To place reasonable safeguards on the use of surveillance and other authorities under the USA PATRIOT Act, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. FEINGOLD (for himself, Mr. DURBIN, Mr. TESTER, Mr. UDALL of New Mexico, and Mr. BINGAMAN) introduced the following bill; which was read twice and referred to the Committee on 

A BILL

To place reasonable safeguards on the use of surveillance and other authorities under the USA PATRIOT Act, and for other purposes.

1 Be it enacted by the Senate and House of Representa-
2 tives of the United States of America in Congress assembled,

3 SECTION 1. SHORT TITLE.

4 This Act may be cited as the “Judicious Use of Sur-
5 veillance Tools In Counterterrorism Efforts Act of 2009”
6 or the “JUSTICE Act”.

7 SEC. 2. TABLE OF CONTENTS.

8 The table of contents for this Act is as follows:

Sec. 1. Short title.
Sec. 2. Table of contents.
TITLE I—REASONABLE SAFEGUARDS TO PROTECT THE PRIVACY OF AMERICANS’ RECORDS

Sec. 103. National Security Letter compliance program and tracking database.
Sec. 105. Emergency disclosures.
Sec. 106. Least intrusive means.
Sec. 107. Privacy protections for section 215 business records orders.
Sec. 108. Technical and conforming amendments.

TITLE II—REASONABLE SAFEGUARDS TO PROTECT THE PRIVACY OF AMERICANS’ HOMES

Sec. 201. Limitation on authority to delay notice of search warrants.

TITLE III—REASONABLE SAFEGUARDS TO PROTECT THE PRIVACY OF AMERICANS’ COMMUNICATIONS

Sec. 301. Limitations on roving wiretaps under Foreign Intelligence Surveillance Act.
Sec. 302. Privacy protections for pen registers and trap and trace devices.
Sec. 303. Repeal of telecommunications immunity.
Sec. 304. Prohibition on bulk collection under FISA Amendments Act.
Sec. 305. Prohibition on reverse targeting under FISA Amendments Act.
Sec. 306. Limits on use of unlawfully obtained information under FISA Amendments Act.
Sec. 307. Privacy protections for international communications of Americans collected under FISA Amendments Act.
Sec. 308. Clarification of computer trespass authority.

TITLE IV—IMPROVEMENTS TO FURTHER CONGRESSIONAL AND JUDICIAL OVERSIGHT

Sec. 401. Public reporting on the Foreign Intelligence Surveillance Act.
Sec. 402. Use of Foreign Intelligence Surveillance Act materials.
Sec. 403. Challenges to nationwide orders for electronic evidence.

TITLE V—IMPROVEMENTS TO FURTHER EFFECTIVE, FOCUSED INVESTIGATIONS

Sec. 501. Modification of definition of domestic terrorism.
Sec. 502. Clarification of intent requirement.
TITLE I—REASONABLE SAFEGUARDS TO PROTECT THE PRIVACY OF AMERICANS’ RECORDS

SEC. 101. NATIONAL SECURITY LETTER AUTHORITY.

(a) NATIONAL SECURITY LETTER AUTHORITY FOR COMMUNICATIONS SUBSCRIBER RECORDS.—

(1) IN GENERAL.—Section 2709 of title 18, United States Code, is amended to read as follows:

“§ 2709. National Security Letter for communications subscriber records

“(a) Authorization.—

“(1) IN GENERAL.—The Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or Special Agent in Charge in a Bureau field office, may issue in writing and cause to be served on a wire or electronic communications service provider a National Security Letter requiring the production of—

“(A) the name of a customer or subscriber;

“(B) the address of a customer or subscriber;

“(C) the length of the provision of service by the provider to a customer or subscriber (in-
cluding start date) and the types of service used
by the customer or subscriber;

“(D) the telephone number or instrument
number, or other subscriber number or identi-
fier, of a customer or subscriber, including any
temporarily assigned network address;

“(E) the means and sources of payment
for service by the provider (including any credit
card or bank account number);

“(F) information about any service or mer-
chandise orders relating to the communications
service of a customer or subscriber, including
any shipping information and vendor locations;
and

“(G) the name and contact information, if
available, of any other wire or electronic com-
munications service providers facilitating the
communications of a customer or subscriber.

“(2) LIMITATION.—A National Security Letter
issued under this subsection may not require the
production of local or long distance telephone
records or electronic communications transactional
information not listed in paragraph (1).

“(b) REQUIREMENTS.—
“(1) IN GENERAL.—A National Security Letter shall be issued under subsection (a) only where—

“(A) the records sought are relevant to an ongoing and authorized national security investigation (other than an assessment); and

“(B) there are specific and articulable facts providing reason to believe that the records—

“(i) pertain to a suspected agent of a foreign power or an individual who is the subject of an ongoing and authorized national security investigation (other than an assessment);

“(ii) pertain to an individual who has been in contact with, or otherwise directly linked to, a suspected agent of a foreign power or an individual who is the subject of an ongoing and authorized national security investigation (other than an assessment); or

“(iii) pertain to the activities of a suspected agent of a foreign power, where those activities are the subject of an ongoing and authorized identified national security investigation (other than an assess-
ment), and obtaining the records is the least intrusive means that could be used to identify persons believed to be involved in the activities.

