this important piece of legislation.

And with that, I guess hearing no objection——

Mr. SCOTT. Without objection, the statement is entered into the record.

[The prepared statement of Mr. Gohmert follows:]

PREPARED STATEMENT OF THE HONORABLE LOUIE GOHMERT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS, AND RANKING MEMBER, SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

Statement of Ranking Member Louie Gohmert

Subcommittee on Crime, Terrorism, and Homeland Security

Legislative Hearing on H.R. 4175, the Cyber-Security Enhancement and Consumer Data Protection Act of 2006

December 18, 2007

Thank you Chairman Scott. I want to thank you for holding this hearing on H.R. 4175, the Privacy and Cybercrime Enforcement Act of 2007.

Advanced technologies, combined with the realties of the post-9/11 digital era, have created strong incentives and opportunities for the collection and selling of personal information about ordinary Americans. Today, private sector and governmental entities alike routinely traffic in billions of electronic personal records about Americans. Americans rely on this data to facilitate financial transactions, provide services, prevent fraud, screen employees, investigate crimes, and find loved ones. The government also relies upon this information to enhance national security and to combat crime.

The growing market for personal information has also become a treasure trove that is both valuable and vulnerable to identity thieves. As a result, the consequences of a data security breach can be quite serious. For Americans caught up in the endless cycle of watching their credit unravel, undoing the damage caused by security breaches and identity theft can become a time-consuming and life-long endeavor. In addition, while identity theft is a major privacy concern for most Americans, the use and collection of personal data by government agencies can have an even greater impact on Americans' privacy.

According to the Privacy Rights Clearinghouse, more than 150 million records containing sensitive personal information have been involved in data security breaches since 2005. The steady wave of data security breaches in recent years is a window into a broader, more challenging trend. Insecure databases are now low-hanging fruit for hackers looking to steal identities and commit fraud. The current estimates of the incidence of identity theft in the United States vary, but they are all disturbingly high.

According to a recent report on identity theft by the Federal Trade Commission, annual monetary losses due to identity theft are in the billions of dollars. In fact, American consumers collectively spend billions of dollars to recover from the effects of identity theft, according to the FTC.

The Internet revolutionized our society in many ways. While the Internet's benefits have been significant, criminals in the United States and abroad have unfortunately been able to exploit the internet to further new and sophisticated criminal schemes. Cybercrime often is faceless and has proven to defy traditional investigative and prosecutorial tools. As a result, the scope and frequency of cybercrime is growing rapidly and now includes many international criminal syndicates, and is threatening our economy, safety and prosperity.

H.R. 4175 was introduced by Chairman Conyers, Ranking Member Smith, and Subcommittee Chairman Scott and then-Ranking Member Forbes. This bi-partisan proposal represents a good first step in tackling the difficult problem of identity theft and cybercrime. The purpose of this hearing is to hear from interested parties as to specific provisions in the bill. I look forward to hearing from the witnesses and also working with my colleagues on this piece of legislation.

Mr. SCOTT. The gentleman from Michigan.

Mr. CONYERS. Thank you. And as the one that is guilty for holding you up so long, I won't—I will not give you my statement, and I will put it in the record and add that the privacy in the Cybercrime Enforcement Act is a strong bipartisan measure that I believe will help combat the growing threat of identity theft and other cybercrimes. This balanced bill protects the privacy rights of consumers, the interest of businesses and the legitimate needs of law enforcement.

And I would like to emphasize that I look forward to the passage of a crime law but not at the expense of the substantive issues involved, including requiring much needed notices for security breaches.

I am aware of the passage of S. 2168 in the Senate, but our bill is more comprehensive, and we need to examine it before making hasty decisions that impact consumers for years to come.

Thank you very much, Mr. Chairman, for your patience and forbearance.

[The prepared statement of Chairman Conyers follows:]

PREPARED STATEMENT OF THE HONORABLE JOHN CONYERS, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN, AND CHAIRMAN, COMMITTEE ON THE JUDICIARY

Statement of the Honorable John Conyers, Jr.
for the Hearing on H.R. 4175, the "Privacy and Cybercrime Enforcement Act of 2007"
Before the Subcommittee on Crime, Terrorism, and Homeland Security

Tuesday, December 18, 2007, at 1:00 p.m.
2141 Rayburn House Office Building

H.R. 4175, the "Privacy and Cybercrime Enforcement Act," helps to protect Americans from the growing and evolving crime of identity theft as well as other types of cyber crimes in several critical respects.

First, it allows victims of identity theft to seek restitution in federal court for the loss of time and money spent restoring their credit and remedying the harms caused by this crime. The bill ensures that identity theft victims will be made whole financially. As we know when the Department of Veterans Affairs lost the personal information of 26.5 million veterans, victims of identify theft should not be punished for the failures of our government to protect their information.

Second, H.R. 4175 updates the criminal laws with respect to identity theft schemes so that they reflect current technologies and better respond to the sophisticated aspects of these crimes.

For example, to address the increasing number of computer hacking crimes that involve computers located within the same state, the bill eliminates the jurisdictional requirement that a computer's information must be stolen through an interstate or foreign communication in order for the crime to be federally prosecuted.

Lastly, H.R. 4175 strengthens consumer privacy in several respects. It requires companies to give timely notice of any breaches to law enforcement and makes it a crime punishable by up to five years in prison to knowingly fail to report such breaches to the appropriate authorities. The bill also 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. With limited exception, such assessments must be made available to the public for comment. This provision results from our work on this issue as far back as March of 2005, when in response to the Choicepoint incident, I requested, along with former Chairman Sensenbrenner, that the GAO review the "legality of data acquisition, verification, and security procedures" in government agencies. The GAO prepared a lengthy report finding that agencies did not appropriately inform the public where and how the collection of personal information is taking

place.

The Privacy and Cybercrime Enforcement Act is a strong, bipartisan measure that will help combat the growing threat of identity theft and other cyber-crimes. This balanced bill protects the privacy rights of consumers, the interests of businesses, and the legitimate needs of law enforcement. I would like to emphasize that I look forward to passage of cybercrime law, but not at the expense of the substantive issues involved, including requiring much needed notices for security breaches. I am aware of the passage of S.2168 in the Senate, but our bill is more comprehensive and we need to examine it before making haste decisions that impact consumers for years to come.

In closing, I want to thank the bipartisan coalition of Representatives who have joined me in cosponsoring this important legislation along with House Judiciary Committee Ranking Member Lamar Smith, Crime Subcommittee Chairman Bobby Scott, and Ranking Member Randy Forbes. My fellow cosponsors have been valuable partners in working to combat the growing problem of identity theft for many years. H.R. 4175 is the result of our collaboration, a bill that provides new and effective tools to combat identity theft and other computer crimes.

Mr. SCOTT. Thank you, Mr. Chairman.

The gentleman from North Carolina.

Mr. COBLE. In view of the belated hour, I waive my opening statement and join you in welcoming our panel.

Mr. SCOTT. And without objection, other Members will be allowed to include opening statements in the record at this point.

I want to thank the witnesses for your patience. Sometimes because of votes and things, the schedule just goes array, and we appreciate your patience in remaining with us.

We have a distinguished panel of witnesses here today to help us consider important issues that are here before us.

The first witness is Andrew Lourie, who was the acting Principal Deputy Assistant Attorney General and chief of staff of the Criminal Division at the Department of Justice. He is currently serving a detail from the U.S. Attorney's Office from the Southern District of Florida where, for the past 5 years, he has served as Managing Assistant U.S. Attorney in the West Palm Beach office. He served two prior details at the Department, both as chief of the Public Integrity Section.

The next witness is Greg Magaw, a special agent in charge of the United States Secret Service. He provides guidance in determining the investigative focus of the division which provides direction to all Secret Service field offices. He is a 20-year veteran of the Secret Service, native of Columbus, Ohio. He received his Bachelor of Arts degree from the University of Maryland and masters degree in the field of management from Johns Hopkins.

Next will be Joel Winton, the associate director of the Division of Privacy and Identity Protection at the Federal Trade Commission's Bureau of Consumer Protection. That division has responsibility over consumer privacy and data security issues, identity theft and credit reporting matters. Mr. Winston is currently serving on the Federal Government's Identity Theft Task Force, which was created by the President in March 2006. Mr. Winston received his undergraduate and law degrees from the University of Michigan.

Next will be Jaimee Napp, executive director of the Identity Theft Action Council of Nebraska. He founded the council in 2006—excuse me, she founded the council in 2006 to use her journey as an identity theft victim to help others. The council is the first nonprofit organization dedicated solely to identity theft issues assisting victims in Nebraska. She received her bachelors of journalism from the University of Nebraska at Lincoln.

Next will be Robert Holleyman, president, CEO, of the Business Software Alliance. Mr. Holleyman has headed the alliance since 1990, overseeing operations in more than 85 countries. He is widely known for his work on policy related issues affecting the technology industry, including intellectual property laws, cyber security, international trade and electronic commerce. He earned his bachelor of arts degree in Political Science at Trinity University in Texas and his juris doctorate from Louisiana State University in Baton Rouge.

Finally, we have Lillie Coney, associate director of the Electronic Privacy Information Center in Washington, D.C. She serves as the coordinator for the Privacy Coalition. The Privacy Coalition has over 40 organizations and affiliates who share a commitment to freedom and privacy rights. She has testified before the Depart-

ment of Homeland Security, the Department of Homeland Security's Data Privacy and Integrity Advisory Committee, on domestic surveillance.

Now each of our witnesses' written statements will be made part of the record and all of those statements in their entirety. I would ask each witness to summarize his or her testimony in 5 minutes or less. And to help you stay within that time, there is a timing device on your table that will start green and go to yellow when you have 1 minute left and then finally to red when your time has expired.

We will begin with—and unfortunately, we are expecting a vote any minute now so we will go as far as we can, break for a vote and then come right back.

Mr. Lourie.

TESTIMONY OF ANDREW LOURIE, ACTING PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL AND CHIEF OF STAFF TO THE CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. LOURIE. Thank you. Good afternoon, Chairman Scott, Ranking Member Gohmert and Members of the Subcommittee.

It is a pleasure to appear before you today to testify about the Department of Justice's commitment to combatting computer crime and identity theft, and about the important legislation this Subcommittee is considering to address these threats.

As information technology increasingly pervades every aspect of our society, the opportunity for criminals to take advantage of it was also increased.

One result has been the rise of identity theft. The Department of Justice is dedicated to aggressively pursuing all forms of cybercrime and identity theft. However, shortcomings in existing law have, at times, inhibited its ability to do so. The Privacy and Cyber Crime Act of 2007 would address several of these shortcomings and provide important tools to promote law enforcement's efforts.

The act includes many provisions also recommended in the strategic plan released earlier this year by the President's Identity Theft Task Force. The Department is pleased to see the depth of the common ground that we share in these key issues. In particular, the Department applauds the amendments in the act that would ensure that victims receive fair restitution for the time spent to remediate the harm resulting from identity theft offenses.

Similarly, the Department supports the provisions of the act that enhance our ability to prosecute the theft of sensitive information from computers, close loopholes in the cyber extortion statute and enable us to bring computer crime charges against criminal conspiracies and organized criminal groups.

In addition to these many positive aspects, the Department would like to provide some suggestions that would strengthen the bill.

First, we strongly encourage the Committee to consider amending 18 USC, section 1030(a)(5), to close a loophole and appropriately penalize the use of malicious spyware, botnets and keyloggers. Current law criminalizes actions that cause damage to

computers by impairing the integrity or ability of data or computer systems. Absent special circumstances, however, the conduct must cause loss exceeding $5,000 to constitute a Federal crime. Many identity thieves obtain personal information by installing malicious software on numerous individual computers. Whether or not the programs succeed in stealing information, they harm the integrity of the computer and data. However, it is often difficult or impossible to measure the loss to each computer owner or to prove that the many small losses together exceed $5,000.

Two amendments could remedy this situation. First, Congress could amend section 1030(a)(5) to make it a misdemeanor offense to damage a protected computer and cause less than $5,000 in loss. Whether or not the Committee considers that amendment, we strongly recommend adding a provision to the act that would make it a Federal felony to damage 10 or more protected computers regardless of loss.

Let me turn now to Section 102 of the bill, the provision that requires victims of major executive breaches to provide notice to law enforcement. The bill defines a major security breach as a breach that involves the means of identification pertaining to 10,000 or more individuals. This threshold is too high. To give the numbers some context, the theft of as few as 1,000 credit card numbers is, under the current sentencing guidelines, presumed to involve a minimum loss of $500,000. We therefore recommend that the threshold for major security breach be reduced.

The definition should also be amended to include any breach where there may be a threat to national security or risk of significant monetary loss without regard to the number of records affected.

I would also like to mention Section 106, which contains a useful provision on the forfeiture of the instrumentalities and proceeds of cybercrime. We support the addition of a forfeiture provision. We suggest, however, that the act explicitly allow for both civil and criminal forfeiture and spell out the appropriate procedures. Language to accomplish these changes and other technical suggestions to improve the forfeiture procedures is included with the written testimony I have submitted to the Subcommittee.

In conclusion, the Department would like to emphasize that law enforcement can continue to fulfill its role in addressing the growing threats of computer crime and identify theft if we have the appropriate laws and appropriate resources. The Privacy in Cyber Crime Act of 2007 addresses many of those needs by closing loopholes in existing cybercrime statutes, improving our ability to prosecute criminal groups and providing much needed resources. We believe the act will be an important tool in the fight against cybercrime.

Mr. Chairman, this concludes my remarks.

[The prepared statement of Mr. Lourie follows:]

PREPARED STATEMENT OF ANDREW LOURIE

Statement of

Andrew Lourie

Acting Principal Deputy Assistant Attorney General
and Chief of Staff
Criminal Division
United States Department of Justice

Before the Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
United States House of Representatives

December 18, 2007

Good morning, Chairman Scott and Ranking Member Gohmert. It is a pleasure to appear before you today to testify about the Department of Justice's commitment to combating computer crime and identity theft, and about the important legislation this Committee is considering to address these crime threats.

I. THE THREAT OF COMPUTER CRIME AND IDENTITY THEFT

As information technology increasingly pervades every aspect of our society, the opportunities for criminals to take advantage of it has commensurately increased. One of the most significant harms of this criminal exploitation of computers and computer networks has been the rise of identity theft. Identity theft is pervasive throughout the United States and around the world. Every day criminals hunt for our personal and financial data so that they can use the data to commit fraud or sell the data to other criminals.

As the President's Identity Theft Task Force recently stated in its Strategic Plan, identity theft "exacts a serious toll on the American public," with annual monetary losses "in the billions of dollars."[1] The harm of identity theft, however, extends well beyond direct financial losses to victims. Businesses must bear indirect costs of fraud prevention and mitigation of the harm once it has occurred, individual victims often suffer indirect financial costs (such as costs incurred in civil litigation by creditors), and some victims spend substantial amounts of time to repair the damage that the identity thieves caused.

Furthermore, many identity-theft victims report that they must bear the uncertainty of whether and how an identity thief will cause new problems for them. As one victim put it, in connection with the recent sentencing of an identity thief,

> I am constantly wondering when I will be attacked again. I have no way of knowing who else [the defendant] has distributed my personal information to . . . . It would have been better to have been mugged at gunpoint, since at least then I would have my peace of mind knowing that it was a one-time event.[2]

Today, criminals are able to obtain personal information nearly everywhere it is located or stored. Hackers have developed tools to penetrate firewalls, use automated processes to search for account data or other personal information, export the data, and hide their tracks. According to the Secret Service, many major breaches in credit card systems in 2006 originated outside the United States, and criminals operating in those two countries have been directly involved in some of the largest breaches of U.S. financial systems over the past five years.[3]

---

[1] PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN at 11 (April 2007), *available at* http://www.idtheft.gov/.
[2] *See* United States Attorney's Office, Western District of Washington, Press Release (May 4, 2007), *available at* http://seattle.fbi.gov/dojpressrel/2007/pr050407.htm.
[3] PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra*, at 15.

"Phishing" is another prevalent attack that has caused massive losses to consumers and businesses. Phishers send emails that appear to be coming from legitimate, well-known sources – often, financial institutions or government agencies – effectively stealing the identities of these entities. In one example, these email messages tell recipients to verify personal information or risk cancellation of their accounts. The emails provide a website to enter the information, but when the user clicks on the link, it leads to a web site that appears legitimate but is in fact controlled by the phishers. The user then enters personal identifying information, such as name, address, account number, PIN, and social security number. Phishers harvest this information and use it to commit fraud or sell it to other criminals.

The Strategic Plan of the President's Identity Theft Task Force provides considerable detail about the many ways that criminals perpetrate identity theft and about the ways in which the Federal Government can address this growing threat. The Identity Theft Task Force, which the President established in May 2006, was charged with producing a coordinated strategic plan to further improve the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution. Released in April, 2007, this comprehensive strategy focuses on improvements in four key areas: (1) keeping sensitive consumer data out of the hands of identity thieves through better data security and more accessible education; (2) making it more difficult for identity thieves who obtain consumer data to use it to steal identities; (3) assisting the victims of identity theft in recovering from the crime; and (4) deterring identity theft by more aggressive prosecution and punishment of those who commit the crime. These themes are consonant with the legislation that the Committee is currently considering. The Department was pleased to recognize how much common ground we share and would commend the Strategic Plan to the members of this committee as an invaluable resource.

II. THE ROLE OF LAW ENFORCEMENT

A. Collecting Information and Receiving Complaints

Currently, federal law enforcement has a number of sources of information about cybercrime and identity theft. For example, the FBI and the National White Collar Crime Center (NWC3) have developed an online complaint mechanism for citizens to report internet-related fraud and other crimes. The Internet Crime Complaint Center (IC3) provides an easy way for computer users across the country and around the world to make these reports. The IC3 currently receives more than 20,000 complaints per month from victims of online crime. Moreover, it provides an important means of analyzing these reports and disseminating that information as case leads to the right law enforcement agency.

In addition, in order to respond to the challenges of multinational Internet fraud, and to enhance consumer protection and consumer confidence in e-commerce, thirteen countries instituted *econsumer.gov,* a joint effort to gather and share cross-border e-commerce complaints. The project has two components: a multilingual public Web site, and a government, password-protected Web site. The public site provides general information about consumer protection in all countries that belong to the ICPEN (International Consumer Protection Enforcement Network), contact information for consumer protection authorities in those countries, and an online complaint form. All information is available in English, French, German, and Spanish. Using the existing Consumer Sentinel network (a database of consumer complaint data and other investigative information operated by the U.S. Federal Trade Commission), the incoming complaints are shared with participating law enforcement agencies, such as the FBI.

B. Promoting Public/Private Partnerships

Private sector entities – including the financial services industry and credit reporting agencies – also are important sources of information for law enforcement agencies. They often are best positioned to identify anomalies that are indicative of identity theft and generally are the first to become aware of intrusions into their computer networks. For this reason and others, federal law enforcement has undertaken numerous public- and private-sector collaborations in recent years to improve information sharing.

For example, corporations have placed analysts and investigators with the IC3 to support its initiatives and investigations. The IC3 has also spun off an organization known as the Cyber Initiative and Resource Fusion Unit (CIRFU). The CIRFU combines resources from law enforcement with those of critical industry partners to identify trends in internet crime, develop enforcement initiatives, and alert consumers to problems, including identity theft scams.

In addition, the United States Secret Service leads Electronic Crimes Task Forces that focus on computer- and identity theft-related crimes. Inaugurated in 2001, the twenty-four task forces include industry and other private sector members. They provide an important forum for the sharing of threat and trend information and for the reporting of cybercrimes.

Finally, InfraGard is a national information sharing network between the FBI and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants. Its goals include increasing the level of information sharing and reporting between InfraGard members and the FBI on a variety of cybercrime matters, including identity theft.

C. Prosecuting Computer Crime and Identity Theft

For some time, the Department of Justice has been deeply committed to aggressively pursuing all forms of cybercrime and identity theft. Through interagency task forces and individual investigations, federal prosecutors have been prosecuting significant cases of identity theft. The following are examples of these prosecutions across the country:

> ***Virginia:*** On February 9, 2007, in the Eastern District of Virginia, a defendant was sentenced to 94 months in federal prison for aggravated identity theft, access device fraud, and conspiracy to commit bank fraud. The defendant, who went by the Internet nickname "John Dillinger," was involved in extensive illegal online "carding" activities. He received e-mails or instant messages containing hundreds of stolen credit card numbers – usually obtained through phishing schemes or network intrusions – from "vendors" located in Russia and Romania. In his role as a "cashier" of these stolen credit card numbers, the defendant would electronically encode these numbers onto plastic bank cards, make ATM withdrawals, and return a portion to the vendors. Computers seized from the defendant revealed more than 4,300 compromised account numbers and full identity information (i.e., name, address, date of birth, social security number, mother's maiden name, etc.) for over 1,600 individual victims.[10]

> ***California:*** On January 16, 2007, in the Central District of California, a defendant was convicted of violating the CAN-SPAM Act of 2003, as well as other counts including aggravated identity theft and wire fraud. The defendant

[10] *See* U.S. Attorney's Office, Eastern District of Virginia, Press Release (February 9, 2007), *available at* http://www.usdoj.gov/usao/vae/Pressreleases/02-FebruaryPDFArchive/07/20070209robertsnr.pdf

operated a sophisticated "phishing" scheme in which he sent thousands of e-mails to America Online users that appeared to be from AOL's billing department. His e-mails urged AOL customers to "update" their AOL billing information or lose service and referred customers to one of several web pages, where they could input their personal and credit information. The defendant actually controlled those webpages. Using information he collected from the AOL customers, he then made unauthorized charges on the AOL customers' credit or debit cards. On June 14, 2007, the defendant was sentenced to six years in prison and ordered to pay over $1 million in restitution to his victims.[12]

Washington: On August 25, 2007, in the Western District of Washington, a man was sentenced to 37 months in prison for creating a botnet – a network of compromised computers that he could control – and using it to commit over $100,000 in fraud. In addition to this harm, however, the malicious code used to create the botnet caused damage to many computers across the Internet. These disruptions affected a Seattle hospital's computer systems in serious ways: doors to the operating rooms did not open, pagers did not work, and computers in the intensive care unit shut down. Luckily, no one was hurt because the hospital was able to switch to back up systems. The defendant accepted responsibility for over $250,000 worth of damage.[4]

In addition, a number of U.S. investigations have resulted in successful prosecutions in foreign countries. For example, based on close cooperation between the

---

[12] *See* U.S. Attorney's Office, Central District of California, Press Release (January 16, 2007), *available at* http://www.usdoj.gov/usao/cac/news/pr2007/079.html

[4] *See* U.S. Attorney's Office, Western District of Washington, Press Release (August 25, 2006), *available at* http://www.usdoj.gov/usao/waw/press/2006/aug/maxwell.html.

Department, the FBI legal attaché, and Romanian authorities, Prosecutors from the Romanian Directorate for Investigating Organized Crime and Terrorism arrested 9 Romanian citizens on fraud and identity theft charges on November 13, 2007. These Romanians were part of a criminal organization that specialized in "phishing" information from computer users, imprinting credit and debit card information onto counterfeit cards, and obtaining cash from ATM machines and Western Union locations. Romanian police officers executed 21 simultaneous search warrants and seized computers, card reading and writing devices, blank cards, and other equipment. Initial loss estimates total more that $130,000.[5]

These prosecutions both at home and abroad properly punish offenders for the harms they cause. Successful prosecutions such as these will also generate a significant deterrent effect, an important part of addressing the overall cybercrime problem.

III. THE PRIVACY AND CYBERCRIME ACT OF 2007 (H.R. 4175)

While law enforcement is taking many steps to aggressively address the threat of cybercrime and identity theft, loopholes and shortcomings in existing law have inhibited its ability to do so. The Privacy and Cybercrime Act of 2007 would address several of these shortcomings and provide important tools to promote law enforcement's efforts.

In particular, the Department applauds the amendments in section 108 of the Act that would assure that victims of identity theft receive fair restitution for the time spent to remediate the harm resulting from identity theft offenses. Similarly, the Department supports the inclusion of section 103 which would enhance our ability to prosecute criminals who steal sensitive information from computers, section 104 (with some technical amendments that I will describe later) that would close loopholes in the cyber-extortion statute, and sections 101 and 105 that would enhance our ability to bring

[5] *See* Department of Justice, Press Release (November 13, 2007), *available at* http://www.cybercrime.gov/romanianphishingArrest.htm

computer crime charges against criminal conspiracies and organized criminal groups. In addition to these many positive aspects, the Department would like to provide some additional proposals that would strengthen the bill. The Department would also like to recommend a number of technical suggestions for Title I of the Act.

A. Additional Provisions That Would Strengthen the Act

1) Malicious Spyware, Botnets, and Keyloggers

The Department strongly encourages the Committee to consider adding to the bill an amendment to 18 U.S.C. § 1030(a)(5) that would appropriately penalize the use of malicious spyware, botnets, and keyloggers. Criminals routinely use these tools to steal sensitive information and commit identity theft and other crimes, and federal law creates a loophole that significantly inhibits the prosecution of such offenders.

Existing section 1030(a)(5) criminalizes actions that cause "damage" to computers, i.e., that impair the "integrity or availability" of data or computer systems. Absent special circumstances, the loss caused by the criminal conduct must exceed $5,000 to constitute a federal crime. Many identity thieves obtain personal information by installing "bots" and malicious spyware on numerous individual computers. Whether or not the programs succeed in obtaining the unsuspecting computer owner's financial data, these sorts of programs harm the "integrity" of the computer and data. Nevertheless, it is often difficult or impossible to measure the loss this damage causes to each computer owner, or to prove that the total value of these many small losses exceeds $5,000.

Two amendments could remedy this situation, and Congress could enact them separately or in tandem. First, Congress could amend section 1030(a)(5) to make it a misdemeanor offense where a person damages protected computers but causes less than $5,000 in loss. The current felony penalty would remain for losses that exceed $5,000.

Second, Congress could create an alternative basis for triggering the existing felony provision: damage to more than 10 protected computers. In either case, the government would have another tool for prosecuting individuals who plant malicious spyware on a large number of computers.

We note that S. 2168, as passed by the Senate on November 15, 2007, as well as the Identity Theft Task Force Report, contains language that accomplishes both of these goals. We urge Congress to add these provisions to H.R. 4175 as it would close a significant gap in the computer fraud and identity theft regime. Moreover, even if Congress decides to enact section 106 without amendment, we urge it to add a provision that would amend existing section 1030(a)(5) to include "***damage affecting ten or more protected computers during any one-year period***."

2) Enhancing the Prosecution of Identity Theft

The current identity theft offense (18 U.S.C. § 1028(a)(7)) and the aggravated identity theft offense (18 U.S.C. § 1028A) are both limited to stealing the identity of an individual and do not specifically address the misuses of the identification of a corporation or organization. The Department recommends adding a provision that would amend both statutes to ensure that identity thieves who steal identity information belonging to corporations and organizations can be prosecuted, such as when they send phishing emails using the entity's name, logo, and other identifying marks in order to trick the end user. The legislation should also add several new crimes to the list of aggravated identity theft offenses to ensure that the aggravated identity theft offense can be applied to a wider range of federal crimes that are frequently associated with identity theft, such as mail theft. This amendment was proposed in the Identity Theft Task Force's Strategic Plan, and S. 2168 contains such a provision. Proposed language for this amendment is contained in Appendix A.

B. Amendments to the Provisions of H.R. 4175

1) Section 102 – Law Enforcement Notification of Security Breaches Involving Sensitive Personally Identifiable Information

Section 102(c)(2) of the Act requires that "[t]he Secret Service and the Federal Bureau of Investigation shall annually publish in the Federal Register a list of all notifications submitted the previous calendar year and the identity of each entity with respect to which the major security breach occurred." Because of the potential national security implications of many security breaches, the Act should waive the publication requirement in some circumstances. We note the bill does later establish a waiver for national security reasons in section 203, but that waiver applies only to the portion of the bill addressing 5 U.S.C. § 553a, and would not affect the publication requirement. A similar national security waiver should be available in Section 102. We look forward to the opportunity to work with the Committee to address this issue.

Section 102(e)(3)(A)(i) of the bill also defines the term "major security breach" to include any security breach whereby the "means of identification pertaining to 10,000 or more individuals" is lost. This threshold is too high. To give the number some context, an intrusion attack involving the theft of as few as 1,000 credit card numbers is, under the current United States Sentencing Guidelines, presumed to involve a minimum loss of $500,000. Similarly, law enforcement should be fully empowered to open an investigation, for example, where the breach involves the records of "only" 9,000 individuals. We therefore recommend that this number be reduced to 1,000. Furthermore, the use of these thresholds could result in failure to report in critical situations that do not involve large numbers. For that reason, we believe that this section should be amended to also require notification where there may be a threat to national security or a risk of significant monetary loss, without regard to the number of records breached.

2) Section 104 – Cyber-Extortion

This provision would add the words "or to access without authorization or exceed authorized access to a protected computer" to 18 U.S.C. § 1030(a)(7). If the goal is to take into account the problem that some cyber-criminals extort companies without explicitly threatening to cause damage to computers, then we recommend a slightly different solution to that problem.

More importantly, section 104 would not cover several emerging types of criminality. For example, the language would not cover the situation in which a criminal has *already* stolen the information and then threatens to disclose it unless paid off. Similarly, other criminals cause damage first – such as by accessing a corporate computer without authority and encrypting critical data – and then threaten that they will not correct the problem unless the victim pays.

In order to address these situations, the Department recommends amending section 104 of the bill so that it matches section 6 of S. 2168, which passed the Senate on November 15, 2007. (The proposal also appeared in the Identity Theft Task Force's Strategic Plan.) That text is provided in Appendix B for your convenience.

3) Section 106 – Penalties for Section 1030 Violations

We support the addition of forfeiture provisions for 18 U.S.C. § 1030. The wording in the current bill, however, does not adequately accomplish its goal because it does not specify what procedures will be used in forfeiture hearings. Thus, instead of the wording in section 106 of the bill, however, we would propose new language to be placed in two new subsections (*See* Appendix C). This new language is necessary for several reasons.

First, the law should allow for both civil and criminal forfeiture. Second, like other forfeiture provisions, the forfeiture of property used to facilitate computer crimes should also include real property.

Third, the following procedural reference should be included for the civil provisions of Chapter 46 of Title 18 at the end of subsection (j):

> *Seizures and forfeitures under this subsection shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) of title 18 shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security.*

This change would take into account the fact that the Homeland Security Act moved certain enforcement officials from the Treasury Department to the Department of Homeland Security. It would also harmonize this section with existing forfeiture law and save limited judicial and prosecutorial resources in uncontested civil forfeiture cases.

Finally, any references to "proceeds" in the forfeiture section should be changed to "gross proceeds." Failure to include the phrase "gross proceeds" will allow criminals to argue that they are entitled to deduct their overhead expenses and costs-of-doing-business from the amounts the government attempts to recover via forfeiture. Criminals should not be allowed such a loophole.

4) Section 107 – Additional Funding

Consistent with the Department's budgetary requests, we support the proposal to give additional funds to various law enforcement agencies to investigate and prosecute criminal activity involving "computers and other information technology." Since almost any crime today uses computers or telephones, however, this broad language would not necessarily target the crimes upon which this bill focuses. Instead, we would suggest that the funds be allocated to "investigate and prosecute criminal activity involving

unauthorized access to computers, identity theft, and similar offenses." This would limit the distribution of the additional funding to combating the types of activity addressed by other sections of the Act.

In addition, we recommend that the Attorney General have authority to decide how best to allocate these funds within the Department. Thus, we propose striking the words "for the Criminal Division of the Department of Justice."

5) Section 109 – Review and Amendment of Federal Sentencing Guidelines

Section 109 provides a useful directive to the Sentencing Commission to reassess the sentencing of cyber-criminals. We support this provision, but would propose adding some additional criteria that the Commission should take into account in its revision of the Guidelines. Many of these additional factors appear in S. 2168, as passed by the Senate on November 15, 2007.

Intent to Cause Harm. Like the current statutory sentencing scheme, 18 U.S.C. § 1030(c)(3)(B) and (c)(4), the Guidelines explicitly address the question of intent to cause damage to computers. If the offender causes damage intentionally, the Guidelines call for a 4-level increase. U.S.S.G. §2B1.1(b)(14). Unfortunately, Subsection 14 contains a number of bases for an increased sentence, and this mix of factors does not always lead to the appropriate outcome. The source of this problem is the subsection's directive to "Apply the Greatest" of three elements, each of which should be treated separately in most cases. For example, the first of these elements directs the court to increase a defendant's guideline range by two levels if the offense includes the unauthorized access to a military computer or the theft of personal information. If the offender also intentionally causes damage, however, he triggers the second element, a 4-level increase, and the court will ignore the first element. Thus, if the offender intentionally damages a Pentagon computer, the Guidelines would assign him the exact same guideline range as

someone who intentionally damages a grocery store computer. This outcome makes little sense, and the Sentencing Commission should allow each of these elements to apply independently of one another. The bill could add as a criteria for the Commission, "*whether the defendant's intent to cause damage or intent to obtain personal information should be disaggregated and considered separately from the other factors set forth in USSG 2B1.1(b)(14)*."

Definition of "Victim." While the definition of victim appropriately includes those that suffer financially, it does not similarly take into account victims who suffer non-financial harm. U.S.S.G. §2B1.1, Application Note 1, restricts the definition of "victim" to include only those who have suffered loss that can be measured in monetary terms. This is inappropriate and should be corrected.

For example, the Guidelines provide for increases where a crime causes harm to many victims, yet this basic principle does not apply to victims whose privacy has been invaded. Thus, if a malicious spyware program invades the privacy of many computer owners but does not cause any quantifiable monetary loss, the sentencing increases set out in the Guidelines for crimes involving multiple victims do not apply. Yet it makes no sense for the guidelines to direct courts to enhance sentences for privacy invasions but then define "victim" to be only those that suffer monetary harm. The Sentencing Commission should address this problem by amending the definition of victim so that it includes persons whose privacy was invaded by the criminal offense. We suggest that the Commission be directed to evaluate "*whether the term 'victim' as used in USSG 2B1.1 should include individuals whose privacy was violated as a result of the offense in addition to individuals who suffered monetary harm as a result of the offense.*"

Disclosure of Personal Information to Others. The Guidelines do not explicitly address the situation in which private information is disclosed to others beyond the individual who gains unauthorized access to it. Because posting stolen information on

the Internet or selling sensitive information to identity thieves increases the significance of the privacy invasion, the Sentencing Commission should amend the Guidelines to include an increased penalty for such an action, by considering "*whether the defendant disclosed personal information obtained during the commission of the offense.*"

Value of Information Stolen. In general, the market value of real-world stolen property is a good measure of the significance of the crime and the Guidelines appropriately increase sentences based on that value. The theft of electronic information, however, differs in one significant respect: the offender generally only *copies* the data and does not deprive the owner of possession or use of it. While this circumstance will reduce the harm experienced by the victim, the value of the information remains a good proxy for the significance of the offense.

In the case of computer data, moreover, it may prove difficult at times to establish the value of the information. Some types of information, such as a customer list, have a market value that can be established at trial through expert testimony or by introducing evidence that the offender sold it to another person. But it may be impossible to put a price tag on other types of information, even though it plainly cost someone a considerable amount of money to create the data. For example, an individual broke into a NASA computer in 1999 and stole a software program developed to control the physical environment on the International Space Station. It cost NASA $1.7 million dollars to develop this software, but it may or may not have value on the open market. In these situations, the cost of developing the information, or the harm caused by disclosing it, provides a reasonable alternative measure of its value, and courts should be able to utilize these measures in calculating the harm caused by the offense. We suggest that the bill direct the Commission to consider:

> *The potential and actual loss resulting from the offense, including the value of information obtained from a protected computer, regardless of whether the owner was deprived of use of the information, and considering such factors as the*

> *market value of the information, the cost of developing the information, the value to the owner of the information remaining confidential, and the harm caused by the disclosure of the information.*[6]

* * *

In conclusion, the Department would like to emphasize that law enforcement has a critical role in addressing the growing threat of computer crime and identity theft. But we can do that only if we have the proper laws in place to investigate and prosecute these criminals and only if we have appropriate resources. The Privacy and Cybercrime Act of 2007 addresses many of those needs by closing loopholes in existing cybercrime statutes, improving our ability to prosecute criminal groups, and providing much-needed resources. With the changes I've suggested, the Act will be an important milestone in the fight against cybercrime.

Mr. Chairman, this concludes my remarks. I would be pleased to answer questions from you and other members of the Committee.

[6] We note that section 10(b)(3)(B) of S. 2168 contains similar language, but it focuses on the cost incurred by the victim. We believe that it is better to direct the U.S. Sentencing Commission to consider other factors as well, such as the harm caused by disclosure and the value of keeping the information confidential, in drafting an appropriate amendment to the U.S. Sentencing Guidelines.

APPENDIX A

PROPOSED AMENDMENTS TO THE IDENTITY THEFT AND AGGRAVATED IDENTITY THEFT STATUTES

Proposed Amendment to Aggravated Identity Theft Statute to Add Predicate Offenses

Congress should amend the aggravated identity theft offense (18 U.S.C. § 1028A) to include other federal offenses that recur in various identity-theft and fraud cases, specifically, mail theft (18 U.S.C. § 1708), uttering counterfeit securities (18 U.S.C. § 513), and tax fraud (26 U.S.C. §§ 7201, 7206, and 7207), as well as conspiracy to commit specified felonies already listed in section 1028A—in the statutory list of predicate offenses for that offense (18 U.S.C. § 1028A(c)).

Proposed Additions to Both Statutes to Include Misuse of Identifying Information of Organizations

(a) Section 1028(a) of Title 18, United States Code, is amended by inserting in paragraph (7) the phrase "(including an organization as defined in Section 18 of this Title)" after the word "person".

Section 1028A(a) of Title 18, United States Code, is amended by inserting in paragraph (1) the phrase "(including an organization as defined in Section 18 of this Title)" after the word "person".

(b) Section 1028(d)(7) of Title 18, United States Code, is amended by inserting in paragraph (7) the phrase "or other person" after the word "individual".

APPENDIX B

PROPOSED AMENDMENTS TO 18 U.S.C. § 1030(a)(7) (CYBER-EXTORTION)

Section 1030(a)

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

APPENDIX C

PROPOSED AMENDMENT TO 18 U.S.C. § 1030 (FORFEITURE)

18 U.S.C. § 1030

(i) Criminal Forfeiture

(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

(A) such person's interest in property, real or personal, that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from, any gross proceeds that such person obtained, directly or indirectly, as a result of such violation;

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) Civil Forfeiture

(1) The following shall be subject to forfeiture to the United States and no property right shall exist in them:

(A) any property, real or personal, used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section; and

(B) any property, real or personal, which constitutes or is derived from gross proceeds traceable to any violation of this section, or a conspiracy to violate this section.

(2) Seizures and forfeitures under this subsection shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) of

title 18 shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security.

Mr. SCOTT. Thank you.
Mr. Magaw.

TESTIMONY OF CRAIG MAGAW, SPECIAL AGENT, CRIMINAL INVESTIGATIVE DIVISION, U.S. SECRET SERVICE, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC

Mr. MAGAW. Good afternoon, Chairman Scott and distinguished Members of the Subcommittee. I would like to thank you for the opportunity to address the Subcommittee on the subject of identity crime and the roll of the Secret Service in these investigations.

While the Secret Service perhaps is best known for protecting our Nation's leaders, we also investigate a wide array of financial crimes and work to safeguard our Nation's critical financial infrastructure.

With the passage of legislation in 1984 and 1986, the Secret Service was authorized to investigate access device fraud, and we were given parallel authority with other law enforcement agencies in identity crimes and computer fraud cases. Through our financial and electronic crime investigations, the Secret Service has developed a particular expertise in the area of identity theft, false identification fraud, access device fraud, bank fraud and computer fraud.

In fiscal year 2007, agents of the Secret Service arrested over 4,300 suspects for identity theft crimes. These suspects were responsible for approximately $690 million in actual fraud loss to American consumers and American institutions.

The Secret Service has observed a marked increase in identity theft and cybercrime. Criminals continue to seek new methods to compromise victims' personal financial information. The recent trend observed by law enforcement is the use of computers and the Internet to launch cyber attacks targeting citizens and financial institutions.

Cyber criminals have become proficient at stealing victims' personal information through the use of phishing e-mails, account takeovers, malicious software, hacking attack and network intrusions resulting in data breach.

This stolen information is often sold in bulk quantities through illicit Web sites on the Internet. Criminal groups involved in identity theft and cybercrimes routinely operate in a multi-jurisdictional environment. By working closely with Federal, State, and local law enforcement representatives, as well as international police agencies, we are able to provide a comprehensive network of intelligence sharing, resource sharing and technical expertise that bridge jurisdictional boundaries. This partnership approach to law enforcement is vital to our criminal investigative mission.

The Secret Service has established a national network of financial crimes task forces and electronic crime task forces in cities across the United States. These task forces leverage the combined resources of local, State, and Federal law enforcement partners as well as technical experts from the academic community and private industry in an organized effort to combat threats to our financial payment system and critical infrastructure.

Collaboration between law enforcement and private sector is critical to our preventative approach to identity theft and cybercrime.

We also build partners with the academic community to ensure that law enforcement is on the cutting edge of technology by leveraging research and development capabilities of teaching institutions and technical colleges. The Secret Service appreciates the Subcommittee's work to enhance the penalties and broaden investigative jurisdictions associated with identity theft and cybercrime.

H.R. 4175 addresses many of the issues I have discussed today concerning these offenses. H.R. 4175 expands the definition of cybercrime; requires data or brokers to notify law enforcement authorities of major security breaches; and increases penalties for identity theft and other violations of data privacy and security. The Secret Service looks forward to working closely with Congress as they address identity crime legislation.

As I have highlighted in my written statement, the Secret Service has implemented a number of initiatives pertaining to identity crimes. We have dedicated enormous resources to increase public awareness, provide training to law enforcement partners and improve investigative techniques. We will continue to aggressively investigate identity theft offenders to protect consumers. The Secret Service is committed to our mission to safeguard the Nation's critical and financial infrastructure.

This concludes my prepared remarks. Thank you again for the opportunity to testify on behalf of the Secret Service.

[The prepared statement of Mr. Magaw follows:]

PREPARED STATEMENT OF CRAIG MAGAW

Good afternoon, Chairman Scott, Ranking Member Gohmert and distinguished members of the subcommittee. I would like to thank you for the opportunity to address this subcommittee on the subject of identity crime and the role of the U.S. Secret Service in these investigations.

While the Secret Service is perhaps best known for protecting our nation's leaders, we also investigate a wide variety of financial crimes. In our role of protecting the nation's critical infrastructure and financial payment systems, the Secret Service has a long history of protecting American consumers and the financial industry from fraud. With the passage of legislation in 1984, the Secret Service was provided authority for the investigation of access device fraud, including credit and debit card fraud, and parallel authority with other law enforcement agencies in identity crime cases. In recent years, the combination of the information revolution and the effects of globalization have caused the investigative mission of the Secret Service to evolve.

Through our work in the areas of financial and electronic crime, the Secret Service has developed particular expertise in the investigation of identity theft, false identification fraud, credit card fraud, debit card fraud, check fraud, bank fraud, cyber crime, and computer intrusions. In Fiscal Year 2007, agents assigned to Secret Service offices across the United States arrested over 4,300 suspects for identity theft crimes. These suspects were responsible for approximately $690 million in actual fraud loss to individuals and financial institutions.

These criminals seek the personal identifiers generally required to obtain goods and services on credit, such as Social Security numbers, names, and dates of birth. Identity crimes also involve the theft or misuse of an individual's financial identifiers such as credit card numbers, bank account numbers, and personal identification numbers.

The Secret Service has observed a marked increase in identity theft and access device fraud. Criminals continue to seek new methods of compromising victims' personal and financial information. In the 1980's and 1990's, criminals obtained stolen personal and financial information through traditional means such as, theft of mail, theft of trash from businesses or victims, home and vehicle burglaries, and theft of a victim's wallet or purse. While these low-tech methods of theft remain popular, criminal activity has evolved to new methods of obtaining large quantities of stolen information.

The recent trend observed by law enforcement is the use of computers and the Internet to launch cyber attacks targeting citizens and financial institutions. Cyber criminals have become adept at stealing victims' personal information through the use of phishing emails, account takeovers, malicious software, hacking attacks, and network intrusions resulting in data breaches.

The Secret Service continues to see a considerable volume of access device fraud, usually in the form of criminal exploitation of stolen credit card data. Of particular concern are those incidents in which large quantities of credit card and related personal data are stolen through electronic intrusions into the networked systems of major retailers or the systems of credit card processors. A considerable portion of this type of electronic theft appears to be attributable to organized groups, many of them based abroad, who pursue both the intrusions, as well as the subsequent exploitation of the stolen data. Stolen credit card data is often trafficked in units that include more than just the card number and expiration date. "Full-info cards" include such additional information as complete name and address information of the cardholder, mother's maiden name, date of birth, Social Security number, PIN, and other personal information that allows additional criminal exploitation of the account. Another marked trend observed in 2007, has been the rise in volume of trafficking in card track data together with PINs; this data allows a criminal to manufacture a fully functional counterfeit card and execute ATM withdrawals or other PIN-enabled transactions against the account.

This stolen information is often sold in bulk quantities on various illicit Internet carding portals. These portals, or "carding websites," can be likened to online bazaars where the criminal element converges to conduct their business. The websites vary in size, from a few dozen members, to some of the more popular sites which boast memberships of approximately 8,000 users. Within these portals, there are separate forums which are moderated by notorious members of the carding community. Members can meet online and discuss specific topics of interest. Criminal purveyors buy, sell, and trade malicious software, spamming services, credit, debit, and ATM card data, personal identification data, bank account information, hacking services and other contraband.

In addition to the exploitation of credit and debit card accounts, many of the more sophisticated online criminal networks are now actively exploiting compromised online financial accounts. Criminals who gain access to victim accounts using online systems then execute fraudulent electronic banking transfers or sell the information to other criminals. The desire to exploit online bank accounts has led to the explosive growth of phishing, as well as the recent wave of "malware" or "crimeware," malicious software designed specifically to harvest account login information from the computers of infected victims. The technical sophistication of the illicit services readily available continues to grow. For example, the online fraud networks are increasingly leveraging the technical capabilities of "botnets" (i.e. networks of thousands of infected computers which can be controlled by a criminal from a central location) for financial attacks ranging in nature from the hosting of phishing and other malicious websites to the launching of widespread attacks against the online authentication systems of U.S. financial institutions.

The information revolution of the 1990's has turned our personal and financial information into a valuable commodity, whether it is being collected and brokered by a legitimate company or stolen by an identity thief. This information is no longer only an instrument used to facilitate a financial crime; it is now the primary target of criminals. Consequently, private citizens as well as corporations and financial institutions must take appropriate measures to secure sensitive personally identifiable information. This information is particularly vulnerable when it is stored on personal computers or disclosed over Internet and email connections. Consumers must adhere to comprehensive computer security practices.

Today, hundreds of companies specialize in data mining, data warehousing, and information brokerage. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals. However, businesses can provide a first line of defense against identity crime by safeguarding the information they collect. Such efforts can significantly limit the opportunities for identity crime. Furthermore, the prompt reporting by data brokers of major security breaches involving sensitive personally identifiable information to the proper authorities would ensure a thorough investigation is conducted.

Globalization has made commerce easy and convenient for corporations and consumers. Financial institutions and systems are accessible worldwide. Today's cyber criminals have adapted to this new means of global trade and exploit our dependence on information technology. With the explosion of Internet accessibility worldwide, the criminal element has modified their fraudulent schemes to a new, more anonymous and constantly evolving cyber arena. Having been the target of many

of these crimes, the financial sector has some of the most sophisticated security and authentication mechanisms and are constantly evolving their practices to counter this criminal activity Likewise, the Secret Service has modified its investigative techniques to keep pace with emerging technologies.

Criminal groups involved in identity crimes routinely operate in a multi-jurisdictional environment. This creates problems for local law enforcement agencies that generally act as the first responders. By working closely with other federal, state, and local law enforcement representatives, as well as international police agencies, the Secret Service is able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries. This partnership approach to law enforcement is vital to our criminal investigative mission.

The Secret Service's expertise is enhanced through partnerships and identity theft task forces to assist in the national effort to safeguard personal and financial information. These partnerships with other law enforcement agencies and industry representatives perform a crucial role in protecting the financial infrastructure and economic stability of the United States by leveraging the technical expertise and investigative experience of partner agencies.

The Secret Service has established unique partnerships with state, local, and other federal law enforcement agencies through years of collaboration on our investigative and protective endeavors. These partnerships enabled the Secret Service to establish a national network of Financial Crimes Task Forces (FCTFs) to combine the resources of the private sector and other law enforcement agencies in an organized effort to combat threats to our financial payment systems and critical infrastructures. The Secret Service currently maintains 29 FCTFs located in metropolitan regions across the country. While our FCTFs do not focus exclusively on identity crime, we recognize that stolen identifiers are often a central component of other financial crimes. Consequently, our task forces devote considerable time and resources to the issue of identity crime.

The Secret Service has always employed a proactive, rather than reactive, approach to combating crime. In 1996, the Secret Service established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private sector, and local, state, and federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. The USA PATRIOT Act of 2001, P.L. 107–56, recognized the effectiveness of the New York ECTF and mandated that the Secret Service establish a nationwide network of ECTFs to prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

ECTFs leverage combined resources in an organized effort to combat threats to our financial payment systems and critical infrastructures. Partnerships between law enforcement and the private sector are critical to the success of the ECTF's "focus on prevention" approach. Our ECTFs collaborate with private sector technical experts in an effort to protect their system networks and critical information by encouraging the development of business continuity plans and routine risk management assessments of their electronic infrastructure. Greater ECTF liaison with the business community provides rapid access to law enforcement and vital technical expertise during incidents of malicious cyber crimes. The ECTFs also focus on partnerships with academia to ensure that law enforcement is on the cutting edge of technology by leveraging the research and development capabilities of teaching institutions and technical colleges.

These resources allow ECTFs to identify and address potential cyber vulnerabilities before the criminal element exploits them. This proactive approach has successfully prevented cyber attacks that otherwise would have resulted in large-scale financial losses to U.S. based companies or disruptions of critical infrastructures.

The Secret Service task force models open the lines of communication and encourage the unlimited exchange of information between federal, state, and local law enforcement. Currently, the Secret Service maintains 24 ECTFs in major metropolitan regions across the United States.

Another important goal of the Secret Service is to raise awareness of issues related to identity theft and financial crimes, both in the law enforcement community and the general public. The Secret Service has worked to educate consumers and provide training to law enforcement personnel through a variety of programs and initiatives. Agents from local field offices routinely provide community outreach seminars and public awareness training on the subjects of identity theft and computer fraud. Agents often address these topics when speaking to school groups, civic organizations, and staff meetings involving businesses or financial institutions.