“(2) INVESTIGATION.—For purposes of this section, an ongoing and authorized national security investigation—

“(A) is an investigation conducted under guidelines approved by the Attorney General and in accordance with Executive Order 12333 (or any successor order);

“(B) shall not be conducted with respect to a United States person upon the basis of activities protected by the first amendment to the Constitution of the United States; and

“(C) shall be specifically identified and recorded by an official issuing a National Security Letter under subsection (a).

“(3) CONTENTS.—A National Security Letter issued under subsection (a) shall—

“(A) describe the records to be produced with sufficient particularity to permit the records to be fairly identified;

“(B) include the date on which the records shall be provided, which shall allow a reasonable
period of time within which the records can be assembled and made available;

“(C) provide clear and conspicuous notice of the principles and procedures set forth in this section and section 3511 of this title, including notification of any nondisclosure requirement under subsection (e), the right to contest the National Security Letter or applicable nondisclosure requirements and procedures for doing so, and a statement laying out the rights and responsibilities of the recipient; and

“(D) not contain any requirement that would be held to be unreasonable if contained in a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or require the production of any documentary evidence that would be privileged from disclosure if demanded by a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation.

“(4) RETENTION OF RECORDS.—The Director of the Federal Bureau of Investigation shall direct that a signed copy of each National Security Letter issued under subsection (a) be retained in the data-
base required to be established under section 103 of
the JUSTICE Act.

“(c) Prohibition of Certain Disclosure.—

“(1) In general.—

“(A) In general.—If a certification is
issued under subparagraph (B) and notice of
the right to judicial review under paragraph (4)
is provided, no wire or electronic communica-
tion service provider, or officer, employee, or
agent thereof, who receives a National Security
Letter issued under subsection (a), shall dis-
lose to any person the particular information
specified in the certification during the time pe-
riod to which the certification applies, which
may be not longer than 1 year.

“(B) Certification.—The requirements
of subparagraph (A) shall apply if the Director
of the Federal Bureau of Investigation, or a
designee of the Director whose rank shall be no
lower than Deputy Assistant Director at Bu-
reau headquarters or a Special Agent in Charge
of a Bureau field office, certifies that—

“(i) there is reason to believe that dis-
closure of particular information about the
existence or contents of a National Secu-
Security Letter issued under subsection (a) during the applicable time period will result in—

“(I) endangering the life or physical safety of any person;

“(II) flight from prosecution;

“(III) destruction of or tampering with evidence;

“(IV) intimidation of potential witnesses;

“(V) interference with diplomatic relations; or

“(VI) otherwise seriously endangering the national security of the United States by alerting a target, an associate of a target, or the foreign power of which the target is an agent, of the interest of the Government in the target;

“(ii) the harm identified under clause (i) relates to the ongoing and authorized national security investigation to which the records sought are relevant; and
“(iii) the nondisclosure requirement is narrowly tailored to address the specific harm identified under clause (i).

“(2) EXCEPTION.—

“(A) IN GENERAL.—A wire or electronic communication service provider, or officer, employee, or agent thereof, who receives a National Security Letter issued under subsection (a) may disclose information otherwise subject to any applicable nondisclosure requirement to—

“(i) those persons to whom disclosure is necessary in order to comply with the National Security Letter;

“(ii) an attorney in order to obtain legal advice or assistance regarding the National Security Letter; or

“(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

“(B) NONDISCLOSURE REQUIREMENT.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a National Security Letter is issued
under subsection (a) in the same manner as the person to whom the National Security Letter is issued.

“(C) NOTICE.—Any recipient who discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

“(3) EXTENSION.—The Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office, may extend a nondisclosure requirement for additional periods of not longer than 1 year if, at the time of each extension, a new certification is made under paragraph (1)(B) and notice is provided to the recipient of the applicable National Security Letter that the nondisclosure requirement has been extended and the recipient has the right to judicial review of the nondisclosure requirement.

“(4) RIGHT TO JUDICIAL REVIEW.—

“(A) IN GENERAL.—A wire or electronic communications service provider who receives a National Security Letter issued under sub-
section (a) shall have the right to judicial review of any applicable nondisclosure requirement and any extension thereof.

“(B) TIMING.—

“(i) IN GENERAL.—A National Security Letter issued under subsection (a) shall state that if the recipient wishes to have a court review a nondisclosure requirement, the recipient shall notify the Government not later than 21 days after the date of receipt of the National Security Letter.

“(ii) EXTENSION.—A notice that the applicable nondisclosure requirement has been extended under paragraph (3) shall state that if the recipient wishes to have a court review the nondisclosure requirement, the recipient shall notify the Government not later than 21 days after the date of receipt of the notice.