Additionally, the Secret Service provides recurring identity theft training to state and local police departments. This training includes formal and informal classes which occur at police roll calls, field office sponsored seminars, police academies, and other various settings. Currently, the Secret Service provides formal computer training to state and local police departments to allow officers to act as "first responders" in cyber crimes investigations. Officers are trained in basic electronic crimes investigations, network intrusion investigations, and computer forensics.

The Secret Service currently participates in a joint effort with the Department of Justice, the U.S. Postal Inspection Service, the Federal Trade Commission (FTC), the International Association of Chiefs of Police (IACP), and the American Association of Motor Vehicle Administrators to host identity crime training for law enforcement officers. In the last three years, Identity Crime Training Seminars have been held in approximately 20 cities nationwide. These training seminars are focused on providing local and state law enforcement officers with tools and resources that they can immediately put into use in their investigations of identity crime.

The Secret Service has also assigned a special agent to the FTC as a liaison to support all aspects of the Commission's program to encourage the use of the Identity Theft Data Clearinghouse as a law enforcement tool. The FTC has done an excellent job of providing people with the information and assistance they need in order to take the steps necessary to correct their credit records, as well as undertaking a variety of consumer awareness initiatives regarding identity theft.

Additionally, the Secret Service is committed to providing our law enforcement partners with publications and guides to assist them in combating identity theft and cyber crime. As criminals increasingly use computers and electronic storage devices, these items become important pieces of evidence. To ensure proper investigation and successful prosecution, officers need specific instructions pertaining to the seizure and analysis of electronic evidence. To provide this essential knowledge, the Secret Service published the *"Best Practices Guide for Seizing Electronic Evidence"* which is designed as a pocket guide for the police officers and detectives acting as first responders. This guide assists law enforcement officers in recognizing, protecting, seizing, and searching electronic devices in accordance with applicable statutes and policies. This guide has been updated as appropriate, and it is currently issued in its third edition.

The Secret Service also cooperated with several of our task force partners to produce the interactive, computer-based training program known as "Forward Edge." *Forward Edge* is a CD-ROM that provides law enforcement and corporate investigative personnel with practical training in the recognition and seizure of electronic storage items. This year we completed an updated version of this training tool and just released "*Forward Edge II*."

In addition, the Secret Service produced an Identity Crime Video/CD-ROM which contains over 50 investigative and victim assistance resources that local and state law enforcement officers can use when combating identity crime. This CD-ROM also contains a short identity crime video that can be shown to police officers at their roll call meetings which discusses why identity crime is important, what other departments are doing to combat identity crime, and what tools and resources are available to officers. The Identity Crime CD-ROM is an interactive resource guide that was made in collaboration with the U.S. Postal Inspection Service, the FTC and the IACP.

To date, approximately 50,000 Identity Crime CD-ROMs have been distributed to law enforcement departments and agencies across the United States. We have distributed over 400,000 *Best Practices Guides* and over 50,000 *Forward Edge* training CD-ROMs to local and federal law enforcement officers nationwide.

In conclusion, I would like to reiterate that identity theft is an evolving threat. Law enforcement agencies must be able to adapt to emerging technologies and criminal methods. The Secret Service is pleased that Congress is considering legislation that recognizes the magnitude of these issues and the constantly changing nature of these crimes. To effectively fight this crime, our criminal statutes must be amended to safeguard sensitive personally identifiable information and to afford law enforcement the appropriate resources to investigate data breaches.

The Secret Service appreciates the Subcommittee's work to enhance penalties and broaden investigative jurisdictions associated with identity theft and cyber crime. H.R. 4175 addresses many of the issues I have discussed in this statement concerning these offenses. H.R. 4175 expands the definition of cyber crime, requires data brokers to notify law enforcement authorities of major security breaches, and increases penalties for identity theft and other violations of data privacy and security. The Secret Service looks forward to working closely with Congress as they address identity crime legislation.

As I have highlighted in my statement, the Secret Service has implemented a number of initiatives pertaining to identity crimes. We have dedicated enormous resources to increase awareness, educate the public, provide training for law enforcement partners, and improve investigative techniques. We will continue to aggressively investigate identity theft offenders to protect consumers. The Secret Service is committed to our mission of safeguarding the nation's critical infrastructure and financial payment systems.

Chairman Scott, Ranking Member Gohmert, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.

Mr. SCOTT. Thank you.

Mr. Winston.

TESTIMONY OF JOEL WINSTON, ASSOCIATE DIRECTOR, DIVISION OF PRIVACY AND IDENTITY PROTECTION, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, WASHINGTON, DC

Mr. WINSTON. Thank you, Chairman Scott, Ranking Member Gohmert and Members of the Subcommittee. I appreciate the opportunity to testify today about these critical issues of privacy and identity theft.

As the Federal Trade Commission's recently issued national survey shows, identity theft continues to afflict millions of Americans every year with losses in the billions of dollars. But beyond these real and substantial direct costs, this crime harms our economic system by threatening consumer confidence. Many polls show that the level of consumer anxiety about identity theft is extremely high.

The FTC plays a lead role in the battle against identity theft through its law enforcement efforts; its work on the President's task force; its extensive consumer and business education; and its assistance to criminal law enforcement partners.

One way to stop identity theft is to keep sensitive information out of the hands of thieves by ensuring that businesses protect the information they collect. Reports of the latest data breaches appear almost daily and continue to shake consumer confidence. Of course, not all data breaches lead to identity theft, but some do, causing real damage to affected consumers.

The Commission uses its authority under several Federal laws to take action against businesses that fail to reasonably protect sensitive consumer information. Since 2001, the FTC has brought 15 data security cases, including our most recent case announced this morning against a mortgage company that threw sensitive consumer loan files into publicly accessible dumpsters.

In addition to its enforcement efforts, the Commission has played a lead role in the President's Identity Theft Task Force. The task force's strategic plan recommended 31 initiatives to reduce the incidence and impact of identity theft. The recommendations focus on, first, prevention, making it more difficult for criminals to steal data or to misuse data they do manage to steal. Second, victim assistance, helping consumers recover from identity theft. And, third, deterrence: Strengthening the tools that we have to catch and punish the criminals. Most of these 31 recommendations have been or are in the process of being implemented.

With respect to prevention, the FTC has developed and distributed highly successful business and consumer guidance on data security. Materials include a very popular data security guide for businesses, which now comes with an online tutorial. And the Commission staff will be holding a series of regional data security seminars across the country beginning next year.

On the consumer side, the Commission launched last year a multimedia campaign titled, Deter, Detect, Defend. Here is a copy of the package. It includes brochures and training kits. And the Commission sponsors a multimedia Web site, OnGuard Online, which has information for consumers on basic computer security. Since its launch, this Web site has attracted over 4.3 million visits.

Despite our best efforts to improve data security, however, there is no foolproof way to stop data theft. For that reason, it is critical that we do whatever we can to make the data less useful for thieves.

As recommended by the task force, the Commission conducted two public workshops this year relating to the issue of consumer authentication. By creating better ways to verify consumers' identities when they open new accounts or when they access existing accounts, we can make it more difficult for criminals to use stolen data.

Regulations recently issued by the FTC and the Federal bank regulatory agencies, under the FACT Act, provide another tool in the battle to prevent identity theft. These rules require all businesses that hold consumer accounts to establish an identity theft prevention program.

With regard to victim assistance, the Commission has continued its role as a central repository for identity theft information. Between 15,000 and 20,000 consumers contact us each week for information on how to guard against identity theft, or to obtain help on recovery from it. Consumers who contact us receive step-by-step advice. At the same time, the information these consumers give us is entered into our clearinghouse and is made available to over 1,700 law enforcement agencies for use in law enforcement.

We are also partnering with other agencies to provide training for local law enforcement across the country. And we have developed and posted a universal police report identity theft victims can complete online, print and take to law enforcement for verification. With this report, victims have access to a number of rights, including the right to place a 7-year fraud alert on their credit file.

To summarize, identity theft is one of the most important consumer protection issues of our time and must be attacked from every angle. The Commission will continue to place a high priority on preventing this crime and helping victims to recover.

We look forward to continuing our work with Congress in this effort. I would be happy to answer any questions you may have.

[The prepared statement of Mr. Winston follows:]

PREPARED STATEMENT OF JOEL WINSTON

PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

HOUSE COMMITTEE ON THE JUDICIARY

on

Protecting Consumer Privacy and Combating Identity Theft

Washington, DC

December 18, 2007

I. INTRODUCTION

Chairman Scott, Ranking Member Gohmert and members of the Subcommittee, I am Joel Winston, Associate Director of the Division of Privacy and Identity Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's testimony on protecting consumer privacy and combating identity theft.

Protecting privacy is a critical component of the Commission's consumer protection mission. The explosive growth of the Internet and the development of sophisticated computer systems and databases have made it easier than ever for businesses and other organizations to gather, store, and use information about consumers.[2] These new information systems can provide tremendous benefits to consumers, such as enabling fast and convenient access to services and information. At the same time, if the sensitive information needed to enable these services is not protected adequately, or if consumers' identities are not authenticated properly, consumers can suffer harm, including identity theft. This testimony will summarize the Commission's efforts to protect privacy and fight identity theft through its law enforcement actions, its participation on the President's Identity Theft Task Force, and its extensive consumer and business education and outreach activities.

---

[1]The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any individual Commissioner.

[2]A recent study by research firm IDC estimates that worldwide digital information will increase to 988 billion gigabytes by 2010, as compared to 161 billion gigabytes in 2006. *See* http://www.emc.com/about/destination/digital_universe/ One gigabyte equals one billion units of information.

II. THE IDENTITY THEFT PROBLEM

Identity theft is a serious concern in our information-based economy. Millions of consumers are victimized by this crime every year.[3] Identity theft takes two primary forms: misuse of existing credit card, debit card, or other accounts ("existing account fraud"); and the use of stolen information to open new accounts in the consumer's name ("new account fraud"). The Commission's most recent national identity theft survey confirmed findings from earlier surveys that new account fraud, although less prevalent than existing account fraud, typically causes considerably more harm to consumers in out-of-pocket expenses and time necessary to repair the damage.[4] At the same time, new forms of identity theft have become more prevalent, including medical ID theft and immigration and employment fraud.

Beyond its direct costs, identity theft harms our economy by threatening consumers' confidence in the marketplace generally and in electronic commerce specifically. An April 2007 Zogby Interactive survey found that 91 percent of adult users of the Internet are concerned that their identities might be stolen (including 50 percent who are "very concerned").[5] In a May 2006 Wall Street Journal/Harris Interactive survey, as a result of fears about protecting their identities,

---

[3] The FTC recently released its second nationwide survey of the incidence and impact of identity theft ("ID Theft Survey"). The survey found that 8.3 million adults were victims of identity theft in 2005. The survey report can be found at www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

[4] The FTC survey found that 6.5 million consumers were victims of existing account fraud, and 1.8 million experienced new account frauds or other types of identity fraud. Over half of the victims of existing account fraud, and 37 percent of victims of new account fraud, suffered no out-of-pocket expenses in coping with the theft. Conversely, 25 percent of new account fraud victims incurred at least $1000 in expenses, compared to fewer than 10 percent of existing account fraud victims. New account fraud victims also spent significantly more time repairing the damage than did existing account fraud victims. ID Theft Survey, at 37-39.

[5] *See* Zogby Poll: Most Americans Worried About Identity Theft, *available at* www.zogby.com/search/ReadNews.dbm?ID=1275

30 percent of consumers polled stated that they were limiting their online purchases, and 24 percent said they were cutting back on their online banking.[6]

III. FTC ACTIONS TO COMBAT IDENTITY THEFT

The government and private sector must work together to reduce the opportunities for thieves to obtain consumers' personal information, and make it more difficult for thieves to misuse the information if they do obtain it. The FTC is playing a lead role in these efforts.

A. Law Enforcement on Data Security

One important way to keep sensitive information out of the hands of identity thieves is by ensuring that those who maintain such information adequately protect it. The Commission plays an active role in furthering this goal by bringing law enforcement actions against businesses that fail to implement reasonable security measures to protect sensitive consumer data.

Public awareness of, and concerns about, data security continue at a high level as reports about the latest data breaches of sensitive personal information continue to proliferate. Recent breaches have touched both the public and private sectors. Of course, not all data breaches lead to identity theft; in fact, many prove harmless or are caught and addressed before any harm occurs.[7] Nonetheless, some breaches - especially those that result from deliberate actions by criminals, such as hacking - have led to identity theft.

---

[6] *See* Jennifer Cummings, *Substantial Numbers of U.S. Adults Taking Steps to Prevent Identity Theft*, The Wall Street Journal Online, May 18, 2006, http://www.harrisinteractive.com/news/newsletters/WSJfinance/HI_WSJ_PersFinPoll_2006_vol2_iss05.pdf.

[7] *See* Government Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), *available at* www.gao.gov/new.items/d07737.pdf.

The FTC enforces several laws that contain data security requirements. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act ("GLB Act"), for example, contains data security requirements for financial institutions.[8] The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,[9] and imposes safe disposal obligations on entities that maintain consumer report information.[10] In addition, the FTC has enforced the Federal Trade Commission Act's proscription against unfair or deceptive acts or practices in cases where a business made false or misleading claims about its data security procedures, or where its failure to employ reasonable security measures caused substantial consumer injury.[11]

Since 2001, the Commission has brought fourteen cases challenging businesses that allegedly failed to reasonably protect sensitive consumer information that they maintained.[12] In a number of these cases, the Commission alleged that the company had misrepresented the nature or extent of its security procedures in violation of the FTC Act's prohibition on deceptive

---

[8] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

[9] 15 U.S.C. § 1681e.

[10] *Id. at* § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 382.

[11] 15 U.S.C. § 45(a).

[12] *See generally* http://www.ftc.gov/privacy/index.html.

practices.[13] In several of the cases, the Commission alleged that the security inadequacies led to breaches that caused substantial consumer injury and were thus unfair practices under the FTC Act.[14] Some of the cases involved enforcement of the Commission's Safeguards Rule or the FCRA.[15]

Although the Commission has brought its data security cases under different laws, the cases share common elements. In each case, the company's alleged security vulnerabilities were multiple and systemic, and in most of the cases readily-available and inexpensive measures were available to prevent them. Together, the cases stand for the principle that companies must maintain reasonable and appropriate measures to protect sensitive consumer information.

---

[13] *E.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of Guidance Software, Inc.*, Docket No. C-4187 (April 23, 2007); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (March 4, 2005); *In the Matter of MTS Inc., d/b/a/ Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002). In its case against ChoicePoint, Inc., for example, the FTC alleged that the company inadvertently sold sensitive information on more than 160,000 consumers to a criminal gang, who used that information in some cases to commit identity theft. The company allegedly approved as purchasers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from nearby commercial photocopying facilities. The Commission alleged, among other violations, that ChoicePoint misrepresented its security measures when it failed to use reasonable procedures to screen prospective purchasers of its information. In settling the case, ChoicePoint agreed to pay $10 million in civil penalties (for alleged violations of the FCRA) and $5 million in consumer redress for identity theft victims. The company also agreed to undertake substantial new data security measures.

[14] *E.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (March 7, 2006); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005).

[15] *E.g., United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga.) (settlement entered on Feb. 15, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of Nationwide Mortgage Group Inc.*, FTC Docket No. 9319 (April 15, 2005); *In the Matter of Sunbelt Lending Services*, FTC Docket No. C-4129 (Jan. 3, 2005).

The FTC Safeguards Rule serves as a good model of this approach. Firms covered by the Rule (financial institutions) must prepare a written plan; designate an official with responsibility for the plan; identify, assess, and address foreseeable risks; oversee service providers' handling of information; monitor and evaluate the program for effectiveness; and adjust the plan as appropriate. The Rule states that what is "reasonable" will depend on the size and complexity of the business, the nature and scope of its activities, and the sensitivity of the information at issue. This standard recognizes that there cannot be "perfect" security, and that data breaches can occur even when a company maintains reasonable precautions to prevent them. The standard also is flexible and adaptable. It acknowledges that risks, technologies, and business models change over time, and that a static technology-based standard would quickly become obsolete and could stifle innovation in security practices. The Commission will continue to apply the "reasonable procedures" principle in enforcing existing data security laws.

B. Participation in the Identity Theft Task Force

On May 10, 2006, President Bush established an Identity Theft Task Force, comprised of 17 federal agencies and co-chaired by FTC Chairman Deborah Platt Majoras, with the mission of developing a comprehensive national strategy to combat identity theft.[16] The President specifically directed the Task Force to make recommendations on ways to improve the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution.

[16]Exec. Order No. 13,402, 71 FR 27945 (May 10, 2006).

In April 2007, the Task Force published its strategic plan for combating identity theft.[17] Broadly, the plan is organized around the life cycle of identity theft – from the thieves' attempts to obtain sensitive information to the impact of the crime on victims – and identifies roles for consumers, the private sector, government agencies, and law enforcement.

The Task Force Strategic Plan recommends 31 initiatives directed at reducing the incidence and impact of identity theft. The recommendations focus on *prevention* through improvements in data security and more effective customer authentication procedures, *victim assistance* by ensuring victims have the means and support to restore their identities, and *deterrence* through stronger tools to punish the criminals who perpetrate this crime.

1. Prevention

The Task Force recognized that both the public and private sectors must develop better protections for sensitive consumer data. For the public sector, the Plan recommended that federal agencies and departments improve their internal data security processes; develop breach notification systems; and reduce unnecessary uses of Social Security numbers, which are often the key item of information that identity thieves need.

For the private sector, the Task Force proposed that Congress establish national standards for data security and breach notification that would preempt the numerous state laws on these issues. The data security standards would follow the Safeguards Rule model, requiring covered entities to implement reasonable administrative, technical, and physical safeguards to ensure the security and confidentiality of sensitive consumer information, protect against anticipated threats, and prevent unauthorized access. The proposed breach notification standards would

---

[17]The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* ("Strategic Plan"), *available at* http://www.idtheft.gov.

require entities to provide notice to consumers when they experience a breach that creates a significant risk of identity theft.

In addition, the Plan recommended:

- the dissemination of additional guidance to the private sector for safeguarding sensitive consumer data,
- continued law enforcement against entities that fail to implement appropriate security,
- a multi-year consumer awareness campaign to encourage consumers to take steps to safeguard their personal information and minimize their risk of identity theft,
- a comprehensive assessment of the private sector's usage of Social Security numbers, and
- holding workshops on developing more reliable methods of authenticating the identities of individuals to prevent thieves who obtain consumer information from using it to open accounts in the consumer's name.

2. Victim recovery

Once consumers have been victimized, it is critical that they have the ability to minimize and reverse the damage to their credit records and other aspects of their identities. The Strategic Plan recommended a number of steps to aid those who assist victims, as well as the victims themselves. These include:

- development of easy-to-use reference materials for law enforcement, often the first responders to identity theft,
- implementation of a standard police report, a key document for victim recovery,
- nationwide training for victim assistance counselors,

- amendments to the criminal restitution statute to enable victims to recover for the value of their time spent in attempting to remedy the harms they suffered,
- development of an Identity Theft Victim Statement of Rights,
- exploration of a national program to allow victims to obtain a special identification document for authentication purposes, and
- studies of the efficacy of state credit freeze laws and the impact and effectiveness of the victim remedies established under the 2003 Fair and Accurate Credit Transactions Act ("FACT Act") amendments to the Fair Credit Reporting Act.

3. Deterrence

The Plan listed a host of recommendations for strengthening law enforcement's ability to detect and punish identity thieves. Some of the major recommendations included:

- development of a national identity theft law enforcement center to better consolidate, analyze, and share identity theft information among law enforcers,
- enhanced tools to target off-shore identity thieves through training of foreign law enforcement,
- diplomatic efforts to encourage other nations to clamp down on identity theft rings operating in their countries,
- expanded training of investigators and prosecutors,
- evaluation of current monetary thresholds for prosecution,
- development of task forces made up of federal, state, and local law enforcement,
- several amendments to criminal statutes, and
- development of more precise data on the cost and prevalence of identity theft.

4. Progress on Task Force recommendations

Most of the Task Force recommendations have already been implemented or are in the process of being implemented. With respect to identity theft prevention, the Office of Management and Budget has issued data security and breach management guidance for government agencies.[18] In addition, the FTC has developed and distributed detailed data security guidance for businesses that includes a brochure and online tutorial,[19] and is planning a series of regional data security conferences beginning early 2008. The FTC also hosted two important public workshops in 2007 on consumer authentication and the private sector use of SSNs.[20] A goal of both workshops was to identify ways of making sensitive consumer information, such as SSNs, less valuable for identity thieves when they are able to obtain that information. The Task Force agencies will use the record from the workshops, along with other information they have gathered from stakeholders, to prepare recommendations to the President by the end of the first quarter of 2008.

The FTC and other Task Force agencies have made substantial progress in implementing the victim assistance recommendations. The FTC has published an identity theft victim statement of rights on its website and at www.idtheft.gov, and is working with the Department of Justice to develop expanded resources for identity theft victims through DOJ grants to not-for-

---

[18]OMB Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (May 22, 2007), *available at* http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf; OMB Memorandum "Recommendations for Identity Theft Related Data Breach Notification" (September 20, 2006), *available at* http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf.

[19]*See* http://www.ftc.gov/infosecurity/

[20]*See* http://www.ftc.gov/bcp/workshops/proofpositive/index.shtml; http://www.ftc.gov/bcp/workshops/ssn/index.shtml. Prior to the SSN workshop, the FTC staff issued a summary of comments and information it had received about the SSN issue.

profit victim advocates and through the development of pro bono programs with the American Bar Association.[21] With regard to deterrence, the Department of Justice forwarded to Congress a series of recommended legislative amendments to enhance the ability of law enforcers to prosecute identity thieves. The Senate has approved a bill reflecting the DOJ recommendations.[22] The Department of Justice also is developing and presenting expanded training for their prosecutors and foreign counterparts, and, in partnership with the FTC, for state and local law enforcement.

C. Support of Identity Theft Investigation and Prosecution

The FTC's identity theft victim resources and assistance also support the investigation and prosecution of identity crimes. Through our online portal and toll-free hotline, between 15,000 and 20,000 consumers contact the FTC every week for information on how to guard against identity theft or to obtain assistance in recovery. The agency receives approximately 250,000 reports of actual identity theft every year. Consumers who report their identity theft to the FTC receive step-by-step guidance on how to minimize the harm and recover from the crime. The information they provide about their experiences is entered into the agency's Identity Theft Data Clearinghouse, a secure online resource for law enforcement. The over 1,700 investigative agencies with access to the Clearinghouse can use the data to create or support ongoing investigations, enhance penalties at sentencing phase, or coordinate with other law enforcement agencies.

---

[21] *See* http://www.ftc.gov/bcp/workshops/ssn/index.shtml.

[22] S. 2168, Identity Theft Enforcement and Restitution Act of 2007, http://www.govtrack.us/congress/bill.xpd?bill=s110-2168

To ensure that law enforcement agencies are aware of these resources and are equipped to respond to identity theft, the FTC has partnered with the Department of Justice, the U.S. Postal Inspection Service, the U.S. Secret Service, the F.B.I., and the American Association of Motor Vehicle Administrators to provide on site training to local law enforcement around the country. Since the first training in 2002, these agencies have conducted more than 26 training sessions for over 3,300 law enforcement officers from more than 1000 agencies. This critical outreach will continue with training sessions planned for North and South Carolina, Minnesota, and the New England states in the coming months.

Because law enforcement officials often are the first responders for identity theft victims, the FTC also has developed a training CD and publications on victim assistance to help law enforcement offices direct ID theft victims to the resources they need for recovery, including the FTC.[23]

D. Implementation of the FACT Act

The FACT Act extensively amended the Fair Credit Reporting Act, including the addition of a number of new provisions intended to reduce the incidence of identity theft or minimize the injury to victims. The FACT Act assigned to the Commission, alone or in coordination with one or more other federal agencies, the task of promulgating approximately twenty implementing rules, guidelines, compliance forms, and notices, and conducting nine studies with reports to Congress.

---

[23] *See* http://www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/helping-victims.html.

The FACT Act added a number of new provisions to limit the opportunities for wrongdoers to obtain unauthorized access to sensitive information, and to assist consumers in avoiding and remediating identity theft. With respect to prevention, the FACT Act requires merchants to truncate the account number and redact the expiration date on consumers' copies of electronic credit card receipts.[24] In addition, the FTC and bank regulatory agencies recently released the final Identity Theft Red Flags Rules. These rules and accompanying guidelines require each financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, to develop and implement an "Identity Theft Prevention Program."[25]

The FACT Act also empowers consumers to take steps to limit the damage from identity theft once they become victims. Initially, the Act enhances consumers' opportunities to review their credit records and spot incipient signs of identity theft before further damage ensues. Consumers, for example, have the right to receive a free credit report every twelve months, through a centralized source, from each of the nationwide consumer reporting agencies ("CRAs"), as well as from nationwide "specialty" CRAs.[26] Consumers who have a good faith

---

[24] 15 U.S.C. § 1681c(g).

[25] *See* http://www.ftc.gov/opa/2007/10/redflag.shtm and accompanying regulatory text. The agencies also recently issued the final Affiliate Marketing Rules intended to enhance consumer privacy. The rules prohibit a person from using information obtained by an affiliate for marketing purposes unless the consumer has been given notice and has had an opportunity to opt out of the marketing. *See* http://www.ftc.gov/opa/2007/10/affiliate.shtm, and accompanying regulatory text.

[26] 15 U.S.C. § 1681j(a)(1)(c). The FTC regulations implementing this program are at 16 C.F.R. Part 610. The Commission has taken action to uphold the integrity of the free report program, including two cases against a company that offered "free" credit reports tied to the purchase of a credit monitoring service, through the web site "freecreditreport.com." *FTC v. Consumerinfo.com, Inc.*, No. SACV05-801AHS(MLGx) (C.D. Cal. Aug. 15, 2005); *FTC v. Consumerinfo.com, Inc.*, No. SACV05-801AHS(MLGx) (C.D. Cal. Jan. 8, 2007). In the first case, the Commission charged, among other things, that the defendants, affiliates of the nationwide consumer reporting agency Experian, had deceptively

suspicion that they have been or are about to become victims of fraud or related crimes such as identity theft may place an initial, 90-day fraud alert on their credit files, warning potential users of their report to exercise special vigilance in opening accounts in the consumers' names.[27] Actual victims may request an extended, seven-year alert if they provide a police report to the CRA.[28] In addition, victims may obtain from creditors the underlying documentation associated with transactions that may have been fraudulent,[29] block fraudulent information on their credit file,[30] and prohibit creditors from reporting fraudulent information to CRAs.[31]

The FTC maintains an active program to implement and enforce the FACT Act provisions and to educate consumers and businesses about their rights and obligations. As recommended by the Identity Theft Task Force, for example, the Commission has developed a "universal police report" that an identity theft victim can complete online, print and take to a local law enforcement agency for verification. The report, in turn, allows victims to request that fraudulent information on their credit report be blocked and to obtain a seven-year fraud alert on

---

mimicked the FACT Act free report program. The stipulated order required the defendants to make prominent disclosures that their program is not associated with the free annual report program and provide a link to the official Web site for that program, www.annualcreditreport.com. The defendants also agreed to pay $950,000 in disgorgement and to provide refunds to dissatisfied past customers. In the second case, the Commission alleged that Consumerinfo had violated the 2005 order. The new order prohibits the company from suggesting that it is affiliated with the FACT Act program, and includes a $300,000 judgment for consumer redress.

[27] 15 U.S.C. § 1681c-1(a).

[28] *Id. at* § 1681c-1(b).

[29] *Id. at* § 1681g(e).

[30] *Id. at* § 1681c-2.

[31] *Id. at* § 1681s-2(a)(6).

their credit file. The reports also ensure that identity theft complaints flow into the FTC's ID Theft Data Clearinghouse for the use of law enforcement officers.

E. Consumer and Business Education

Both independently and pursuant to the Identity Theft Task Force Strategic Plan, the Commission had undertaken substantial efforts to increase consumer and business awareness of the importance of protecting data and taking other steps to prevent identity theft, as well as steps that can be taken to minimize the damage when a theft does occur. As noted earlier, the Commission receives approximately 15,000 to 20,000 contacts each week through its toll-free hotline and online complaint form from consumers who are seeking advice on how to recover from identity theft or how to avoid becoming a victim in the first place. The FTC's identity theft primer[32] and victim recovery guide[33] are widely available in print and online. Since 2000, the Commission has distributed more than 9.7 million copies of the two publications, and recorded over 4.5 million visits to the Web versions.

Last year, the Commission launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend." It includes direct-to-consumer brochures, as well as training kits and ready-made materials (including presentation slides and a video) for use by businesses, community groups, and members of Congress to educate their employees, communities, and constituencies. The Commission has distributed over 2.6 million brochures and 60,000 kits to date, and has recorded more than 4.8 million visits to the education program's

---

[32] *Avoid ID Theft: Deter, Detect, Defend, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.htm.

[33] *Take Charge: Fighting Back Against Identity Theft, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.htm.

Web site this year alone. The Commission also has partnered with other organizations to broaden its reach. As just one example, the U.S. Postal Inspection Service initiated an outreach campaign to place FTC educational materials on subway cars in New York, Chicago, San Francisco, and Washington D.C.

The Commission also sponsors a multimedia website, OnGuard Online, designed to educate consumers about basic computer security, including the importance of not disclosing personal information to possible fraudsters.[34] OnGuard Online was developed in partnership with other government agencies and the technology sector, and since its launch has attracted more than 4.3 million visits.

The Commission directs its outreach to businesses as well. As noted earlier, the FTC widely disseminates its business guide on data security, along with a new online tutorial based on the guide. The guide articulates the key steps that businesses should take as part of a sound data security plan:

- "Take stock" - know what personal information you have in your files and on your computers,
- "Scale down" - keep only what you need for your business,
- "Lock it" - protect the information that you keep,
- "Pitch it" - properly dispose of what you no longer need, and
- "Plan ahead" - create a plan to respond to security incidents.

---

[34] *See* www.onguardonline.gov/index.html.

IV. OTHER FTC PRIVACY INITIATIVES

A. Pretexting

The Commission has acted aggressively on several other issues that threaten consumer privacy, with a particular focus on practices that cause consumer harm. One example of the injury that can befall consumers from threats to their privacy results from "pretexting," a practice whereby perpetrators use fraud or pretense to obtain access to consumers' financial information, telephone call records, or other sensitive information. Consumers who fall victim to pretexting may become the targets of stalking or other crimes. The Commission has brought a number of law enforcement actions in recent years against alleged pretexters and those who hire them.[35]

B. Spam, Spyware, and Telemarketing

The Commission has acted to protect consumers from other privacy threats, including spyware, spam, and unwanted telemarketing calls. The Commission has brought eleven spyware cases, including a recent action against a company that allegedly used deceptive practices to install adware on consumers' computers that tracked their online activity and targeted pop-up

---

[35] *E.g., FTC v. Action Research Group*, No. 6:07-CV-0227-ORL-22JGG (M.D. Fla. filed Feb. 15, 2007), *available at* http://www.ftc.gov/os/caselist/0723021/070214actionresearchgrpcmplt.pdf; *FTC v. Info. Search, Inc.*, No. 1:06-CV-01099-AMD (D. Md. filed May 1, 2006), *available at* http://www.ftc.gov/os/caselist/pretextingsweep/060501informationsearch-cmplt.pdf; *FTC v. AccuSearch, Inc. d/b/a Abika.com*, No. 06-CV-0105 (D. Wyo. filed May 1, 2006), *available at* http://www.ftc.gov/os/caselist/pretextingsweep/060501accusearchcomplaint.pdf; *FTC v. CEO Group, Inc. d/b/a Check Em Out*, No. 06-60602 (S.D. Fla. filed May 1, 2006), *available at* http://www.ftc.gov/os/caselist/pretextingsweep/060501ceogroup-cmplt.pdf; *FTC v. 77 Investigations, Inc.*, No. EDCV06-0439 VAP (C.D. Cal. filed May 1, 2006), *available at* http://www.ftc.gov/os/caselist/pretextingsweep/060501-77investigcmplt.pdf; *FTC v. Integrity Sec. & Investigation Servs., Inc.*, No. 2:06-CV-241-RGD-JEB (E.D. Va. filed May 1, 2006), *available at* http://www.ftc.gov/os/caselist/pretextingsweep/060503integritysecurcmplt.pdf.

ads back to them.[36] Since 1997, the Commission has brought 92 law enforcement actions involving spam, 29 of which were filed after Congress enacted the CAN-SPAM Act.

With respect to telemarketing, the National Do Not Call Registry currently includes more than 145 million telephone numbers, and this program has been tremendously successful in protecting consumers' privacy from unwanted telemarketing calls. Although the Commission appreciates the high rate of compliance with its Do-Not-Call Rule, it vigorously enforces the requirements of the Registry to ensure its ongoing effectiveness. Violations of the Do-Not-Call rule subject telemarketers to civil penalties of up to $11,000 per violation. Thirty-four FTC telemarketing cases have alleged Do-Not-Call and/or Abandoned Call violations, resulting in $16.4 million in civil penalties and $8.2 million in consumer redress or disgorgement ordered. Last month, the Commission announced its latest crackdown on Do-Not-Call violations, including six settlements and a seventh lawsuit against companies and individuals alleged to have violated the Rule. The settlements, which involved such prominent companies as Craftmatic Industries, ADT Security Services, and Ameriquest Mortgage Company, resulted in total fines of nearly $7.7 million.[37]

C. Children's Online Privacy Protection Rule

The Commission also enforces the Children's Online Privacy Protection Rule ("COPPA"), which prohibits the collection, use, or disclosure of personal information from

---

[36] *In the Matter of DirectRevenue, LLC,* FTC Docket No. C-4194 (June 29, 2007), *available at* http://www.ftc.gov/opa/2007/06/fyi07258.shtm.

[37] *See* http://www.ftc.gov/opa/2007/11/dncpress.shtm.

children under age 13 without prior parental notice and consent.[38] The Rule covers operators of child-directed websites, as well as general audience websites that have actual knowledge that they are collecting, using, or disclosing children's personal information. Since 2000, the FTC has brought eleven COPPA enforcement actions, obtaining more than $1.8 million in civil penalties.[39] In September 2006, the FTC brought a COPPA action against the popular social networking site Xanga.com, resulting in a record $1 million penalty. Additional COPPA cases are forthcoming.

D. Emerging Privacy Issues

The FTC is committed to understanding the implications of the development of technology on privacy and consumer protection. Last November, the FTC convened public hearings on the subject of *Protecting Consumers in the Next Tech-Ade*.[40] One of the issues explored at the hearings was "behavioral advertising," a practice whereby advertisers use

---

[38] 16 C.F.R. Part 312.

[39] *United States v. Xanga.com, Inc.*, No. 06-CIV-6853(SHS) (S.D.N.Y., filed Sept. 7, 2006), *available at* http://www.ftc.gov/opa/2006/09/xanga.shtm; *United States v. UMG Recordings, Inc.*, No. CV-04-1050 (C.D. Cal., filed Feb. 18, 2004), *available at* http://www.ftc.gov/opa/2004/02/bonziumg.shtm; *United States v. Bonzi Software, Inc.*, No. CV-04-1048 (C.D. Cal., filed Feb. 18. 2004), *available at* http://www.ftc.gov/opa/2004/02/bonziumg.shtm; *United States v. Mrs. Fields Famous Brands, Inc.*, No. 2:03 CV205 JTG (D. Utah, filed Feb. 27, 2003), *available at* http://www.ftc.gov/opa/2003/02/hersheyfield.shtm; *United States v. Hershey Foods Corp.*, No. 4:CV03-350 (M.D. Penn., filed Feb. 27, 2003), *available at* http://www.ftc.gov/opa/2003/02/hersheyfield.shtm; *United States v. The Ohio Art Company*, No. 02-CV-7203 (N.D. Ohio, filed Apr. 22, 2002), *available at* http://www.ftc.gov/opa/2002/04/coppaanniv.shtm; *United States v. American Popcorn Co.*, No. 02-CV-4008 (N.D. Iowa, filed Feb.14, 2002), *available at* http://www.ftc.gov/opa/2002/02/popcorn.shtm; *United States v. Lisa Frank, Inc.*, No. 01-1516-A (E.D. Va., filed Oct. 3, 2001), *available at* http://www.ftc.gov/opa/2001/10/lisafrank.shtm; *United States v. Monarch Services, Inc.*, No. AMD 01 CV 1165 (D. Md., filed Apr. 21, 2001); *United States v. Bigmailbox.com, Inc.*, No. 01-606-B (E.D. Va., filed Apr. 21, 2001); *United States v. Looksmart Ltd.*, No. 01-605-A (E.D. Va., filed Apr. 21, 2001), *available at* http://www.ftc.gov/opa/2001/04/girlslife.shtm.

[40] *See* FTC News Release, *Hearings Will Explore Emerging Technologies and Consumer Issues in the Next Decade* (July 26, 2006), *available at* http://www.ftc.gov/opa/2006/07/techade.htm.

sophisticated technology to analyze consumers' online activities and provide advertising identified as relevant to their interests. This November, the Commission held a follow-up "town hall" public meeting to examine the privacy implications of behavioral advertising in more depth.[41] Participants at this town hall discussed and debated the various costs and benefits of behavioral advertising to consumers and the business community, as well as possible government or private sector responses to the burgeoning of this type of advertising.

V. CONCLUSION

Maintaining the privacy and security of sensitive consumer data is one of the highest priorities for the Commission. In particular, identity theft remains a serious problem in our society, causing enormous harm to consumers and businesses and threatening consumer confidence in the marketplace. As new information technologies and privacy threats emerge, the Commission, through its own efforts and its participation on the Identity Theft Task Force, works to educate itself and the public about these new developments, advise businesses on their legal obligations, educate consumers to help them better protect themselves, train state and local law enforcement, assist identity theft victims, and take action against businesses that violate the law.

To succeed in the battle against identity theft, government and the private sector, working together, must make it more difficult for thieves to obtain the information they need to steal identities, and make it more difficult to misuse that information if they do obtain it. The Commission will continue and strengthen its efforts to combat identity theft and protect consumer privacy.

---

[41] *See* http://www.ftc.gov/opa/2007/10/thma.shtm

Mr. SCOTT. Thank you.

We have about 10 minutes before we have to be on the floor. So we will take your testimony, and then we will come back as soon as we can.

Ms. Napp.

TESTIMONY OF JAIMEE NAPP, EXECUTIVE DIRECTOR, IDENTITY THEFT ACTION COUNCIL OF NEBRASKA, OMAHA, NE

Ms. NAPP. Thank you, Chairman Scott and Members of the Subcommittee.

Thank you for this opportunity to share my story today and for your leadership and interest in this issue.

My name is Jaimee Napp, and I am the executive director of the Identity Theft Action Council of Nebraska, a proud mother of a 7-year-old, and I am also an identity theft victim. Today I will speak about my own personal experience and offer support for the Privacy and Cybercrime Enforcement Act of 2007 but also will provide some additional suggestions on what can be done.

I have regrets in my life, and one of them was taking a particular part-time job and handing over my Social Security number to my employer.

In May 2005, my personal information, including my name, birth date and Social Security number were stolen and used to apply for four credit cards.

The perpetrator turned out to be a manager at my former employer who stole my information from employee records. She was arrested in October of 2005 and charged with criminal impersonation, a felony, for stealing my identity. She served 5 months in county jail only because she couldn't make bail, and then she was ordered to go undergo drug treatment for methamphetamine addiction.

My perpetrator pleaded guilty on the felony charge in October of 2007 and was ordered to drug court, which is a program for nonviolent offenders with substance abuse problems. At drug court graduation in January 2008, a total of four felonies will be wiped clean from her criminal record like they never existed after only a year and a half of drug treatment.

I have lost more than a nine-digit number from a piece of paper. This number happens to be the key to my financial past, present and future, even though no one assigns monetary value to a Social Security value number.

When I became a victim of identity theft, I was not prepared for the overwhelming feeling of helplessness. And I was stunned at how quickly destruction came and how easy it was for my perpetrator to open credit cards.

What I experienced was a deep sense of loss, including the sense of who I am, my entire core belief system, friends who didn't understand what I was going through and a sense of safety.

The worry and uncertainty caused me to change my physical appearance and intensely watch for strange people or cars following me.

In April 2006, the trauma started to affect my personal life working for a different employer. Because the original theft happened in the workplace, I started to become very uncomfortable and

wasn't able to function at a normal level with my coworkers nor did I feel like I could trust management or my employer.

Shortly thereafter, the stress became too much to hide or control. It started showing itself physically through my inability to sleep and increased paranoia, cloudy vision and forgetfulness. In May 2006, I sought counseling and was officially diagnosed with post-traumatic stress disorder. I am not a victim of a violent physical crime, but I certainly feel like someone who is.

My reality is that I will never be in total control of how and when my Social Security will be used for the rest of my life. I must always have my guard up.

My story does not end with heartache. It ends with hope. I had a choice to make. I could either forget, let this crime ruin my life, or create change. And the choice was easy.

I founded a nonprofit organization in 2006 called the Identity Theft Action Council of Nebraska, and we educate consumers about identity theft and provide victim resources.

I support tougher penalties and greater victim restitution included in this bill but would also like to offer a few suggestions.

Criminal penalties and tools for law enforcement are only part of the solution. To more fully address the problem, Congress should require mandatory notification when personal information is breached and require mandatory data security requirements for business and government, and also provide consumers with affordable, easy-to-use security freeze rights.

This is the first time I have spoken publicly about the depths of my pain with my crime, and I thank you for this opportunity. But my story only represents one person out of the millions of Americans who become victims each year.

I would like to thank you again for this opportunity, and I would be happy to answer any questions.

[The prepared statement of Ms. Napp follows:]

PREPARED STATEMENT OF JAIMEE NAPP

Chairman Conyers and members of the Subcommittee, thank you for this opportunity to share my story today and for your leadership and interest in this important issue. Today I will speak about my own personal experience with identity theft, offer support for the Privacy and Cybercrime Enforcement Act of 2007 and provide additional suggestions on what can be done to prevent identity theft. I hope my words will give you a glimpse into what real people—real victims of identity theft—are facing today and the depth of their suffering.

No one actively seeks out opportunities to tell the world about the most vulnerable time in his or her life, but I speak today out of necessity. It is time for change—for new protections for victims and new tools to prevent ID theft—and time for identity theft victims to become visible to make that happen.

HOW I BECAME VICTIMIZED:

I have regrets in my life as many people do. One of them was taking a part-time job in 2004 and handing over my social security number to my employer. It is an experience no one ever dreams could change your life in such a drastic way. Unfortunately for my family and me, this choice came with consequences for which I will pay for the rest of my life. Because of this one innocent exchange of information with my employer, I became a victim of identity theft.

In May 2005 my personal information, including my name, birth date and social security number, was stolen and used to apply for four credit cards over the Internet. The perpetrator was a manager at my former employer who stole my information from employee records. I trusted my employer to keep these pieces of information safe and my employer had failed me.

The perpetrator was not working in position that should have had access to employee's personal information. But the file cabinet where my information and that of twenty-three other employees was not kept locked as corporate security policy stated it should be. My employer also failed to complete a background check on the perpetrator, something also required by corporate policy. A background check would have shown my manager's criminal record contained forgery and theft-by-deception felony arrests.

HOW I DISCOVERED THE THEFT AND WHAT HAPPENED TO THE PREPETRATOR:

I am considered lucky because I was alerted to the crime soon after it occurred. One of the credit card companies called me to verify information on the application I had submitted. There was just one problem. I never submitted an application. After many hours digging for clues on my credit reports, I found three other credit cards that had been applied for in my name.

I'm a member of a very small group of identity theft victims who have experienced the arrest and prosecution of their perpetrator. My perpetrator was arrested in October 2005 and charged with criminal impersonation—a felony—for stealing my identity. But the journey from investigation, arrest and charges was not an easy road. I had to fight everyday for seven months for someone to listen to me, pay attention to me and to acknowledge me.

There wasn't a day that I didn't want to give up and let the perpetrator win, but something kept me going. I believe the arrest and prosecution of my perpetrator only happened because of my sheer determination. Most victims give up because the feeling of helplessness is overwhelming. Identity theft victims are largely invisible to law enforcement and the judicial system. We are seen as victims of property crime and many times not seen as victims at all.

My imposter served five months in county jail before going to court and being ordered to undergo drug treatment for Methamphetamine addiction. Then for over a year and a half, I waited.

Finally in October 2007 the plea hearing for the case was held. My perpetrator pleaded guilty to felony criminal impersonation for stealing my identity and was ordered to drug court. For the past year and a half, my perpetrator was participating in the drug court program for three additional felony charges.

In January 2008, my perpetrator will graduate from drug court and all four felonies will be wiped clean from her criminal record, like they never existed. As I watch this happen, I stand before the court invisible.

IMPACT ON ME AND MY FAMILY:

On that day over two years ago I lost more than a nine-digit number from a piece of paper. No one assigns monetary value to a social security number even though it is the key to my financial past, present and future.

Identity theft feels a lot like having your home being robbed. A burglar goes through all your possessions and belongings and takes items you cannot replace. But before they leave, they steal the front door. Now what? Do you get a new door, change your locks, increase security around your home or move if you don't feel safe? As an identity theft victim none of these are options. You are helpless. Imagine what it would be like to try to sleep at night without a front door protecting your family from the night. It's a scary proposition. Your choices would be to either stand guard twenty-four hours a day or give up. Most identity theft victims give up.

I consider myself an educated woman and capable of handling a lot of what life throws at me. When I became a victim of identity theft, I was not prepared for the overwhelming feeling of helplessness. There was literally nothing I could do but watch as my strong credit score, the result of years of hard work and sacrifice for my family's future hopes and dreams, was destroyed in a matter of moments. I am a young person and what flashed before my eyes was my dream house which I didn't live in yet, trips of a lifetime I dreamed of taking with my family and my eventual retirement. I was stunned at how quickly destruction came and how easy it was for my perpetrator to execute.

What I experienced was a deep sense of loss of:

- A sense of who I am
- How I am portrayed to society
- My core belief system
- My internal intuition
- My love of hobbies
- My ability to express feelings and emotion

- Friends who didn't understand what I was going through
- My safety and security

I had no idea how much information my perpetrator and their friends knew about me, but had to assume it was everything contained in my initial job application—name, address, social security number, education, references, phone numbers, previous work experience, birth date and email. The worry and uncertainty caused me to change my physical appearance, watch for strange cars around my home, watch for people or cars following me. I even went to my local police department to request mug shots of my perpetrator's friends so I could identify them if I was attacked.

In April 2006, this trauma started to affect my professional life while I was working for a different employer. Because the original theft happened at work, I started to become very uncomfortable in the workplace. I was not able to function at a normal level with co-workers nor could I trust management and my employer.

Shortly thereafter, the stress became too much to hide or control. It started showing itself physically. They included, cloudy vision; forgetfulness; increased heart rate; increasing paranoia; agitation; and inability to sleep

In May 2006, I sought counseling and was officially diagnosed with Posttraumatic Stress Disorder—a definition adapted from the DSM-IV (American Psychiatric Association) as being exposed to a traumatic event, re-experiencing the event, persistently avoiding things or events, called triggers, associated with the trauma, persistent symptoms of physical arousal, symptoms that last more than a month. Because of these symptoms, there is significant impairment and distress in social, occupational or other important areas of functioning.

I understand this may be difficult to comprehend. I fought the diagnosis, too. I'm not a soldier returning home from war; I'm not an assault victim; and I'm not a battered woman. I'm not a victim of violent physical crime, but I feel like someone who is. What I've learned is that no one can determine how a crime victim responds to the trauma of any type of crime.

For a year I could not sleep through the night. I was awakened by every car door I heard in the street, every gust of wind and every sound of the night. I had increasing nightmares and became isolated. I numbed emotions and was paralyzed with irrational fear.

My counselor, in collaboration with another psychologist, determined that my trauma triggers and crime scene were associated with the workplace. Even though my current work place was different, certain elements were constant. I was subjected to my trauma everyday, all day and it became clear I needed a break.

My doctors determined I needed to be removed from the situation in order to learn how to cope, grieve for what I have lost, and respond to feelings in order to return as a productive worker. Their official diagnosis stated I needed three months away from work to complete this task. Because this time off could not be arranged with my employer, I left the job. Since then I have not been employed full-time by any company and my family continues to suffer from my lost wages.

Identity theft is a cycle of victimization that can last for years. I do believe I will be victimized again in my lifetime. There's nothing stopping my perpetrator from harming me again. There is no protection order I can request from law enforcement that will keep me safe. My reality is that I will never be in total control over how or when my social security number is used for the rest of my life.

For me, the damage was increased by the deliberateness of the perpetrator, whom I knew from a six-month working relationship and the indifference of law enforcement, the judicial system, my former employer, my current employer, the credit bureaus, and creditors. To be clear, I do not place blame on these entities. They appear uneducated about the harms they subject consumers to by either using lax security or by simply doing nothing at all. As I note below, more must be done to ensure that those who hold our financial futures in their hands are held accountable for their failure to meet their responsibilities.

HOW I TRANSFORMED MY EXPERIENCE:

My story does not end with heartache. It ends with hope. Early in my journey I asked myself a lot of questions. Why isn't someone helping me? Why is this so difficult? Why am I constantly being asked to step aside, given no answers or hope? I had a choice to make; either forget, let this crime ruin my life or create change. The choice was easy and actually felt as though it chose me. As I asked myself those questions, I quickly realized I couldn't wait for someone else to do something. I had to do it myself.

I founded a nonprofit organization in 2006 called the Identity Theft Action Council of Nebraska. Our mission is to educate about identity theft, provide victim resources and help shape legislation that empowers consumers. Our goals are to cre-

ate a national model on how to tackle identity theft issues and reduce its impact on victims' lives.

On this journey I have done things I have never imagined possible: traveled, met with leaders in the field and seen the difference courage to speak out can make. I have spoken to local, state and national media about identity theft.

I have testified before the Nebraska legislature and played an integral part in the passage of the first consumer-led identity theft legislation in the state that gave consumers the right to place a security freeze on their credit files—a tool that prevents creditors from checking credit files, thus preventing ID thieves from opening new accounts.

In 2007 our organization has educated over 2,000 Nebraskans about identity theft.

We have built relationships with Nebraska Attorney General, Nebraska AARP, Consumers Union and other community groups. Our organization will continue to bring to the table groups and entities that can contribute and facilitate discussions across the state on how we can best help consumers and victims.

WHAT SHOULD BE DONE ABOUT THE PROBLEM:

First, provide tougher penalties and greater victim restitution.

The Privacy and Cybercrime Enforcement Act addresses that aspect of the problem by enhancing penalties and making it easier for victims to receive restitution for out-of-pocket costs and the value of the time spent resolving the problems of ID theft. Because one of the long-term impacts of ID theft is credit score damage—the cost of which may only later be realized—I'd recommend that the Committee make clear that the time spent resolving the problems of ID theft includes time spent repairing one's credit score—a process that goes beyond just wiping errors off one's credit file. In addition, I urge the committee to ensure that the actual and potential higher cost of credit to a victim of ID theft is explicitly covered as an out of pocket cost for which restitution is available.

But criminal penalties alone cannot solve the problem of ID theft.* *Identity theft has been a federal crime for many years, but those penalties didn't deter my perpetrator. Thus, criminal penalties and tools for law enforcement are only part of the solution. To more fully address the problem, Congress should:*

- **Require business and government to notify consumers when they are at risk.*** *Congress should require mandatory consumer notification when the security of sensitive personal information held by businesses about their customers and their employees is compromised. We need to know when we are at heightened risk so we can take steps to protect ourselves. But without requirements that we be notified, businesses have every incentive to sweep any security breach incident under the carpet. Tough penalties for failure to notify should also be imposed. Your bill, while not providing for mandatory notification, at least imposes penalties on those who do not meet existing, albeit largely weak, notification requirements under state and federal law.*
- **Impose duties upon business and government to safeguard our data.*** *Congress should couple mandatory notification with mandatory requirements that private businesses and government agencies adopt new data security procedures and technologies. Doing so creates both strong incentives and real obligations for businesses to protect sensitive information to prevent any breach from occurring in the first place. Tough penalties should be imposed for failure to comply. More than likely, I wouldn't be here before you as a victim of identity theft if my employer had simply locked a file cabinet containing my social security number. Data security can be achieved through both common-sense low-tech and high-tech means, just as identity thieves use both low-tech and high-tech means to perpetrate their crimes.*
- **Provide consumers with security freeze rights.*** *Congress should also provide consumers with affordable, easy to use security freeze rights. Right now, though the rights exist in many states, the freeze is still expensive and cumbersome (consumers must submit freeze requests via mail and most states don't provide for quick thaw allowing consumers to quickly and securely lift the freeze when they want to access credit). And the voluntary freeze the credit bureaus are making available is too expensive, and it is a tool that they could withdraw at any time. Plus, they have little incentive to promote its availability because, with the freeze in place, it makes their for-profit tools, like credit monitoring, irrelevant. Yet the security freeze is the only tool we have to stop the cycle of victimization of new account theft. It is not a luxury item and shouldn't be priced as one.*

CONCLUSION:

Even though I have spoken many times about my victimization over the past two years, this is the first time I have spoken about the depth of my pain publicly. It was not easy to do. And because ID theft is a crime that rarely leaves physical marks, beyond tarnished credit records, it is not easy for those who haven't been victims to understand how deeply identity theft affects us. So I thank you for this opportunity.

My story represents just one of the approximately ten million stories of Americans who were victimized by identity theft in 2005. I join a group of roughly fifty million American who have become victims of this crime since 2003. Each victim has his or her own unique story of loss.

I applaud the committee again for your interest in the issue and urge you to move forward with your legislation. But I also urge Congress to do more. Congress must adopt tools that prevent these crimes from occurring in the first place by imposing new duties on those businesses and government agencies that hold the key to our identities in their databases and filing cabinets. Congress should go beyond criminal penalties and adopt strong protections without interfering with existing state laws regarding notice of breach, affordable, easy to use security freeze rights for all Americans and obligations for all businesses and government entities to protect sensitive data.

Thank you again for this opportunity to testify.

Mr. SCOTT. Thank you very much for your very moving testimony.

We will vote. There are three votes pending, and we will be back as soon as we can. It will probably be about 15 minutes.

[Recess.]

Mr. SCOTT. The Subcommittee will come to order.

The gentleman from California has approved starting off without the Ranking Member. So if the Ranking Member comes, he can blame it on the gentleman from California.

Thank you.

Mr. Holleyman.

TESTIMONY OF ROBERT W. HOLLEYMAN, II, PRESIDENT AND CEO, BUSINESS SOFTWARE ALLIANCE, WASHINGTON, DC

Mr. HOLLEYMAN. Mr. Chairman, Mr. Lungren, Mr. Coble, Members of the Subcommittee, I want to thank you for the opportunity to testify today. There is an urgent need to update our Federal criminal laws. And law enforcement needs new tools to find and prosecute cyber criminals.

Why does the Business Software Alliance care about this issue? Several reasons. First, it hurts our member companies' businesses. Second, it hurts the development of electronic commerce. And third, because it hurts the economy as a whole.

I want to thank you, Mr. Chairman, for calling this hearing and for the leadership you have shown in sponsoring the pending legislation, H.R. 4175. I also want to commend Congressmen Schiff, Chabot, Mr. Lungren and others for their leadership in introducing H.R. 2290 earlier this year.

Today's hearing could not come at a better time. We are in the midst of the holiday season, and Americans will spend nearly $30 billion in online shopping activity. They will be able to shop at thousands of sites, compare products, services and get prices that would have been unavailable just a few years ago because of the advances related to geography and comparative shopping that are brought about by the Internet.

At the same time, we know—studies show that many individuals are concerned about their safety when doing business online, about the risk of criminals who might be lurking in cyberspace who want to steal their identity, their financial records or more. Unfortunately, these concerns are fully justified.

The reality is that we use our computers at home and the office in ways today that were unimaginable the last time there were major revisions in the Federal criminal laws. This has led to an evolution of cybercrime, and it has changed the type of criminals.

Two big changes have occurred in computing. First is the sheer growth of the number of people using computers. The second is the fact that computers are now almost always on and connected to the Internet. This has given criminals the opportunity to create malicious code that can be sent out surreptitiously and can compromise thousands or hundreds of thousands of computers. This results in the creation of zombie computers that the criminal can then remotely control to carry out the attacks. The zombies may not themselves suffer monetary damage, but they may become an unwitting accomplice in attacking other victims of financial crimes or identity theft or denial of service.

We also see that cybercrime today is overwhelmingly fueled by profit. Criminals used to write malicious code for the bragging rights. Today they do it for the money. And that is a change.

What can Congress do about it? We believe that there is an urgent need to update our criminal laws to get law enforcement the tools they need to respond to the changing nature of the threat and the changing nature of cybercrime. We would suggest doing this in five ways.

First, targe botnets in ways that have been identified today by criminalizing cyber attacks on 10 or more computers even if they don't suffer more than $5,000 worth of damages.

Two, address new forms of cyber extortion.

Three, broaden the coverage of cybercrime laws to include computers affecting interstate and foreign commerce.

Fourth, attack organized cybercrime by creating an explicit conspiracy to commit cybercrime as an offense.

And fifth, strengthen penalties by calling for the forfeiture of computers and other equipment that are used to conduct crime and by adopting tougher sentencing guidelines.

Fortunately, there is broad congressional, law enforcement and industry support for such legislation. There are a number of pending bills, including H.R. 2290, that address these issues. Last month, the Senate adopted S. 2168, and finally, Mr. Chairman, your bill does that with the exception of the provision to target botnets, which we hope will be added to any final measure.

Of course H.R. 4175 has many other provisions, including data breach notification and privacy. BSA understands the seriousness of the problems data breaches represent. We are committed to working with this Committee and with the six other Committees who have jurisdiction over this legislation in data breach to develop a comprehensive Federal legislation. But we are very concerned that the inclusion of data breach or privacy in cybercrime legislation will delay or prevent enactment.

In conclusion, we are eager to work with this Committee. We believe the time is now, and we encourage moving forward and addressing and closing the loopholes that exist under today's cybercrime laws.

Thank you.

[The prepared statement of Mr. Holleyman follows:]

PREPARED STATEMENT OF ROBERT W. HOLLEYMAN

HOUSE JUDICIARY COMMITTEE
SUBCOMMITTEE ON CRIME, TERRORISM AND HOMELAND SECURITY

HEARING ON HR 4175
THE PRIVACY AND CYBERCRIME ENFORCEMENT ACT OF 2007

WRITTEN TESTIMONY FOR THE RECORD

ROBERT HOLLEYMAN
PRESIDENT AND CEO,
BUSINESS SOFTWARE ALLIANCE

DECEMBER 18, 2007

Thank you very much for the opportunity to testify today on the urgent need for legislation to update our criminal laws and provide law enforcement with much-needed tools to find and prosecute cyber criminals.

Mr. Chairman, Ranking Member Forbes, we greatly appreciate the interest and leadership you have shown on this issue with your recent introduction, with Chairman Conyers, Ranking Member Smith, Chairman Scott, Ranking Member Forbes, and Representatives Davis, Jackson-Lee and Sanchez, of H.R. 4175, the Privacy and Cybercrime Enforcement Act of 2007. We also want to commend Congressmen Schiff and Chabot for their leadership on HR 2290, The Cyber Security Enhancement Act of 2207, which they introduced with Committee Members Delahunt, Lungren, Davis, Goodlatte, Wexler, Issa, and Sanchez. We appreciate their continued commitment to promoting consumer trust in the internet and online transactions.

BSA is the foremost organization dedicated to promoting a safe and legal digital world. We are the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Our members represent one of the fastest growing industries in the world. BSA

programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce.[1]

This holiday season, Americans will spend as much as 30 billion dollars for their online holiday shopping. They will be able to shop at thousands of stores, compare products, services and prices, without regard to time or geography in order to find just the right gift at the right price. But while they are doing so, many will worry that criminals are lurking in cyberspace waiting to steal their money or even their identity. Unfortunately, their concerns are justified.

We urge you to act swiftly to enact cybercrime legislation. Under today's law, the ability of law enforcement officers to act against cyber-criminals is limited by gaps and ambiguities in the law. Legislation is needed to correct these deficiencies.

The nature of the threat has changed. Today's cyber criminals are more potent than ever before:

1. Cyber crime today is overwhelmingly fueled by profit. Cyber criminals used to write malicious code for bragging rights. Not anymore. Now they are drawn to cyber space for the same reason that Willie Sutton robbed banks – because that's where the money is. Cyber criminals

[1] BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, CA, Cadence Design Systems, Cisco Systems, CNC Software/Mastercam, Dell, EMC, Entrust, HP, IBM, Intel, McAfee, Microsoft, Monotype Imaging, PTC, SAP, Siemens PLM Software, SolidWorks, Sybase, Symantec, Synopsys, and The MathWorks.

attack business and financial institutions. But they also go after individuals' Social Security, credit card or bank account numbers. That information leads to identity theft and fraud and is often illegally traded online, for great profit.

2. Cyber crime is increasingly technologically sophisticated. Because cyber crime has become a profession, and because it is financially motivated, criminals have a tremendous incentive to innovate. In particular, the rise of vast, surreptitiously controlled computer networks, called "botnets," has led to an explosion in the number and types of cyber crimes committed.

For too long, cyber criminals have taken advantage of legal blind spots to brazenly threaten online confidence and security. For that reason, BSA has strongly advocated updating our cyber crime laws to meet the changing nature of the threat.

Importantly, this is an issue that Members of Congress on both sides of the aisle and on both sides of the Hill agree they can do something about and have shown that they want to take action.

There is broad congressional, law enforcement and industry support for legislation that will:

- Target botnets by criminalizing cyber attacks on 10 or more computers even if they don't suffer $5,000 worth of damages.
- Address new forms of cyber extortion where a criminal threatens to obtain information from a computer or to publicize information already obtained from a computer.
- Broaden coverage of the cyber crime laws to include computers "affecting" interstate or foreign commerce.
- Attack organized cyber crime by creating an explicit conspiracy to commit cyber crime charge
- Strengthen penalties by calling for the forfeiture of computers and other equipment used to commit cyber crime and by adopting tougher sentencing guidelines.

Earlier this year, Congressmen Schiff and Chabot introduced H.R. 2290, the Cyber Security Enhancement Act of 2007. BSA welcomed this legislation which addressed all the key issues I outlined. We would be delighted if this bill were to become law.

More recently, however, the action shifted to the Senate. On November 1st, the Judiciary Committee reported legislation introduced by Chairman Leahy and Ranking Member Specter, S. 2168, the Identity Theft Enforcement and Restitution Act of 2007. This bill also incorporated many of the provisions of a bill introduced

by Senators Hatch and Biden, S. 2213. The Senate passed this legislation **unanimously** on November 15th.

BSA applauded Senate passage of S. 2168, which covered the major areas needed for improvement that I highlighted earlier. We also would be pleased if this bill was enacted.

Most recently Mr. Chairman, you and Ranking Member Forbes and others on the Committee introduced H.R. 4175. This bill also covers the same major areas as the earlier bills, with the exception of a crucial provision to target botnets.

The legislation also has other provisions including data breach notification. BSA understands the seriousness of the problem that data breaches represent, and we are working with this Committee, and the seven other Congressional committees involved, to develop legislation. We are committed to comprehensive legislative action that increases online security, including data breach reform, but we are very concerned that inclusion of this or other provisions in a cyber crime bill will delay enactment of cyber crime legislation, on which there is substantial bicameral consensus.

In conclusion, our message is simple. Cyber criminals are not waiting to attack and we can't afford to delay. There is broad bipartisan support in the House and Senate for legislation to update our criminal laws in the areas I have summarized. We think it is vital to make these changes to our criminal laws as soon as possible. Such legislation deserves to be enacted, can be enacted and should be enacted as soon as possible.

Thank you.

Mr. SCOTT. Thank you very much.
Ms. Coney.

TESTIMONY OF LILLIE CONEY, ASSOCIATE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER, WASHINGTON, DC

Ms. CONEY. Thank you, Chairman Scott, Ranking Member Gohmert and Members of the Subcommittee for this opportunity to testify on the bill H.R. 4175, the "Privacy and Cybercrime Enforcement Act of 2007."

My name is Lillie Coney. I am associate director at the Electronic Privacy Information Center. EPIC is a nonprofit research center based here in Washington, D.C. We focus on privacy, civil liberties and constitutional values.

With me this afternoon is Jonathan David, a student at Northeastern Law School who assisted with the preparation of our statement. Our thanks go to the sponsor of the bill.

To a great degree, the lack of transparency on data breaches, computer system breaches, anomalies and software failures inhibits the ability of the government to proactively address computer network vulnerabilities and enforce privacy laws. The old saying that what you don't know won't hurt you has rarely held true, and when it relates to data breaches, it is never true.

According to the Federal Trade Commission, for the seventh year in a row, identity theft is the number one concern of American consumers. We also know that 260 million Americans have had data breaches impact them. The failings of private actors to manage the personally identifiable information entrusted to their care justify the passage of H.R. 4175.

Further, a report from the Samuelson Clinic confirms that the private sector is willing and able to act in putting in place security measures to protect computer networks that house personally identifiable information when that data—when data breaches require, under statute, notification to consumers.

We appreciate that this bill will do what the Privacy Act should have done: Include private data networks under the requirements to protect personally identifiable information. This is a key component for privacy protection afforded by fair information practices that are outlined in the Privacy Act.

The provisions of the bill do not preempt State law but rather create an important Federal baseline. As we have learned, the States can respond more quickly than the Federal Government can to emerging privacy challenges, and it is very important that the Federal Government not limit the important work of the States in this area.

The bill creates a great start on defining personally identifiable information, but more needs to be done.

We are now seeing a tremendous increase in the collection of personal information in the form of biometrics, behavioral targeting and associational information, all of which is completely unregulated.

The challenge for the Committee is to create a definition that recognizes the ever-evolving risk data collection poses to privacy.

EPIC endorses the bill language that requires technology protection measures that render the data elements indecipherable. We

note that significant data breaches have occurred because of poor security practices or circumvention of security measures, such as removal of large quantities of data records from office locations on personal portable computer devices that were subsequently lost or stolen.

Regarding the promulgation of the final privacy impact assessment, electronic records are illusive things. It may be very difficult to enforce the intent of the provisions of this statute.

For example, EPIC recently discovered in the midst of our involvement in an agency proceeding before the Federal Trade Commission regarding the proposed merger of Google and DoubleClick that the chair of the FTC's spouse's law firm, Jones Day, represents one of the parties to the merger. Upon our making a complaint requesting the recusal of the chair from participation in the commission's decision-making role on the merger request, the electronic document disappeared from the Jones Day Web site.

This phenomena of the disappearing of electronic documents is not limited to non-government Internet communications. It has also been observed by EPIC and the actions taken by Federal Government agencies when publishing documents online.

In closing, I would like to thank the Subcommittee for this opportunity speak on the record regarding the important measures set forth in H.R. 4175 and strongly endorse the efforts to address the issue of data breaches involving personally identifiable information, and the efforts of the sponsors of the bill and the Subcommittee to make more transparent the rule-making process related to privacy impact assessments.

Thank you.

[The prepared statement of Ms. Coney follows:]

PREPARED STATEMENT OF LILLIE CONEY

f

Prepared Testimony and Statement for the Record of

Lillie Coney
Associate Director, EPIC

Hearing on

H.R. 4175, the "Privacy and
Cybercrime Enforcement Act of 2007"

Before the

House Judiciary Committee
Subcommittee on Crime, Terrorism, and Homeland Security

December 18, 2007
2141 Rayburn House Office Building

Chairman Scott, Ranking Member Gohmert, and Members of the Subcommittee, thank you for this opportunity to testify on the need to improve data privacy and security, as well as make more transparent the process of federal Privacy Impact Assessment rule promulgation. My name is Lillie Coney, and I am the Associate Director of the Electronic Privacy Information Center in Washington, DC. EPIC is a non-partisan research organization that was established to focus public attention on emerging privacy and civil liberties issues.[1] With me this afternoon is Jonathan David, a student at Northeastern Law School, who has assisted with our testimony.

The old saying that "what you don't know won't hurt you" has rarely held true, and when it relates to data breaches, it is never true. According to the Federal Trade Commission, for the seventh year in a row identity theft is the number one concern of American consumers.[2] We also know that 216 million Americans have been impacted by data breaches.[3]

However, what is unknown is to what extent the lack of transparency on the part of industries, businesses, and data brokers about the full scope of data breaches frustrates the ability of the Federal government to make policy, enforce laws, and protect privacy rights of citizens. This is a far-reaching problem that effects Americans all across the country.

Background on Privacy Protection

The protection of privacy is hardly a new problem. An 1890 journal article written by American lawyers Samuel Warren and Louis Brandies entitled the "Right to Privacy," captured the attention of law scholars, legislators, and the public. This law journal article has been cited and debated for over a century, and has guided the establishment of laws and international norms that restrain the power of technology and human curiosity to encroach on an individual's "right to be let alone."[4]

In 1948, the right of privacy found a place in international law through its adoption into the Universal Declaration of Human Rights.[5] Article 12, states:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[1] Electronic Privacy Information Center (EPIC), About EPIC, available at <http://www.epic.org/epic/about.html>.
[2] Federal Trade Commission, Consumer Fraud and Identity Theft Complaint Data, January-December 2006, available at <http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf>.
[3] Privacy Rights Clearinghouse, A Chronology of Breaches, available at <http://www.privacyrights.org/ar/ChronDataBreaches.htm#3>, December 14, 2007.
[4] Samuel Warren & Louis Brandies, The Right to Privacy, 4 Harvard Law Review 193 (1890).
[5] Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 A(III) on December 10, 1948, available at <http://www.un.org/Overview/rights.html>.

The "Digital Information Age," ushered in a much-needed expansion of the fundamental human right of privacy. During the 1960s and 1970s the interest in the protection of privacy rights increased with the arrival of the information technology revolution. Congress in its wisdom acted not in the wake of disaster, but prospectively to address the real threats posed by powerful computer systems. The Federal Privacy Act established the right of citizens to be free from government abuse and misuse of personal information, and the right to be informed of the actions taken by the federal government on their behalf.

The Privacy Act of 1974 was passed in response to concerns about how the creation and use of computerized databases might impact individuals' privacy rights. However, its scope was limited to federal government agencies. It safeguards privacy of federal government-held records through the creation of four procedural and substantive rights in personal data. First, the Privacy Act requires government agencies to show an individual any records kept on him or her. Second, it requires agencies to follow certain principles, called "fair information practices," when gathering and handling personal data. Third, it places restrictions on how agencies can share an individual's data with other people and agencies. Fourth and finally, it allows individuals to sue the government for violating the provisions of the Act.

There are, however, several exceptions to the Privacy Act. For example, government agencies that are engaged in law enforcement can excuse themselves from the Act's rules. Agencies have also circumvented information sharing rules by exploiting a "routine use" exemption. In addition, the Act applies only to certain federal government agencies (except for Section 7's limits on the Social Security Number (SSN) that applies to federal, state, and local governments). Aside from Section 7, the Privacy Act does not cover state and local governments, though individual states may have their own laws regarding record keeping on individuals.

The Privacy and Cybercrime Enforcement Act of 2007

The Privacy and Cybercrime Enforcement Act of 2007 would strengthen penalties for identity theft, require notices for security breaches, and establish privacy impact assessments for federal rulemakings.[6] To a great degree, the lack of transparency on data breaches, computer system breaches, anomalies, and software failures inhibits the ability of the government to proactively address computer network vulnerabilities and enforce privacy laws.[7]

---

[6] Conyers, Smith, Scott, Forbes, Sanchez, Davis, and Jackson-Lee, H.R. 4175, the Privacy and Cybercrime Enforcement Act of 2007, November 14, 2007.
[7] Peter G. Neumann, Testimony, U.S. Senate Permanent Subcommittee on Investigations of the Senate Committee on Government Affairs, June 25, 1996.

The failings of private actors to manage the personally identifiable information entrusted to their care justify the passage of H.R. 4175. Further, a recent report from the Samuelson Clinic confirms that the private sector is willing and able to act in putting in place security measures to protect computer networks that house personally identifiable information when there are state statutes that require notice to consumers should a data breach occur.[8]

Section 102. Failure to Provide Notice of Security Breaches involving Sensitive Personally Identifiable Information

We appreciate that this bill will do what the Privacy Act should have done—include private data networks under the requirements to protect personally identifiable information. This is a key component for the privacy protections afforded by "fair information practices" that are outlined in the Privacy Act. This effort will do what the Congress should have done upon completion of the 1974 law-- include private data holders, that manage records containing personally identifiable information under the requirements to protect that information, and to disclose failures to do so.

In 2006, the largest data breach in US history was revealed when TJX Companies Inc., acknowledged that at least 45.7 million credit and debit cards were stolen by hackers who managed to penetrate its network. Another 455,000 customers who returned merchandise without receipts were robbed of their drivers' license numbers and other personal information. Also in 2006 the Department of Veterans affairs reported that the names, SSN, and dates of birth of 26.5 million U.S. veterans were on a lap top computer that was stolen from a Virginia employee's home—the computer was later recovered.[9]

The provisions of the bill do not preempt state law, but rather create an important federal baseline. As we have learned, the states can respond more quickly than the federal government to emerging privacy challenges and it is very important that the federal government not limit the important work of the states in this area. As of August 2007, according to Consumers Union, 39 states had enacted laws requiring notice regarding data security breaches involving personal information.[10]

Defining "Sensitive Personally Identifiable Information"

The bill before the Subcommittee addresses the difficult issue of defining "personally identifiable information," which is a key step in addressing the security of personally identifiable information. The names, addresses, and phone numbers of

---

[8] Samuelson Law, Technology & Public Policy Clinic, Security Breach Notification Laws: Views from Chief Security Offices, University of California-Berkeley School of Law, available at <http://www.law.berkeley.edu/clinics/samuelson/cso_study.pdf>, December 2007.
[9] EPIC & Privacy International, Privacy and Human Rights 2006., pages 23-36 (2007).
[10] Consumers Union, Notice of Security Breach State Laws, available at <http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf>, August 21, 2007.

individuals are clearly personally identifiable information and should be protected. The bill also correctly covers other types of identifiers, such as a Social Security Number (SSN), biometric identifier or drivers license number that raise particular privacy risks when linked to a person's name. In fact, many of these identifiers alone could be considered "sensitive personally identifiable information" and should be separately protected.

The bill also allows the use of the last four digits of the SSN as a means of identification. This is a reasonable safeguard that EPIC has long advocated, but it may not fully address the privacy concerns associated with the use of the SSN. The SSN is a classic example of "mission creep," where a government-designed program instituted for a specific, limited purpose has become something completely different, sometimes with disastrous results.[11]

The SSN was created in 1936 to facilitate the administration of Social Security laws, a well-intended and proven benefit to our nation. Over time, however, legislation allowed the SSN to be used for purposes unrelated to the administration of the Social Security. For example, in 1961 Congress authorized its use by the Internal Revenue Service as a taxpayer identification number.

Congress in its deliberation on the 1974 Privacy Act recognized the threats posed by abuse of the SSN and made it unlawful for a government agency to deny a right, benefit or privilege because an individual refuses to disclose his or her SSN.[12] Unfortunately, due to the abuse of the SSN by the private sector for commercial purposes, consumers are routinely threatened with denial of benefits or services should they refuse to disclose the number to non-federal government actors.[13]

In 2006, the President's ID Theft Task Force was established to "track down criminals who traffic in stolen identities and protect American families from this devastating crime."[14] EPIC participated in the Task Force proceedings and provided extensive comments.[15] The Task Force recommended the reduction of reliance on SSNs at all levels of government, and pointed the misuse of the SSN by businesses.

Pattern recognition is the Achilles Heel of any security system. The SSN has been exploited to the point that for the benefit of all - today's consumers as well as the

---

[11] Marc Rotenberg, Executive Director, EPIC, Testimony, Protecting the Privacy of the SSN from Identity Theft, available at <http://www.epic.org/privacy/ssn/idtheft_test_062107.pdf>, June 21, 2007.
[12] Privacy Act of 1974, 5 U.S.C. § 552 (a) (2006).
[13] GAO Report, Social Security Numbers: Subcommittee Questions Concerning the Use of the Number for Purposes Not Related to Social Security, <http://epic.org/privacy/ssn/gao-00-253.pdf>, July 2000
[14] Press Release, Office of the Press Secretary, Fact Sheet: The President's Identity Task Force, available at <http://www.whitehouse.gov/news/releases/2006/05/20060510-6.html>, May 10, 2006.
[15] EPIC, Comments to the Federal Identity Theft Task Force, P065410, available at <http://www.epic.org/privacy/idtheft/EPIC_FTC_ID_Theft_Comments.pdf>, January 19, 2007.

generations yet to come - the entire number should be protected, its use strictly limited by force of law.

The challenge is to create a definition for the term "personally identifiable information" that recognizes the ever-evolving risks to privacy. As written in the bill, the definition of personally identifiable information is too narrow. Identity in a cyber-enabled computer communication environment is very different from that of our physical world. A first name, last name, or first initial and last name was often the first piece of information needed to identify an individual in the pre-networked computerized world. Today, a name is not needed to identify a person with extreme accuracy.

In 2006, AOL published a list of 650,000 users' search queries on the Internet. The 20 million search terms included names, addresses, and SSNs, as well as a number of sensitive topics. Queries were listed under individual "user numbers," though users were not identified by name or screen name. Even though AOL later apologized and removed the pages with the information, subsequent copies of the data remain online. A New York Times reporter was able to successfully re-identify a user based on the search histories made available by AOL.[16]

The bill makes a good start on this challenge, but more will need to done in order to adequately protect the privacy of individuals. EPIC offers the following observations from our research on the topic of identification and identification systems, which can be found in our publication of "Privacy & Human Rights 2006: An International Survey of Privacy Laws and Developments." The critical point is that many new forms of identification are emerging and effective legislation will need to address these challenges.

New Forms of Identification and New Privacy Risks

In recent years, technology has evolved rapidly to enable electronic record creation and the construction of large commercial and state databases. The trend in technology is that computers and networked systems that contain personally identifiable information are on the rise.[17] The forms of information used to identify and track persons online can be static, such as screen names or computer-assigned Internet Protocol addresses; or dynamic, such as in the case of service-assigned Internet Protocol addresses, which can change. Dynamic Internet Protocol addresses are small software files stored on users' personal computers, with or without the users' knowledge, by web sites, web site advertisers, electronic communications, or search engine services as a means of tracking and recording online activity.[18]

---

[16] Michael Barbara and Tom Zeller Jr., A Face Is Exposed for AOL Searcher No. 4417749, New York Times, page 1, August 9, 2006

[17] EPIC and Privacy International, Privacy and Human Rights 2006, pages 23-36 (2007).

[18] EPIC, Privacy? Proposed Google/DoubleClick Deal, available at <http://www.epic.org/privacy/ftc/google/>, see also Center for Digital Democracy

The privacy and consumer rights advocacy communities are becoming increasingly aware of the threats posed by a whole host of activities based on what has been termed "micro-targeting." The amounts and types of personally identifiable information that may eventually rest in the hands of businesses because of the pervasiveness of this type of surveillance is tremendous.

EPIC has also noted a rapidly expanding use of biometrics, from the physical capture of digitized signatures of consumers at the point of sale at retail establishments to the collection of fingerprint scans or fingerprint geometry. The latter practice is being deployed in a broad spectrum of contexts, from retail customers to elementary schools.

Emerging technologies for identification of individuals include face recognition systems, hand geometry (palm prints), voice recognition systems, gait recognition (how a person moves), and DNA databases.

In addition to these areas of identification, the Subcommittee should be aware that identity can be derived from with whom we associate in our day-to-day on-line and off-line lives. Freedom of association is fundamental to our democratic experience. Social justice, environmental, religious, and political movements have their foundation in the freedom of persons who share like beliefs to associate with one another.

The deployment of Fusion Centers absent the oversight of federal government regulation or statutes to control and direct the application of surveillance is a threat to privacy and civil liberties.[19] Fusion Centers marks the emergence of an inter-networked communication infrastructure that could facilitate the creation of a modern surveillance society. The name given to the criminal justice/national security components of this endeavor are "information fusion centers." Fusion Centers are an amalgamation of commercial and public sector resources for the purpose of optimizing the collection, analysis, and sharing of information on individuals. To achieve this objective, underlying communication infrastructure must support access to identity data networks that are managed by federal and state agencies of every description as well as private sector data warehouses.[20]

Another consideration for the subcommittee's deliberation of the legislation is an especially sensitive area for victims of domestic violence who have minor children or dependents.[21] The bill considers the issue of a mother's maiden name, but EPIC would

---

<http://www.democraticmedia.org/> and US Public Interest Research Group <http://www.uspirg.org/> 2007.

[19] EPIC, Fusion Centers and Privacy, available at <http://www.epic.org/privacy/fusion/>.

[20] Lillie Coney, Testimony, DHS Privacy Advisory Committee, available at <http://www.epic.org/privacy/fusion/fusion-dhs.pdf>, September 26, 2007.

[21] EPIC, Domestic Violence and Privacy, available at <http://www.epic.org/privacy/dv/>.

strongly encourage that in the interest of privacy and security that other relationships be considered in the scope of the definition of "personally identifiable information."

For the reasons outlined above, EPIC recommends that the Subcommittee ensure routine review of the definition of personally identifiable information so that the law will remain abreast of changes as custom, technology, and the law forge new relationships that define our identity in cyberspace.

The Entire Data Record Must be Protected

EPIC endorses the bill language that requires "technology protection measures that renders the data element indecipherable."

EPIC offers the following observations and recommendations for the committee's consideration. This provision of the law should apply to the protection of all personally identifiable information in digital form. It will not matter to the victim of a data breach if the information was lost through accident, poor security practices, or mischief. We note that significant data breaches have occurred because of poor security practices or circumvention of security measures, such as removal of large quantities of data records from office locations on personal portable computer devices that were subsequently lost or stolen. Data can also be lost or stolen by insiders who abuse or misuse legitimate access to data networks or computers.[22] The miniaturization of computer storage devices is making the specter of insider abuse of information networks more pressing.[23] Computer storage devices literally the size of an adult's thumb can potentially hold thousands of records. For these reasons, EPIC recommends that the bill include language that requires the application of proven and sufficient cryptographic measures to protect and control access to personally identifiable information.

EPIC supports the language in the bill that focuses on actions of "covered obligation," because of the harm caused to consumers by data breaches. We are also in strong favor of the definition of "security breach" as defined by the bill, which encompasses "the security, confidentiality, or integrity of computerized data that there is a reason to believe has resulted in a improper access…" Further, we concur with the findings of the Samuelson Clinic's report that companies are reacting to address the problem of data breach only in the presence of state statutes that require breach notification to consumers. Finally, we recommend that the entire data record be protected with cryptographic and data access protocols that create oversight and accountability for the protection of personally identifiable information. The required reporting of data breaches to federal government agencies, coupled with the publication of breaches in the federal register are powerful tools to help consumers and the federal government define

[22] Peter G. Neumann, Computer Related RISKS, Chapter 8, A Human-Oriented Perspective, Addison-Wesley Publishing Company, 1995.
[23] Bruce Schneier, Big Risks Come in Small Packages, Wired News, available at < http://www.wired.com/politics/security/commentary/securitymatters/2006/01/70044>, January 26, 2006

the scope of the problem. Secrecy has never been a good rule for increasing security—disclosure makes the process of addressing computer security vulnerabilities viable.[24]

Ownership of Personally Identifiable Information

We are our data—a cyber-based economy will mean that our lives are judged by the sum total of personal information that is collected, stored, maintained, and shared among commercial data holders. The bill's "Obligations to Report" identifies the "person who owns or possesses data" as the responsible party. EPIC recommends that the focus should not be limited to ownership, but should extend applicability of the statute to anyone who "has custody" of personally identifiable information. This approach will leave in play state statutes or federal protections that exist to aid consumers or states, where data breaches protection laws are enacted.[25]

Today there are product offerings that provide data storage options that move repositories for business, and personal information from the business or home computer to host computer sites that provide storage and processing services.[26] In addition, social networking sites are proving to be attractive to individuals as a means of communicating with others, but it is also creating a wealth of information on the private lives of users.[27] Social networking web sites, such as MySpace, Facebook, and Friendster have become established forums for keeping in contact with old acquaintances and for meeting new ones. Users can create their own web page and post details about themselves: where they went to school, their favorite movie titles, and their relationship status. They can link to friends on the same site, whose photos, names, and perhaps a brief description, will also appear on the webpage. While these websites are useful tools for exchanging information, there has been growing concern over breaches in privacy caused by these social networking services.

E-mail services, such as Google's Gmail, provide what is described as "free" email and large storage capacity in exchange for the ability to enable auto-text reading of customers and incoming and outgoing e-mail communications and serving ads based on the content of messages. The privacy of Gmail subscribers is definitely an issue, and for e-mail senders to Gmail subscribers the reading of e-communication should be prohibited. The communications involved can be private personal matters, business or organization plans, or deliberations on a sensitive business or policy discussion. How this e-mail system might be used is open for discussion, but what should be very clear is that the communication content of these messages includes personally identifiable information.

---

[24] RISKS Digest, Dodger, The, Visabilities viable. Cyber-terrorists blackmail banks and financial institutions, available at <http://catless.ncl.ac.uk/Risks/18.17.html#subj6.1>, June 2, 2006
[25] Consumer Reports, Notice of Security Breach State Laws, August 21, 2007.
[26] Computer Storage Services, available at <http://www.computerstorageservices.com/>, December 2007.
[27] EPIC, Social Networking Web Sites, available at <http://www.epic.org/privacy/socialnet/default.html>.

EPIC recommends that the bill respect the copyright and personal privacy of users who are customers of third party services that host personally identifiable information created by their users.

Title II – Non-Criminal Privacy Enforcement and Privacy Impact Statements

EPIC is very pleased with the bill's language found in Section 202, that describes coordination of state and federal efforts, except in cases where the state attorney general determines that it is not feasible to provide notice to the US Attorney General when filing of an action. The bill does allow for the US Attorney General to stay any non-Federal action under section 201 pending the resolution of a pending federal case under section 201 of this title.

It is the experience of privacy and consumer advocates that the States play a vital role in identifying and addressing threats to consumer right, often more quickly than the federal government. As a rule, the federal government should establish a floor in the areas of privacy and consumer protection, which act as a complement in facilitating the States' vital function in these areas of law.

Section 203. Requirement that Agency Rulemaking take into Consideration Impacts on Individual Privacy

EPIC is very supportive of the bill language regarding Privacy Impact Assessments and rulemaking. The stress on greater and statutorily defined obligations to provide transparency on the rulemaking process related to Privacy Impact Assessment requirements is important for the following reasons:

First, the language of the bill is explicit: "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 Untied States, and such rule or proposed rulemaking pertains to the collection, maintenance, use, or disclosure of personally identifiable information for 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."

Second, transparency is a key component of a functioning healthy democracy. It can be translated into public policy decisions that allow citizens, policymakers, and the media to assure themselves that a local, state or federal government agency is functioning as intended.[28] This title of the bill will serve the purposes of checking the authority

[28] EPIC, Litigation Under the Federal Open Government Laws (FOIA) 2006, web page, available at <http://www.epic.org/bookstore/foia2006/>.

exercised by federal government agencies as it relates to privacy rights. The section also creates a necessary bridge between the enforcement of several Federal statutes with complementary purposes—the Privacy Act, Freedom of Information Act, the E-government Act.

Finally, the language will remove ambiguity that may currently exist in the minds of agency administrators regarding their obligations to make public information related to privacy impact assessments. EPIC filed a court challenge to an attempt by the Transportation Security Administration to withhold a Privacy Impact Assessment from the public, which was in violation of federal law.[29] EPIC requested the Privacy Impact Assessments from the TSA under the Freedom of Information Act, and received heavily redacted documents from the agency in its reply.[30] EPIC sued the agency for full disclosure of the documents as required by the E-Government Act. The TSA argued that the Federal Privacy Act and the E-Government Act, which requires publication of Privacy Impact Assessments, were segregated.

EPIC is pleased to see the language of Section 553 (2) (A) because it is the heart of our nation's Federal Privacy Act. The bill embodies the much-awaited linking of the protections of the fair information practices provisions outlined in the Federal Privacy Act to the E-Government Act. Privacy rights and privacy impact assessments are made whole by creating a level playing field regarding the collection and use of personally identifiable information. The requirements that privacy impact assessments measure and report on whether an individual is informed by a federal government agency at the time of collection of personally identifiable information that it is occurring, allowing persons access to such information, preventing the use of the information collected for one purpose to be used for another, requiring securing of the information, and in the event of compromise notice to consumers with 14 days of the date of compromise, will be the most important accomplishment of this statute should become law.

EPIC strongly endorses section 553a guidance on the agency ruling making process as it relates to public notice of work related to Privacy Impact Assessments.[31] The requirement for a senior agency official to sign the final document will improve accountability and transparency on the agencies privacy impact assessment process.

Notice of proposed rulemaking is the key to the public's fuller understanding of what the privacy consequences might be for agency actions that impact personally identifiable information. The language found in Section 553a better serves the public comment process on matters related to privacy.

---

[29] EPIC v. US Transportation Security Administration, Civil Action No. 03-1846 (CKK), available at <http://www.epic.org/privacy/airtravel/pia_order.pdf>, August 2, 2004.
[30] EPIC, Alert e-Newsletter, Volume 11.18, available at <http://legalminds.lp.findlaw.com/list/epic-news/msg00164.html>, September 24, 2004 .
[31] Conyers, Smith, Scott, Forbes, Sanchez, Davis, Jackson-Lee, H.R. 4175, Section 203, November 14, 2007.

Regarding the "Final Privacy Impact Assessment," EPIC offers the following observations and recommendations to the Subcommittee. Electronic records are very elusive things—it may be very difficult to enforce the intent of the provisions of this law without taking steps to ensure that there is transparency in the publication of e-documents that are only available via the Internet or its equivalent. For example, EPIC recently discovered in the midst of our involvement in an agency proceeding before the Federal Trade Commission regarding the proposed merger of Google and DoubleClick that the Chair of the FTC's spouse's law firm Jones Day had one of the parties to the merger as a client.[32] The relationship was discovered because of a document posted on the Jones Day web site. The Jones Day web page referenced the European Parliaments and the US Federal Trade Commission proceedings on the merger request by Google and DoubleClick. Needless to say, we were surprised to discover this relationship last Monday, December 10, 2007, and upon our review and analysis determined that it had not been disclosed during the agencies proceedings on the matter.

Upon our making a complaint requesting the recusal of the Chair from participation in the Commission's decision making role on the merger request—the e-document disappeared from the Jones Day web site. EPIC has the original e-document through no help of the Federal Trade Commission or Jones Day.[33] This is a serious matter and one that we hope that Congressional Oversight and Judiciary Committees will take under consideration. The two issues are fairness and transparency in agency proceedings where the stakes are high and the interest in the billions of dollars. Agency rulemaking, like the rule of law under court proceedings, must be without blemish.

This phenomenon of the disappearing e-document is not limited to non-government Internet publications; it has also been observed by EPIC in the actions taken by federal government agencies when publishing documents online. For example, the Election Assistance Commission, after voting on December 13, 2005 in a public proceeding to adopt new voting systems standards, posted the final document online. However, by March 2006 the document initially posted by the agency had been replaced by another version. The new version of the final guidance on voluntary voting systems standards had substantial changes to key areas of the final reported document. EPIC's voting project identified the document switch, and raised questions regarding the lack of transparency on the agency's part in not reflecting on the record the withdrawal of the version passed in December 2005 and its replacement with another document.[34] The

[32] EPIC, Privacy? Proposed Google-DoubleClick Deal, available at <http://www.epic.org/privacy/ftc/google/>, 2007.
[33] EPIC, Recusal of Chair of the Federal Trade Commission in the Merger review for Google-DoubleClick Merger Request, see original motion available at <http://www.epic.org/privacy/ftc/google/recusal_121207.pdf> and the new filing available at <http://www.epic.org/privacy/ftc/google/recusal2_121307.pdf>.
[34] EPIC's Project the National Committee for Voting Integrity, documents, Security section Dec. 13, 2005 version, available at <http://votingintegrity.org/pdf/security-121305.pdf> and the Security section published on line sometime is early 2006, available at <http://votingintegrity.org/pdf/security-011206.pdf>.

highly controversial issue of electronic voting security coupled with public scrutiny of the process of standards development is an important indication that the oversight authority of the Congress should strictly enforce agency rule promulgation in electronic online formats.

EPIC is very supportive of the language in the promulgation of agency analysis, as it is very helpful to the cause of openness in federal government actions related to privacy rights.

In addition to the measures outlined in section 553 of the bill, EPIC recommends that the entire Privacy Impact Assessment announcements of public comment periods, final documents, agency analysis, and changes to documents be published in the federal register. We further recommend that version control measures be enforced on any electronic publication of these documents.

Version control is a process developed by software engineers to keep track of multiple versions of documents in electronic form. Often, subsequent iterations of a document may appear to be very much the same, but in fact have minor or major differences. The adoption of version numbers, date and time stamps, and making available past versions (linked from the current e-version of the document), a change document (reflecting all changes made in the new version), and requiring that any update, or upgrades to web pages ensure that old link addresses for documents once made public remain in working order should go a long way in protecting the integrity and efficacy of laws to ensure transparency in rulemaking related to privacy impact assessments.

EPIC would caution that Section 553 (c) Waivers might offer opportunities for avoidance of compliance with the law. We note agencies' designation of broad "routine use" provisions that frustrate the intent of the Federal Privacy Act. If there is a pressing need for an agency to act without first conducting a privacy impact assessment due to some unforeseen or emergency situation, or if the rule is considered classified and only reported to oversight committees, thus requiring a reassessment under Section 553 (e), the period of reconsideration should be every 3 years until the provisions of 553 (a) are enforced.

Further, the collection of public comments is at least as important as the agency's internal decision making processes. EPIC and a coalition of organizations under the umbrella of the Privacy Coalition led a public comment campaign during the Department of Homeland Security's REAL ID rulemaking process.[35] Typically, the Federal agency comment process is so cumbersome and convoluted that if non-government groups had not invested so much time and resources on the issue of stopping REAL ID, promoting a grassroots public comment campaign would have been out of the question. Electronic

[35] Bruce Schneier, Schneier on Security Blog, REAL ID Action Required Now, available at <http://www.schneier.com/blog/archives/2007/05/real_id_action.html>.

access to the comment process should be easy for the average person to engage. The irony was that despite the difficulty of engaging the public comment process on REAL ID, the demand for access to the public comment process exceeded the agency's ability to manage the volume. In the last hours of the comment period on REAL ID the Department of Homeland Security's fax reception of comments was overtaxed, necessitating the addition of an e-mail option for comments to be sent. At the close of the effort over 10,000 persons successfully overcame the obstacles during the REAL ID public comment period.[36]

EPIC recommends that the bill stress access and usability features of the public comment process to enhance the effectiveness of the effort for gaining a true sense of the public sentiments regarding the privacy implications of Federal agency proposed actions. E-mail, faxes, webpage comment based systems should not be too complicated or require specialized knowledge to use. Several Privacy Coalition partners in the REAL ID Public Comment Campaign worked to make the process simple and accessible with great success.[37] EPIC also believes that all comments submitted during agency rulemaking public comment periods should be made available and accessible online, and should be available to the public at no cost.

Private Right of Action

Finally the private right of action afforded to those who object to the final rule promulgated by the action is very important for judicial oversight of an agency's decision making authority. The rules for the right of judicial review make it very important that the public notice provisions of the law rises to the level of "effective public notice." There should be great care taken to be sure that interested parties will have every opportunity to be made aware of the agency actions related to privacy impact assessments. For this reason, EPIC recommends that publication of the final rule should be in the physically published federal register in addition to any other electronic means available to the agency.

EPIC recommends that as an added incentive to agencies not to amend or change election documents on the final rules for privacy impact assessments that the date of a one-year limit can be adjusted accordingly should the agency's online version of the rule be altered, changed, become unavailable (that the time on the period to seek judicial remedy be extended by the exact amount of time that the e-version of document is not available to the public).

Conclusion

---

[36] Privacy Coalition, REAL ID Public Comment Campaign, available at <http://www.privacycoalition.org/stoprealid/#action> May 2007.
[37] Privacy Coalition, REAL ID Public Comment Campaign, available at <http://www.privacycoalition.org/stoprealid/#action> May 2007.

In closing I would like to thank the Subcommittee for this opportunity to speak on the record regarding the important measures set forth in H.R. 4175, and strongly endorse the effort to address the issue of data breaches involving personally identifiable information and the efforts of the sponsors of the bill and the Subcommittee to make more transparent the rulemaking process related to Privacy Impact Assessments.

Security breaches and identity theft are serious problems in the United States. Although we fully recognize the benefits of new technology, more must be done to address the problems when technology breaks down or creates new risk to persona privacy. The Privacy and Cybercrime Enforcement Act of 2007 contains many important provisions that begin to address this problem.

I would be pleased to answer your questions.

Mr. SCOTT. Thank you very much.

We will now have questions from the Members, and I will recognize myself for 5 minutes at this time.

Mr. Lourie, Mr. Magaw, the Identify Theft Penalty Enhancement Act included $10 million authorized to track down identity thieves. What have you done with the money?

Mr. LOURIE. We have been actively pursuing identity theft cases around the country, Chairman Scott. In the last—between 2005 and 2006, identity theft cases alone increased about 22 or 23 percent from 1,500 and change to 1,900 and change.

Many of those were under the aggravated identity fraud statute. Those numbers increased from 226 in 2005 to 507 in 2006.

In addition, there are—the Secret Service and the FBI have been establishing task forces all over the country joining together with their Federal colleagues as well as local law enforcement and State law enforcement to attack identity crime at a local level and to ensure that as few of these cases as possible slip through the cracks.

Mr. SCOTT. So you are putting the $10 million to good use?

Mr. LOURIE. Yes.

Mr. SCOTT. Did you run out of money?

Mr. LOURIE. I don't know if we did, but I can get back to you.

Mr. SCOTT. Well, if you are tracking down cases with the money, do you have enough? When one of the bills, the $10 million came out of, the original bill had $100 million, and we were told by the Administration they didn't need any money so we just left it $10 million; $10 million we got left. It seems to me that this ought to be a high priority, and I think the Committee—maybe, I can't speak for the Committee—but I would be willing to put some more authority so that you could track down more thieves so that people will get the idea that they might get caught.

Have you used up all of the $10 million so we might consider increasing the authorization?

Mr. LOURIE. As I sit here today, I can't tell you whether or not we have used up all of the $10 million, and I would be happy to work with the Committee and get back to you on that.

Mr. SCOTT. If you have limited funds, you have to make decisions. You have the $5,000 threshold. Anybody stealing less than $5,000 is pretty much home free. What would it—how much would it take to get cases under $5,000 also on your target list?

Mr. LOURIE. Well, I can't tell you how much it would take with respect to money, if that is your question, for prosecution offices, U.S. Attorneys' Offices around the country to lower their thresholds or if the Department would support that.

I can tell you that we have used the money that we have had to create these regional task forces to work together closely with the State prosecutors' offices and State law enforcement, and train them in the investigation and prosecution of these types of crimes.

Mr. SCOTT. The problem with these cases, they are, in fact, labor intensive because there is a lot of work that needs to be done. And the information is there, but some of it might include, when you find out that somebody with a stolen credit card has it delivered to a post office box, you may have to have somebody sit out there until they come and pick it up. You have to pay for that. That is an hourly rate.

So that many of these cases can be solved if you just had the resources, and so we will work together to find out what resources you may need to lower the threshold, so if somebody gets the information, they may feel they have—they are at risk of actually getting caught.

Now if a database is breached, is the mere possession of the database a crime?

Mr. LOURIE. It depends if it is knowing. If a database is breached and somebody extracts the information, then, yes. If it is unauthorized extraction, it is a crime.

Mr. SCOTT. Is buying a Social Security number from somebody a crime before you actually—without using it——

Mr. LOURIE. I don't have the statutes in front of me, but I believe under title 42, the Social Security statute, that that possession, if it is with intent to commit fraud, would be a crime.

Mr. SCOTT. But mere position, if you buy a Social Security number and that is all you have got, you don't know what they are going to do with it?

Mr. LOURIE. Well, it is fairly easy to prove that somebody who buys somebody else's Social Security number intends to commit fraud with it.

But the answer to your question is, yes; if you could not prove that element, then you would not be able to satisfy the statute.

Mr. SCOTT. Is phishing a crime?

Mr. LOURIE. Phishing is a crime if it violates one of the statutes set forth in 1030, the elements.

Mr. SCOTT. Do we need to make it clear that phishing is in fact a crime?

Mr. LOURIE. No, Chairman Scott. I don't think it is necessary—it is necessary to change the language of the bill the way you have it now to indicate that phishing itself is a crime. The language set forth in the bill is adequate to capture those types of scams with the suggestions that we have set forth here today.

Mr. SCOTT. Several people have mentioned whether or not just putting a cookie on somebody's computer where you can extract information without so-called damaging the computer, is that not trespassing or some crime, unauthorized placing of one of those cookies in somebody's computer so that you can get information? Isn't that some kind of crime?

Mr. LOURIE. Well, what I would like to do is go back and get back to the Committee on that question.

Certainly it sounds like a variation of a botnet the way you asked that question. But there are, depending on the way you analyzed the statute and the various elements of the statute, the intent of the person who puts it there is significant.

Mr. SCOTT. I have heard the suggestion that it ought to be a crime if you do it to 10 computers. Is there any reason why if you do it to one computer, why that shouldn't be a crime?

Mr. LOURIE. It may very well be a crime under various State statutes. What we are attempting to do is bring more crimes within the purview of the Federal statute, not less.

Mr. SCOTT. So we will be working together on that.

The gentleman from Texas.

Mr. GOHMERT. Thank you, Mr. Chairman.

Appreciate your testimony and appreciate your patience.

Just so I am clear on the BSA's position,

does BSA support a new Federal law that would require businesses to report or to notify consumers every time a security breach occurs?

Mr. HOLLEYMAN. We support the concept of a comprehensive Federal data breach bill that would address the issue of businesses notifying consumers when there is a significant or major breach that occurs.

Mr. GOHMERT. My question is not whether we should have a comprehensive bill that addresses that but whether you support actually requiring businesses to notify consumers when the breaches occur.

Mr. HOLLEYMAN. We support notification to consumers under a properly crafted definition of what a significant breach is with other key components. For example, as one of my colleagues on the panel spoke of, if information is encrypted or redacted or otherwise stored in such a fashion that it is not accessible when it is breached, there shouldn't be an obligation to notify.

We also believe that there are a number of other important provisions in an overall data security bill. That is simply one element of a number of provisions we would like to see.

Mr. GOHMERT. Ms. Napp, we appreciate your coming forward. Apparently, we may not even know how many people have actually been adversely harmed as you have. And you mentioned that the perpetrator against you was going to have their record wiped clean after a year and a half of drug treatment apparently.

So let me ask. I know there have been laws, like in Texas where people have become so outraged about driving while intoxicated or driving under the influence, depending on what your State calls it, or negligent infliction of harm through driving while intoxicated, and people became outraged enough they said, okay, let us have a law. No more deferred adjudication. If you commit this, it ought to be on your record for good and you can't come out from under it.

By bringing that up, are you actually urging the possibility, at least in the Federal realm as far as we can, end deferred adjudication where it has to be on someone's record?

Ms. NAPP. I was referring to my case as it stands and what is happening to me.

Mr. GOHMERT. But I am asking. You were adversely affected. What do you think?

Ms. NAPP. I personally don't think, you know, something like this—I think it has to do with identity theft victims in general. A lot of the time in the judicial system, we are not seen as victims of a crime a lot of times. And in my case, I don't believe that I was seen as a victim when the judge at the plea hearing—he felt like a restitution hearing wouldn't be needed because, how could I possibly have any type of out-of-pocket costs, and that comment to me says, I don't see you.

Mr. GOHMERT. Obviously the judge didn't understand the crime. But it seems to me that as we contemplate this crime, what is a crime, that it brings to mind some of the lessons we learned in law school about crimes of moral turpitude, and in society, we think

those are more serious crimes because they involved a *mens rea*. They involved an intent.

You brought up intent a lot of times. It seems to me that this ought to be one of those crimes that if you break into somebody's computer, if you get their private information, then regardless of what the intent is, you know, the res ipsa loquitur ought to apply; the thing speaks for itself. You have the intent and take that intentional aspect out of the proof that you have to put on.

So think about it. It involves lying. It involves fraud. It involves theft. In some cases, like when recently a week or so ago, it involved burglary to break in and put stuff on a computer so you could track what they were doing.

So I think this hearing is a great thing, and I do think we need to make this bill as tough as possible so that America understands how serious this crime is.

I would like to ask. I note, Ms. Napp, you recommended requiring mandatory notification when data is breached.

Let me ask you all. Who among the witnesses has actually read this bill that we are here about today? Anybody? Wow. All of you.

Well, I see my red light is on.

I would like to ask specifically if you could quickly say if you have any specific provisions that you would like to see changed so we could make note of them and try to improve the legislation.

Mr. Lourie, starting with you. If you have got a long list there, I would like to hear the list.

Mr. LOURIE. Thank you, Congressman.

Our recommendation and request would be to modify Section 1030(a)5 regarding damage to computers, as we spoke about before, to add language that would make it a felony if the conduct affected 10 or more computers, and also to make it a misdemeanor for damage under $5,000.

We would recommend modifications to Section 1028 and 1028(a) to define persons to include corporations so that the stealing of identity of a corporation often used in phishing schemes would also be a crime under 1028.

We would also add certain crimes to the list that would be predicates for the aggravated felony under 1028(a), and we provided those in our papers.

We would ask for a modification to 1030(a)7, which is the extortion statute, to enable that statute to reach threats to do—to release—for example, to release information that had already been stolen.

The way that the statute is drafted now, it covers threats to do damage but not necessarily threats related to damage already done.

So we believe that the statute needs a little bit of tweaking there.

We have some suggestions for the forfeiture section to include real property and to change the language in one of the prongs from proceeds to gross proceeds.

And, finally, and perhaps most significantly, we request changes or directives to the sentencing commission to focus not just on the sentences in general but certain specifics which would include defining a victim as not just somebody who suffers monetary loss but

somebody who suffers an invasion of privacy. And that relates to some of the topics that have already been discussed in this hearing today. And in any event, it is hard to value information stolen.

Finally, with respect to the sentencing commission, we would request that they be directed to look into the aggravating factors that are already there or the enhancements that are already in the statute, that they be accumulated instead of now, applying whether they are the greatest of, is the language that is now used.

We would also suggest an enhancement that the sentencing commission look at whether there should be an enhancement for disclosure of information stolen, because it is a separate harm and in some senses maybe even a more significant harm once information is stolen to disclose it, depending on how many people it is disclosed to.

Thank you for that opportunity.

Mr. GOHMERT. We have got five more, and I don't want to exceed my time that much. If I could ask the witnesses if you could submit in writing any suggestions for changes to the legislation, that would be greatly appreciated. And that would include all of you, including, Mr. Lourie, if you think of anything else. But thank you so much.

Mr. SCOTT. The gentleman from North Carolina.

Mr. COBLE. We appreciate you all being here.

Mr. Holleyman, you responded to Mr. Gohmert's question regarding notifying consumers under a properly crafted statute. Would you also require—support the requirement that business notify law enforcement?

Mr. HOLLEYMAN. Mr. Coble, I appreciate your follow-up question on that.

The answer is yes. We would support the requirement that businesses notify law enforcement when there is a breach, and I think there is probably great clarity in terms of our support for that.

Again, it is with the caveat that the requirement it needs to define what a significant breach is. It needs to ensure that there is not notification if it is unnecessary, but the principle is worthwhile. We would hope that is addressed as part of a comprehensive breach bill.

Mr. COBLE. Thank you, sir.

Mr. Winston, what steps does the FTC take to make sure that businesses adequately protect personal information from identity thefts.

Mr. WINSTON. We go about this in several ways, beginning with law enforcement. As I mentioned in my testimony, we have brought 15 law enforcement cases now against companies that failed to reasonably protect consumer data, in most cases leading to a data breach.

And in addition to law enforcement, we also do a lot of consumer and business education and outreach. We have published educational materials. We are going to be holding regional seminars for businesses so that they understand what their obligations are and they understand what the consequences are if they don't meet their obligations.

Mr. COBLE. Thank you, sir.

Are laws, Mr. Winston, requiring protection of personal information limited to certain industries or certain sectors, such as banking or other financial industries?

Mr. WINSTON. Yes, that is correct. There are a number of data security laws that apply to different kinds of data or different kinds of industries. The financial services industry is one; the health care industry is another.

As part of the Identity Theft Task Force recommendations, we have supported a national data security law that would apply across the board to any business that maintains personal information. We think that there should be one rule.

Mr. COBLE. Thank you, sir.

Ms. Napp, how can we assist in improving restitution for identity theft victims?

Ms. NAPP. Thank you, sir, for that question.

I think what you are doing with allowing victims to count their time is very important. I think this is the first time that we have actually seen some of that, because time is so much of what we deal with.

Mr. COBLE. Now, fortunately I have never been a victim. How does one fairly and, if possible, easily restore one's credit record after having been a victim?

Ms. NAPP. That one is—each——

Mr. COBLE. It probably can't be done easily.

Ms. NAPP. In my opinion, it is difficult. There are barriers and things. And each person's victimization is different, but the journey is not an easy one, I can tell you that.

Mr. COBLE. Well, again, thank you all for being here.

Mr. Chairman, note that I am yielding back before the red light illuminates.

Mr. SCOTT. That is very kind of you, Mr. Coble.

The gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman. I didn't know whether the Ranking Member needed more time for his questions.

Mr. SCOTT. That is between you and the Ranking Member.

Mr. GOHMERT. Thank you for yielding.

Mr. LUNGREN. Well, it must be a Texas thing.

Representative of the Justice Department and also the gentleman representing the FTC, I am concerned about this whole area, particularly, of identity theft. And if we enact legislation, I would like to ensure that it actually works.

And one of the things that strikes me on the bill that we have before us is that it acts a little differently than some other laws that I am aware of, which is that when the Congress preempts State law, it then gives the State AGs the authority to assist in the enforcement of Federal statutes.

This bill as drafted, as I understand it, allows that, but does no preemption at all. Is that unusual in law, in your experience, or is that something that we see somewhere else?

Mr. LOURIE. Well, with respect to our experience, I would be happy to get back to the Committee on other areas where we have seen this.

I will note that in the Task Force's strategic report, which is co-chaired by the Department, they did recommend that type of preemption.

Mr. LUNGREN. See, my concern is we are creating a lot of criminalization of activity on a Federal level, and yet I wonder whether we have the resources to follow through with it truly. And, therefore, is this really an attempt to create a Federal statute of criminal sanctions, but with the expectation that it will truly be enforced by the States instead of the Feds? And if we are going to do that, we ought to know about that.

But it seems to me a little different than we've done before. And maybe I am wrong. Maybe there are other areas of the law. Maybe the gentleman from the FTC can help me on this.

Mr. WINSTON. As Mr. Lourie said, the Identity Theft Task Force, in some of its recommendations, particularly with regard to——

Mr. LUNGREN. Look, I understand they may have suggestions. I am asking, is this a precedent or is this something that we have found in other areas of the law? That is what I am trying to figure out.

Mr. WINSTON. I think there are a number of laws that provide for Federal preemption but allow for State attorney general enforcement. The Fair Credit Reporting Act is one. So that model is, I think, not uncommon.

Mr. LUNGREN. Where we have no preemption here, but still extending that.

Mr. WINSTON. Well, that I am not sure about. I know there are——

Mr. LUNGREN. Okay. That is what I am trying to figure out. If you can help me in looking at that and submitting that for the record.

Title 2 of the legislation authorizes a civil action with civil penalties up to $500,000 or a million dollars if it is intentional from any business entity that—it says, "from any business entity that engages in conduct that constitutes a violation of Federal law relating to data security."

If you have had a chance to look at the bill, do you think that limits it to for-profit entities only, or would that be not-for-profit as well? And how would you look at it from the Justice Department standpoint?

Mr. LOURIE. I am appearing here as a member of the Criminal Division, so I did not scrub the civil sections of the bill. But we would be happy to review that and get back to you on our opinions about whether or not it would cover both those types of entities.

Mr. LUNGREN. Okay. I am trying to sort of figure out where we are here. Because I want a statute that works, but I also want one that doesn't just sit on the books and we think it is going to work. Or, frankly, if we pass Federal laws that are primarily being enforced by Federal authorities, to me that is extremely important, but it is more difficult for us to have oversight if what we are doing is passing Federal laws that are going to be absolutely, if not exclusively—or primarily, if not exclusively, prosecuted at the State level. And I wonder if there are implications with respect to constitutional authority in that.

The way I read the bill—I would ask you if this seems to make sense, because we can certainly change it—it looks like it provides an across-the-board maximum penalty of 20 years for all violations of Section 1030 of title 18.

Now, unless I missed something, that could be interpreted as meaning that failure to notify breaches would carry a harsher penalty for the businesses than for the ID thieves themselves. To me, that doesn't sound like a proper priority. Would you agree with that, or is that something that you think makes sense?

Mr. LOURIE. I believe the way the bill was drafted, it provides for a 5-year penalty, maximum penalty, for the failure to notify.

Mr. LUNGREN. So your answer is, that is what you would want, rather than the way I thought it was written.

I have a lot more questions, but I would like to respect my time limits and would yield back.

Mr. SCOTT. That is a novel concept on this Subcommittee, but thank you.

The gentleman from Ohio.

Mr. CHABOT. I thank the gentleman for yielding.

Mr. Holleyman, news reports indicate that crimes committed via computers are becoming increasingly prevalent, and I know that is what we have been discussing today, with as many as 10 million computers falling victim to hackers. FBI Director Mueller is quoted as saying that, quote, "Botnets are the weapon of choice for cyber criminals," unquote.

How urgent is it that we pass cybercrime legislation? And can we afford to wait on cybercrime legislation while we address other problems with Internet security?

Mr. HOLLEYMAN. Mr. Chabot, thank you for that question.

I think that it is imperative and urgent to pass cybercrime legislation. I think there is broad agreement in both houses of Congress and across the aisle in terms of what loopholes need to be closed.

Your question is correct, the growth in botnets is an enormous problem. And that is bringing law-abiding citizens unwittingly into a process in which their computers are being hijacked and used to perpetrate crimes. It may slow down their computer, it may be a nuisance for them, but they don't otherwise know what is happening. And we should not insist that law enforcement be required to show that there is $5,000 worth of damage to take action in that case.

So we believe the problem is immediate, and is growing. There is a solution, and we hope the Congress moves quickly on this.

Mr. CHABOT. Thank you.

And are legislative efforts enough? And what can consumers and businesses do to protect themselves to minimize the threat of cybercrime?

Mr. HOLLEYMAN. Legislation is a key part, but it is not, by itself, the sole solution. There are public awareness activities that are under way through the FTC and other agencies to build awareness of cybercrime. There are private-sector efforts to provide checklists to business owners of the type of security products they need to deploy and security procedures.

And finally, there are joint partnerships between industry and law enforcement. The National Cyber Forensic Training Alliance in

Pittsburgh is just such an organization. BSA supports it, as do many in the industry. They collect data on cybercrime, share that information with law enforcement, and assist with investigations.

So it takes a combined effort, of which legislation is only one component, but it is an essential component.

Mr. CHABOT. Thank you very much.

And, Mr. Chairman, as my colleague from North Carolina did, I would be happy to yield back my time at this time in the interest of the rest of the Committee. I could divide it between the gentleman from Texas and the gentleman from California here, but I think I will just yield back.

Mr. SCOTT. Well, we will see.

The gentlelady from Texas.

Mr. JACKSON LEE. Thank you very much, Mr. Chairman.

Let me thank you, Mr. Conyers, and the other cosponsors for moving forward on what will continue to grow to be, maybe in some eyes, an insurmountable problem as we become more technological and the sophistication of the technology that we use becomes more finite, certainly, and more broadly utilized.

It seems that privacy in the midst of innovation is a stepchild. And I think that the Congress has a duty to ensure, as the ninth amendment instructed us to do, to not forget privacy but also the abuse of too much information, identity theft and otherwise. With the good comes the bad; with the benefit comes the burden.

And so, Mr. Magaw, as it relates to the potential crime that may come about through the misuse of this technology, cyber security, my question would be the ability and the need, if you will, to ensure coordination between all levels of law enforcement, even if you are speaking of, for example, in Houston, Texas, what we call layered police work.

We have, like, a constable that has a jurisdiction, maybe, of 750,000 or 800,000. Those are individuals that are closer to the constituents. They are the ones who do the eviction work and otherwise. But, again, they are right there on the ground. And we have sheriffs, we have police officers, of course we have the FBI, and of course the U.S. Secret Service, and just a number of layers.

So I would be interested in that.

I would be interested for Ms. Coney—and welcome—to again establish for us how significant a problem is this whole issue of the invasion of our privacy. Give us, if you will, the broadness of the problem and the depth of the problem, if you will.

And I have another question, but let me yield to Mr. Magaw.

Mr. MAGAW. Thank you very much.

We partner very well with State and local law enforcement, as well as Federal agencies. And we realize the importance of sharing information on different cases that we are working.

Quite frankly, across the country we have 29 different financial crimes task forces and 24 electronic crime task forces. Those task forces are built on sharing of information, not only with law enforcement, with the private sector, as well as the academic community. I feel the sharing of the information with Federal, State and local law enforcement addresses those concerns that you have.

Mr. JACKSON LEE. And let me just expand a little bit more. Are you in constant communication with local law enforcement? Maybe

I have missed it. Are there task forces that are addressing this question?

Mr. MAGAW. Yes. On all of our task forces, financial crimes task forces, as well as electronic task forces, State and local law enforcements are key partners in those task forces. Information is disseminated through them back to their department, so that we are coordinating our efforts to address identity theft.

Mr. JACKSON LEE. Ms. Coney?

Ms. CONEY. Thank you, Congresswoman Jackson Lee.

This is probably the most significant part of why data breach is even being considered by this Committee. Millions of records of individuals are online or available through electronic transfer. The question is whether it is the victim's responsibility or whether it is the data holder's responsibility to manage control of that information.

You have to remember, victims are in damage-control mode. They have no idea that they have been attacked until they get notice. When they get notice, they can react. Unfortunately, the notice is usually coming because they have gotten some communication through the mail or looked at their credit report and that is when they know that someone has appropriated their identity and literally stolen their names.

It takes hundreds of hours sometimes just to correct that information. And the mental anxiety and the stress that comes with that is very difficult for people who have not been victimized to even understand.

Those who are in possession of the data have an obligation, a moral obligation—and it should be a legal obligation—to inform people when these things occur.

Now, the jurisdiction of this Committee limits what you can do in that regard. You can hold data managers—because the data owners are really the people whose information they are controlling—make them responsible for reporting to a Government agency. That agency, in turn, will report through the Federal Register a list of those entities who have had their data compromised.

I think this is a reasonable approach. The numbers of victims—216 million Americans have been impacted by loss of data. It is appropriate and definitely——

Mr. JACKSON LEE. Is that in this legislation, what you have just recommended?

Ms. CONEY. Yes, it is. The part that requires those entities that suspect that their data has been compromised must report to the Secret Service the compromise. And the Secret Service, in turn, once a year, will publish in the Federal Register a list of those entities.

Mr. JACKSON LEE. Thank you, Mr. Chairman.

Let me just comment and highlight Section 102 that provides criminal penalties for those who don't provide the notice of the security breach.

And, finally, might I say, what we don't have yet, which we expect to have in the next couple of years, is electronic reporting of medical records. Once we add that large component required to the system, putting all medical facilities and physicians online, we have an enhanced opportunity for abuse. And so I hope this legisla-

tion will move through this Committee and move to the floor and have the President's signature.

I yield back.

Mr. SCOTT. Thank you.

And I want to thank all of our witnesses for their testimony.

Members may have additional questions to ask, and we will submit those to you in writing, and we would appreciate it if you could respond as soon as possible so the answers can be part of the record.

Without objection, the hearing record will remain open for 1 week for the submission of additional materials.

The Chairwoman of the Commercial and Administrative Law Subcommittee has offered a statement. She has reminded us that some of the parts of the bill come under the jurisdiction of her Subcommittee, as well as most of it in this Committee, and so she has an interest in this legislation.

The gentleman from Texas.

Mr. GOHMERT. Thank you, Mr. Chairman.

I was made aware that there may have been a study that actually deals with how often businesses notify consumers of breach or loss of data. And is that right, Mr. Lourie?

Mr. LOURIE. It is not a Government study, but there has been a study done.

Mr. GOHMERT. Okay. Could you direct us to that and the information to follow?

Mr. LOURIE. Yes, I will provide that information.

[The information referred to is available in the Appendix.]

Mr. SCOTT. And does that study indicate how often criminal activity takes place after a breach?

Mr. LOURIE. I don't know if it does. The only thing I know about this study is that—and, again, this is not a Government study, and we cannot say with any degree of certainty whether it is accurate. But the only thing I know about the study as I sit here—and we will provide it to you—is that they estimate that approximately 30 percent of breaches are reported by victims.

Mr. SCOTT. Thank you.

Without objection, the Committee stands adjourned.

[Whereupon, at 4:55 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

SHEILA JACKSON LEE
18TH DISTRICT, TEXAS

WASHINGTON OFFICE:
15 Rayburn House Office Building
Washington, DC 20515
(202) 225-3816

DISTRICT OFFICE:
1919 SMITH STREET, SUITE 1180
THE GEORGE "MICKEY" LELAND FEDERAL BUILDING
HOUSTON, TX 77002
(713) 655-0050

ACRES HOME OFFICE:
6719 WEST MONTGOMERY, SUITE 204
HOUSTON, TX 77019
(713) 691-4882

HEIGHTS OFFICE:
420 WEST 19TH STREET
HOUSTON, TX 77008
(713) 861-4070

FIFTH WARD OFFICE:
3300 LYONS AVENUE, SUITE 301
HOUSTON, TX 77020

Congress of the United States
House of Representatives
Washington, DC 20515

COMMITTEES:
JUDICIARY
SUBCOMMITTEES:
COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY
IMMIGRATION, CITIZENSHIP, REFUGEES, BORDER SECURITY, AND INTERNATIONAL LAW
CRIME, TERRORISM AND HOMELAND SECURITY

HOMELAND SECURITY
SUBCOMMITTEES:
CHAIR
TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION
BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM

FOREIGN AFFAIRS
SUBCOMMITTEES:
AFRICA AND GLOBAL HEALTH
MIDDLE EAST AND SOUTH ASIA

SENIOR WHIP
DEMOCRATIC CAUCUS

WHIP
CONGRESSIONAL BLACK CAUCUS

CHAIR
CONGRESSIONAL CHILDREN'S CAUCUS

CONGRESSWOMAN SHEILA JACKSON LEE, OF TEXAS

STATEMENT BEFORE THE COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

H.R. 4175, THE "PRIVACY AND CYBERCRIME ENFORCEMENT ACT OF 2007"

DECEMBER 18, 2007

Thank you Mr. Chairman, for holding today's important legislative hearing. H.R. 4175, introduced by Mr. Conyers, with myself and five other Members from both sides of the aisle as original cosponsors, represents an important stride forward toward increased cyber security. I would like to welcome our

distinguished panel of witnesses: Andrew Lourie, Chief of Staff and Senior Advisor to the Criminal Division, U.S. Department of Justice; Craig Magaw, Special Agent, Criminal Investigative Division, U.S. Secret Service, U.S. Department of Homeland Security; Joel Winston, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission; Jaimee Napp, Executive Director, Identity Theft Action Council of Nebraska; Robert W. Holleyman, II, President and CEO, Business Software Alliance; and Lillie Coney, Associate Director, Electronic Privacy Information Center. I look forward to your informative testimony.

Mr. Chairman, the "Privacy and Cybercrime Enforcement Act of 2007" addresses a specific and serious problem that has arisen in our society. Though the internet has proven an invaluable communications resource, making more information available to more people than ever before, it has also opened the door for new areas of criminal activity. As use of the internet has grown exponentially in recent years, cybercrime has also become

increasingly organized. It is now a business spanning national borders, with criminals selling their online skills to customers ranging from individuals to nation states and possibly even to terrorist groups.

The bipartisan support for this legislation is indicative of the seriousness of the issue. Cybercrime can involve theft of intellectual property, a violation of patent law, trade secret, or copyright laws. In addition, the category of cybercrime also includes attacks against computers to deliberately disrupt processing, and it may include espionage to make unauthorized copies of classified data.

With over 150 million people in this country using the internet, and, last year alone, spending over $102 billion via the internet, Americans are increasingly at risk of cybercrime. With the advent of the internet age, identity theft has quickly become one of the most prolific crimes in the United States, topping the list of consumer complaints filed with the Federal Trade Commission in 2005. Internet users are lured into clinking on links, which then

load malicious software onto the victim's computer. Through this software, the cybercriminal is able to gather personal information off the user's computer. This may include their name, address, place and date of birth, social security number, mother's maiden name, and telephone number. This information may allow the criminal to create false identity documents.

The FBI estimates that identity theft currently costs American businesses and consumers almost $50 billion per year. During the last year alone, over 70 million people had their identities stolen through the theft of personal records and information.

Based on a survey conducted in 2003, the Federal Trade Commission estimated that nearly ten million consumers were victims of some form of identity theft in the preceding 12 months. According to media reports this year, a stolen credit card number sells online for only $1, and a complete identity, including a U.S. bank account number, credit-card number, date of birth, and a government-issued ID number now sells for just $14 to $18.

Additionally, identity theft can be the result of inadequate computer security practices within organizations and companies. Since November 2005, there have been at least 436 data security breaches in this country, affecting millions of consumers. MasterCard International reported that in 2005 more than 40 million credit card numbers belonging to U.S. consumers were accessed by computer hackers, and some of the stolen numbers were allegedly being sold on foreign websites. To cite one particularly egregious example, in January 2007, a retailer called TJX disclosed that it had suffered the largest data breach in U.S. history. In this one case alone, at least 45.7 million credit and debit cards were affected.

Security breaches have also been reported at government agencies, including the National Nuclear Security Administration and the United States Department of Agriculture. When the laptop of an employee of the Department of Veterans Affairs was stolen in 2006, with it was taken the personal information of more than 26 million veterans. More recently, in May 2007, the

Transportation Security Administration reported the loss of the personal and financial records of 100,000 TSA employees, when a computer hard drive went missing.

The danger posed by cybercrime is not limited to individuals. A recent study by the Government Accountability Office (GAO) found that 21 out of 24 federal agencies have significant weaknesses in information security controls. This includes access controls, which ensure that only those individuals with proper authorization are able to read and edit data, and configuration management controls, which regulate the software programs that can be used. Many of these agencies have, in their computer systems, the personal information of millions of Americans; the vulnerabilities of government agency systems put all of us, and the United States as a nation, at risk.

Under current federal law, there is no requirement that companies or state agencies must disclose security breaches. Only 35 states have passed legislation making such notification mandatory. As new technologies continue to outpace policy, and

law enforcement continues to struggle to fight the high-profit potential of cybercrime. Additional barriers exist due to the international nature of the offense, and the difficulties inherent in reconciling conflicting national policies about crime in cyberspace. Because of the nature of the offense, cybercrime is extremely mobile, allowing perpetrators to move their bases of operations to avoid penalties.

As Chairwoman of the Homeland Security Subcommittee on Transportation Security and Infrastructure Protection, I am particularly concerned about the vulnerability of U.S. critical infrastructure to internet attacks. The 2005 attacks on the London transit system indicated that terrorist groups are making use of large communication networks and computerized infrastructures to plan attacks on key targets. Breaches at government agencies, in particular the loss of a hard drive at the Transportation Security Administration, expose our nation to serious threats.

Mr. Chairman, the legislation we are here today to discuss addresses the gaps in federal law to protect personal information,

promote data security, and to prevent cybercrime. To do so, it strengthens the penalties and prosecutions against cyber violations, and encourages increased cyber security. Further, H.R. 4175 would require agencies to conduct privacy impact assessments when an agency develops a rule requiring data collection, retention, or use by non-governmental entities. By mandating breach notification, this legislation goes further than any of its counterparts to ensure that both state and local agencies are informed of any and all security breaches and can therefore work to accommodate victims and prevent further breaches. By converging the provision of state and local funding, mandating breach notification, and providing enforcement mechanisms, this legislation is a comprehensive way forward for our nation's cyber security.

Mr. Chairman, I am proud to cosponsor this legislation, and I look forward to hearing from our witnesses about how we can do more to protect the privacy and personal information of Americans on the internet.

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

PREPARED STATEMENT OF THE HONORABLE LINDA T. SÁNCHEZ, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA, AND CHAIRWOMAN, SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW

STATEMENT FOR
CONGRESSWOMAN LINDA SÁNCHEZ
CHAIR OF THE SUBCOMMITTEE FOR
COMMERCIAL AND ADMINISTRATIVE LAW
Subcommittee on Crime, Terrorism, and
Homeland Security Legislative Hearing on H.R.
4175, the "Privacy and Cybercrime Enforcement
Act of 2007"
December 18, 2007 at 1:00 p.m. in 2141
Rayburn HOB

As technology and the Internet have advanced, an increasing amount of personally identifiable information has been collected and disseminated electronically. Along with this unprecedented trend, cybercrime has expanded dramatically. Cyber criminals have recently developed methods to steal identities online, commit online extortion, and engage in phishing scams. Despite the rise of new criminal techniques in cyberspace, the law has yet to be sufficiently strengthened to address these new techniques.

H.R. 4175, the "Privacy and Cybercrime Enforcement Act of 2007," is a vital measure that will update the criminal code and give law enforcement the tools they need to find, prosecute, and bring cyber criminals to justice.

Title II of the bill, which deals with privacy impact assessments, falls within the jurisdiction of the Subcommittee on Commercial and Administrative Law.

The provisions within this title would require agencies to prepare privacy impact assessments for proposed and final rules that contain a description of the extent to which the rule will impact the privacy interests of individuals. The assessment must be prepared when personally identifiable information from 10 or more individuals, other than agencies, instrumentalities, or employees of the Federal Government is collected, maintained, used, or disclosed. With limited exceptions, such assessments must be made available to the public for comment.

Title II is an important addition that requires agencies to analyze how their rules will impact the privacy interests of individuals. I support its inclusion in the broader legislation.

With the disclosure in January 2007 that retailer TJX suffered the largest data security breach in history, of at least 45.7 million credit and debit cards, it is clear that Congress must respond to the growing problem of identity theft and cybercrime. I applaud Chairman Conyers and Ranking Member Smith for their efforts to strengthen consumer privacy and to protect consumers from cybercrime. As an original cosponsor of H.R. 4175, I am hopeful that this bill will receive bipartisan support as it moves through the legislative process.

PREPARED STATEMENT OF THE HONORABLE LAMAR SMITH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS, AND RANKING MEMBER, COMMITTEE ON THE JUDICIARY

Statement of Judiciary Committee Ranking Member Lamar Smith
Subcommittee on Crime, Terrorism, & Homeland Security
Legislative Hearing on H.R. 4175, the "Cyber-Security Enhancement and Consumer Data Protection Act of 2006"
December 18, 2007

Thank you, Chairman Scott, for holding today's hearing on H.R. 4175, the Privacy and Cybercrime Enforcement Act of 2007. I am an original co-sponsor.

This bipartisan proposal is an important first step in addressing the growing threat of cybercrime and identity theft.

Criminals have always been able to steal possessions or money, but with access to personal information online, they can now steal your identity. During the past year, personal records for approximately 73 million people were lost or stolen.

Thieves steal personal data through a variety of means, ranging from mail-theft to sophisticated computer hacking schemes.

But these breaches can also occur as the result of careless practices such as lost or stolen laptop computers or the inadvertent disclosure of personal data on public websites.

The cost of cybercrime to the American economy is staggering. According to the FBI, the annual loss due to cybercrime is approximately $67 billion. The annual cost of identity theft alone is estimated to be $49.3 billion.

Because of the immense damage caused by cybercrime and identity theft, every public and private entity must take reasonable measures to protect personal data.

It is also important for Congress to ensure that industry representatives notify consumers and law enforcement agencies when serious security breaches occur.

Currently, 35 states have enacted legislation that requires companies or state agencies to disclose security breaches involving personal information.

However, there is no federal law in this area. This bill requires appropriate notification to law enforcement officials by federal agencies.

In addition to the theft of personal data, Cybercrime also poses a serious threat to our national security. Critical infrastructure that relies on computers to operate and sensitive information that is stored on computers are particularly vulnerable to tampering and theft by America's adversaries. Terrorist organizations also can use cybercrime to fund their operations.

Combating cybercrime presents additional challenges for law enforcement officials. As with most crime, victims turn first to their local police departments for assistance. ~~Often times~~, these individuals are often ill-equipped to address cybercrimes, particularly if the crime involves multiple jurisdictions.

Federal law enforcement agencies have the resources and expertise to investigate complex cybercrimes, but typically handle only large investigations. So, how do we bridge this gap?

Coordination between federal, state and local law enforcement agencies has led to greater success in stopping identity theft. Today, many local law enforcement agencies are equipped with the training and expertise to help identity theft victims file police reports and investigate these crimes.

Despite the progress we've made in the past 10 years, we must be realistic: technology will always advance faster than the law.

We must also acknowledge that crime is no longer merely a "local problem;" cybercrime has taken it to both the national and global levels.

With continued education and training, and a continued partnership between federal, state and local law enforcement officials, we can address these crimes before they escalate.

Earlier this year, I introduced H.R. 836, the Cyber-Security Enhancement and Consumer Data Protection Act of 2007. H.R. 4715 includes several provisions from my earlier bill.

I look forward to working with Chairman Conyers, Subcommittee Chairman Scott and other Members to enact broad cybercrime legislation this Congress.

CONCERNS REGARDING TITLES I AND II OF H.R. 4175 AS INTRODUCED

I. Section 102 – Criminal Penalties for Failure to Provide Notice of Security Breaches

- **The Imposition of Criminal Penalties for Failing to Notify Individuals of Security Breaches Would Create Harsher Criminal Penalties for Victimized Businesses Than for Identity Thieves**: The tough criminal penalties imposed on businesses under Section 102 would apply regardless of whether the data subjects faced any prospect of identity theft, fraud, or financial harm. Furthermore, the potential imprisonment of up to five years for individuals or entities with a "covered obligation" to provide notice of security breaches would be more punitive than most, if not all, state larceny statutes. This would create a scenario where a victimized business that fails to notify affected individuals (even in good faith) of a security breach would face more significant criminal sanctions than a thief who steals a laptop or portable media that contains sensitive personally identifiable information.

- **To Avoid a Confusing, Additional but Quite Different Breach Notice Obligation, the Definition of "Covered Obligation" Should Be Clarified to Preempt State Law (Page 3, Lines 16-20):** Under Section 102, an entity with a "covered obligation" must notify affected individuals of a security breach. The term "covered obligation" means "an obligation under Federal law or, if the breach is in or affects interstate commerce, *under State law*." This is very confusing because the notice obligation does not track state law and is in some respects much broader than under state breach notice obligations, yet Section 102 does not preempt state law. Thus, section 102 would create scenarios in which notification is required under state law, but not federal law, and *vice versa*, leaving affected entities to sort through what to do under conflicting statutes and under threat of serious penalties. Security breach notification obligations should be clear, unambiguous, and uniform. Continuing to maintain a patchwork quilt of notification laws that would vary based on the jurisdiction where affected individuals reside defeats the purpose of a federal security breach notification law.

- **Definition of "Sensitive Personally Identifiable Information" Differs from and is Broader Than In All of the 39 Existing State Security Breach Laws**

  - The definition of "sensitive personally identifiable information", whose breach would trigger a notice obligation under federal law, would be different from any definition under federal or state law, and would require notice in many situations that do not create risk to the data subject.

  - **"[A]n individual's first and last name, or first initial and last name, or address or phone number…" (Page 3, Line 24):** We believe that the District of Columbia is the only jurisdiction that includes an address or phone number as a data element that, when combined with other specified data elements, requires

500 Eighth Street N.W., Washington, D.C. 20004
tel: 202.799.4441 fax: 202.799.5441

notification to affected state residents. The bill appears to require notification to individuals when an address, date of birth, and mother's maiden name are compromised, *even where no name is or can be associated with such data elements*. Not only would notification be difficult in such circumstances, since there is no name associated with the data elements, but it would also be unnecessary, since the information could not be used to commit identity theft, fraud, or inflict financial harm.

- **Mother's Maiden Name and Birth Date (Page 4, Lines 9-13):** North Dakota is the only state that identifies these elements as "sensitive," such that notification is required where a mother's maiden name and birth date, when combined with other specified data elements, are breached. These data elements are not particularly sensitive and present little to no risk of identity theft, fraud, or financial harm.

- **Unique Biometric Data (Page 4, Lines 14-16):** Finger prints, voice prints, and retina and iris images are not data elements that, if acquired by an unauthorized person, would render an individual susceptible to financial harm. The overwhelming majority of states do not include biometric data within the ambit of "personal information". Only North Carolina and Wisconsin, to our knowledge, include biometric data as a sensitive data element.

- **Definition of "Security Breach" (Page 4, Line 23 – Page 5, Line 2)**: This term is defined in a confusing, idiosyncratic way that is far broader than under any federal or state law. In other words, notice would be required under this bill in many situations that are not even considered a data security breach under other laws. This would result in a confusing minefield of potential criminal liability for businesses. The definition would mean the "compromise of the security, confidentiality, or integrity of computerized data that there is reason to believe has resulted in <u>improper access</u> to sensitive personally identifiable information."

- **"Improper Access" Definition (Page 5, Lines 3-4):** The term "improper access" is defined to mean "access without authorization or in excess of authorization." Connecticut is the only state that requires notification to affected residents where there is unauthorized "access" to personal information. Even Connecticut law does not contain the "in excess of authorization" element. The overwhelming majority of state security breach laws require notification upon the unauthorized *acquisition* of personal information, not *access to* personal information. The distinction is subtle, but critical.

  - **An "Access" Standard Would Require Notification Under Circumstances Where Consumers Face No Threat of Identity Theft, Fraud, or Financial Harm:** The vast majority of state security breach laws specifically exempt an employee's good faith acquisition of personal information where the personal information is not further disclosed. H.R. 4175 does not exclude good faith acquisition of personal information, which poses no risk of identity theft, fraud, or potential harm to consumers. Under the bill as introduced, businesses would be required to notify affected residents where an employee accidentally accessed the personal information of a customer. This could occur simply by mistyping a

customer's name into a database, which may consequently retrieve the personal information of another customer. While the Interagency Guidance, which applies to financial institutions, requires notification upon "unauthorized access," unauthorized acquisition is the majority rule that most business entities have adapted to in order to comply with the vast majority of security breach notification laws.

- **"Major Security Breach" Definition (Page 6, Lines 1-11)**: The term "major security breach" is defined to mean a breach involving "means of identification pertaining to 10,000 or more individuals is, or is reasonably believed to have been acquired."
    - **"Means of Identification" (Page 6, Lines 12-14):** The term "means of identification" in H.R. 4175 is identical to the sweeping definition of "means of identification" under an existing statute (18 U.S.C. § 1028). Under that statute, "means of identification" encompasses any individually identifiable information, including a mere name of an individual, for which there is no breach notice obligation under current law. This definition is confusing and very different from the definition of "sensitive personally identifiable information" for which the bill requires notice to individuals. There is no good reason to use a different, broader definition here.

- **Section 103 – Use of Full Interstate and Foreign Commerce Power for Criminal Penalties:** Section 103(b) eliminates the interstate or foreign communication requirement under 18 U.S.C. § 1030(a)(2)(C) of the Computer Fraud and Abuse Act for obtaining any information from a protected computer in excess of authorization. Eliminating the interstate or foreign communication requirement from the Computer Fraud and Abuse Act would effectively criminalize conduct that is wholly intrastate and it may present serious Commerce Clause issues, as the Supreme Court has issued two significant decisions since 1995 that have struck down Congressional authority to regulate purely intra-state conduct. Moreover, it would further expand an overbroad provision in the federal hacking statute that makes it a felony, for example, simply to access a public website in a manner that violates its terms of use and obtaining some information from the site.

- **Section 106 – Penalties for Section 1030 (Computer Fraud and Abuse Act) Violations:** H.R. 4175 would impose criminal penalties of up to 20 years for these "routine" violations. It would authorize a court to order forfeiture of property "used or intended to be used to commit or to facilitate the commission of the offense…" This facilitation language is broad and could potentially reach perpetrators' home or office communications infrastructure. The facilitation language would be particularly problematic if the language in S. 2168 eliminating the $5,000 damages threshold under 18 U.S.C. § 1030 emerges from conference.

- **Section 108 – Criminal Restitution (Page 9, Line 23 – Page 10, Line 2):** Section 108 requires individuals convicted of certain identity theft offenses to "pay an amount equal to the value of the victim's time reasonably spent to remediate actual harm resulting from the offense." This sets a troubling precedent in that it is foreseeable that individuals could demand such compensation under circumstances where there is no discernible loss

to the individual. A similar (if not identical) provision appears in S. 2168. The practical problems associated with this provision are also significant. It is not clear whose time would be valued. For example, can an attorney demand compensation equal to her hourly billable rate if she is the victim of identity theft?

- **Section 201 – Enforcement by Attorney General and State Authorities:** This section would authorize civil penalties of up to $500,000 for any business entity that "engages in conduct constituting a violation of a Federal law enacted *after the date of the enactment of this Act relating to data security*." This provision would enact a remedy before a legal requirement exists, in effect putting "the cart before the horse." It is unnecessary and would have far-reaching, unintended consequences.

  First, businesses are already subject to civil penalties for violating the FTC Act, state data security mandates, and sector-specific data security requirements that apply to a broad range of entities in financial and health care fields. What is more, there are already powerful incentives – both legal and reputational – to employ strong data security protocols.

  Second, Section 201 would trigger massive penalties regardless of any nexus to actual harm from the violation. Every State Attorney General, state consumer protection authority and any local authorities deputized by a State Attorney General, as well as the Department of Justice, would *each* be authorized to seek $500,000 penalties regardless of whether a data security violation was intentional or resulted in consumer harm. This could mean tens of millions of dollars of penalties for a single, technical violation.

  Third, these huge penalties would be targeted in discriminatory fashion only at businesses, when government and non-profit entities have worse records on data security. Finally, these penalties might be triggered even absent an adjudicated violation of a data security mandate. The phrase "engages in conduct constituting a violation" is ambiguous, and could be read to authorize civil penalties upon informal findings that a data security standard has been violated.

- **Section 203 -- Privacy Impact Assessment in Rulemaking:** This provision would require an unworkable, burdensome set of procedures that would encumber every federal rulemaking. Every rulemaking would have to adhere to a rigorous set of privacy requirements more extensive than virtually any of the many existing federal privacy laws. It would also have the unintended consequence of encouraging any entity with an amorphous "privacy interest" to invoke this interest as a pretext for challenging a government rule that they did not like, freed from the "substantial evidence" standard that applies to ordinary challenges under the Administrative Procedures Act. Both the initial and final privacy impact assessment that would accompany a proposed rule or final rule must include a description and analysis of the extent to which the proposed rule provides a set of privacy requirements far more detailed and exacting than that passed by Congress in federal privacy statutes. For example, it would require written notice within 14 days of a security breach, even though the breach might not have been discovered within 14 days and it often takes more than 14 days of forensic work after discovery to figure out which individuals' data were in fact compromised.

BUSINESS SOFTWARE ALLIANCE

Robert W. Holleyman, II
President and Chief Executive Officer

1150 18th Street, NW
Suite 700
Washington, DC 20036

p. 202/872.5500
f. 202/872.5501

December 21, 2007

JAN 07 2008

The Honorable Bobby Scott
Chairman

The Honorable Louie Gohmert
Ranking Member

Subcommittee on Crime, Terrorism and Homeland Security
Committee on the Judiciary
US House of Representatives
Washington, DC 20515

Dear Mr. Chairman and Ranking Member Gohmert:

The Business Software Alliance (BSA)* and its members thank you for this opportunity to provide comments on HR 4175, the Privacy and Cybercrime Enforcement Act of 2007.

We greatly appreciate the interest and leadership you have shown in addressing the urgent need to update criminal laws and provide law enforcement with tools to find and prosecute cyber criminals.

As I explained in my testimony at the hearing, BSA believes it is critical to enact cyber crime legislation in several areas. Moreover we believe there is broad support on the Committee and in the House and Senate to address these key areas. With one exception, HR 4175 covers these areas, as does HR 2290.

At the same time, I expressed our serious concern about the inclusion of data breach and privacy provisions in cyber crime legislation. While we support the enactment of data breach and data security legislation, sharp differences of opinion remain among stakeholders as well as interested congressional leaders. Therefore, we believe that the inclusion of data breach and privacy provisions in cyber crime legislation will delay its enactment.

We strongly urge the Committee to:

1. consider legislation addressing cyber crime separately from legislation to address data breach notification and privacy; and

2. amend the cyber crime provisions of HR 4175 as discussed below.

If, however, the Committee decides to consider all of the provisions in HR 4175 as a single bill, then BSA urges the Committee to make several important changes to the data breach provisions.

In addition, BSA believes that the data breach provisions of the bill must include two additional elements that are not currently in the bill and are within the Committee's jurisdiction: clear federal preemption of conflicting state requirements; and exclusive enforcement with the US Attorney General and State Attorneys General (and their authorized agents).

Proposed Amendments to the Cybercrime Provisions of HR 4175

Include a Provision on Botnets – BSA strongly urges the Committee to include a provision criminalizing cyber attacks on 10 or more computers even if they don't suffer $5,000 worth of damages. Indeed, BSA believes this is one of the most important changes to 18 USC 1030 that needs to be made. This change is included in HR 2290 and we understand it is supported by the Department of Justice.

Delete Section 101 – this section would add violations of 18 USC 1030 to the list of RICO predicate offenses. The same provision is included in HR 2290. However, BSA shares the concerns of those who have noted that this change could also result in civil RICO exposure. Although BSA believes the drafting could be fixed, we are more concerned that continuing concerns could delay progress of the legislation. Therefore, we recommend deleting the provision from this bill, and consider this change at a future date.

Amend Section 104 – BSA supports this extortion provision. However, we understand that the Department of Justice proposes to include in the provision an element related to impairing the confidentiality of information already obtained from a computer. BSA believes this addition is warranted.

Amend Section 106 – BSA believes that a court should be required – not authorized – to order the forfeiture of property used in a cyber crime offense and resulting proceeds. BSA believes that, for a number of cyber criminals, the certain loss of their equipment is, in fact, the best deterrent. HR 2290 provides that courts "shall" order forfeiture.

Delete Section 107 – BSA supports this provision which provides needed funding to law enforcement for personnel, equipment and training. The same provision was included in HR 2290. However, BSA understands that political realities in the Senate are such that inclusion

will preclude enactment of any legislation that contains such a provision, and so reluctantly urges the Committee to delete it from this bill.

Amend Section 109 – BSA believes that it is appropriate and helpful for the Sentencing Commission to adopt tougher guidelines for cyber crimes. The comparable provisions in HR 2290 provide further direction to the Commission regarding factors that should be taken into account and BSA urges the inclusion of this greater specificity in HR 4175.

Proposed Amendments to the Data Breach Provisions

BSA supports comprehensive data breach legislation and urges the Committee to consider data breach provisions as part of such separate legislation. As requested, however, BSA is providing specific comments on the data breach provisions in HR 4175.

Amend Section 102 – This section: a) imposes criminal penalties on those who fail to notify consumers; and b) requires notification of major breaches to law enforcement.

BSA opposes the imposition of federal criminal penalties (imprisonment of up to 5 years) for knowingly failing to provide notice of a data breach when required to do so. We believe businesses have sufficient incentives now to provide timely and proper notification when breaches occur and will have additional obligations under a new federal law. It is our sense that the underlying objectives of this legislation can be met by existing practice and potential civil penalties under a new federal law, without imposing criminal penalties. We urge the deletion of the provision on criminal penalties.

BSA could support, with amendments and in the context of broader data breach legislation, the requirement that law enforcement be notified of a major security breach. Here, BSA urges the following specific changes:

- "Means of identification" – the bill should be amended to cover those who possess sensitive personally identifiable information in electronic form, not just means of identification.
- "Security breach" – the definition should be amended to:
  - Limit breaches requiring notification to those that "present a significant risk of harm to one or more individuals" (this language needs to be added). BSA is concerned about the problem of over notification and resulting consumer inattention. Requirements for data breach notification should be focused on

those instances where there is or could be a significant risk of harm.

- Exclude unauthorized access to or acquisition of sensitive personally identifiable information that has been rendered unusable, unreadable or indecipherable to an unauthorized third party through the use of practices or methods such as encryption, redaction, access controls and other such mechanisms which are widely accepted as an effective industry practice or industry standard.

- "Encryption" should be defined to mean –

  - the protection of data in electronic form, in storage or in transit, using an encryption technology that has been adopted by an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

  - includes appropriate management and safeguards of such cryptographic keys so as to protect the integrity of encryption.

Amend Section 201 – This provision authorizes the US Attorney General to pursue civil penalties and injunctions "with respect to any conduct constituting a violation of a Federal law enacted after the date of the enactment of this Act relating to data security..." A State Attorney General is authorized to proceed "with respect to that conduct to the extent the conduct adversely affects an interest of the residents of a State."

As written, this provision would establish the Attorney General and states' Attorneys General as the general regulators and enforcers of the manner in which organizations secure and manage consumer data. This is a task for which they are highly unlikely to have the necessary resources or expertise. We strongly urge the Committee to limit the scope of this enforcement provision to a violation of the bill's requirement to notify law enforcement of major security breaches.

The provision in the bill stating that the rights and remedies available under the bill do not affect any other rights and remedies available under Federal or State law also should be amended to clarify that nothing in the data breach notification section of the bill establishes a private cause of action against an entity subject to its requirements for violation of the bill's provisions.

Important additional provisions: BSA believes that any data breach legislation must also include the following provisions:

- Federal Preemption: federal data breach notification law must supersede any provision of a statute, regulation, or rule of a State or political subdivision of a State, which requires notification to individuals of a data breach.

- Exclusive Enforcement: federal data breach notification law must be clear that only the US Attorney General and a State consumer protection attorney (as defined in Section 202) may bring a civil action for violation of the data breach provisions of the bill and that nothing in the bill establishes a private cause of action for any violation of its data breach provisions.

Sincerely,

Robert Holleyman

Robert W. Holleyman, II
President and CEO

**The Business Software Alliance (www.bsa.org) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, CA, Cadence Design Systems, Cisco Systems, CNC Software/Mastercam, Corel Corporation, Dell, EMC, Entrust, HP, IBM, Intel, McAfee, Microsoft, Monotype Imaging, PTC, Quark, Inc., SAP, Siemens PLM Software, SolidWorks, Sybase, Symantec, Synopsys, and The MathWorks.*

DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft

Each year, millions of consumers have their identities stolen. Identity theft is a serious crime, and can cost people time and money.

At the Federal Trade Commission, our message on identity theft is practical and concise: Deter, Detect, Defend. While there is no fool-proof way to avoid ID theft, there are ways to minimize the chances of becoming a victim, and minimize the damage should a theft occur.

Many people just don't have all the information they need. That is where you come in. Raising awareness and educating your community – whether it's a business, place of worship, social club or professional association – is critical.

We appreciate your help in the fight against identity theft.

Deborah Platt Majoras
Chairman, Federal Trade Commission