“(C) INITIATION OF PROCEEDINGS.—If a recipient of a National Security Letter issued under subsection (a) makes a notification under subparagraph (B), the Government shall ini-
tiate judicial review under the procedures established in section 3511 of this title.

“(5) TERMINATION.—If the facts supporting a nondisclosure requirement cease to exist prior to the applicable time period of the nondisclosure requirement, an appropriate official of the Federal Bureau of Investigation shall promptly notify the wire or electronic service provider, or officer, employee, or agent thereof, subject to the nondisclosure requirement that the nondisclosure requirement is no longer in effect.

“(d) MINIMIZATION AND DESTRUCTION.—

“(1) IN GENERAL.—Not later than 180 days after the date of enactment of the JUSTICE Act, the Attorney General shall establish minimization and destruction procedures governing the acquisition, retention and dissemination by the Federal Bureau of Investigation of any records received by the Federal Bureau of Investigation in response to a National Security Letter issued under subsection (a).

“(2) DEFINITION.—In this subsection, the term ‘minimization and destruction procedures’ means—

“(A) specific procedures that are reasonably designed in light of the purpose and tech-
nique of a National Security Letter, to mini-
mize the acquisition and retention, and prohibit
the dissemination, of nonpublicly available in-
formation concerning unconsenting United
States persons consistent with the need of the
United States to obtain, produce, and dissemi-
nate foreign intelligence information, including
procedures to ensure that information obtained
under a National Security Letter that does not
meet the requirements of this section or is out-
side the scope of the National Security Letter,
is returned or destroyed;

“(B) procedures that require that nonpub-
licly available information, which is not foreign
intelligence information (as defined in section
101(e)(1) of the Foreign Intelligence Surveil-
lance Act of 1978 (50 U.S.C. 1801(e)(1))) shall
not be disseminated in a manner that identifies
any United States person, without the consent
of the United States person, unless the identity
of the United States person is necessary to un-
derstand foreign intelligence information or as-
sess its importance; and

“(C) notwithstanding subparagraphs (A)
and (B), procedures that allow for the retention
and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

“(e) Requirement That Certain Congressional Bodies Be Informed.—

“(1) In general.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the Senate and the Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives concerning all National Security Letters issued under subsection (a).

“(2) Contents.—Each report under paragraph (1) shall include—

“(A) a description of the minimization and destruction procedures adopted by the Attorney General under subsection (d), including any changes to the minimization and destruction procedures previously adopted by the Attorney General;

“(B) a summary of any petitions or court proceedings under section 3511 of this title;
16

“(C) a description of the extent to which information obtained with National Security Letters issued under subsection (a) has aided intelligence investigations and an explanation of how the information has aided the investigations; and

“(D) a description of the extent to which information obtained with National Security Letters issued under subsection (a) has aided criminal prosecutions and an explanation of how the information has aided the prosecutions.

“(f) USE OF INFORMATION.—

“(1) IN GENERAL.—

“(A) CONSENT.—Any information acquired under a National Security Letter issued under subsection (a) concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization and destruction procedures established by the Attorney General under subsection (d).

“(B) LAWFUL PURPOSE.—No information acquired under a National Security Letter issued under subsection (a) may be used or dis-
closed by Federal officers or employees except for lawful purposes.

“(2) Disclosure for Law Enforcement Purposes.—No information acquired under a National Security Letter issued under subsection (a) shall be disclosed for law enforcement purposes unless the disclosure is accompanied by a statement that the information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

“(3) Notification of Intended Disclosure by the United States.—Whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States against an aggrieved person any information obtained or derived from a National Security Letter issued under subsection (a), the United States shall, before the trial, hearing, or other proceeding or at a reasonable time before an effort to so disclose or so use the information or submit the information in evidence, notify the aggrieved person and the court or other authority in which the infor-
information is to be disclosed or used that the United States intends to so disclose or so use the information.

“(4) Notification of intended disclosure by state or political subdivision.—Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the State or political subdivision thereof against an aggrieved person any information obtained or derived from a National Security Letter issued under subsection (a), the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use the information.

“(5) Motion to suppress.—

“(A) In general.—Any aggrieved person against whom evidence obtained or derived from a National Security Letter issued under subsection (a) is to be, or has been, introduced or otherwise used or disclosed in any trial, hear-
ing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, or a State or political subdivision thereof, may move to suppress the evidence obtained or derived from the National Security Letter, as the case may be, on the grounds that—

“(i) the information was acquired in violation of the Constitution or laws of the United States; or

“(ii) the National Security Letter was not issued in accordance with the requirements of this section.

“(B) TIMING.—A motion under subparagraph (A) shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the aggrieved person concerned was not aware of the grounds of the motion.

“(6) JUDICIAL REVIEW.—

“(A) IN GENERAL.—In a circumstance described in subparagraph (B), a United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority
shall, if the Attorney General files an affidavit under oath that disclosure would harm the national security of the United States, review in camera such materials as may be necessary to determine whether the National Security Letter was lawfully issued.

“(B) CIRCUMSTANCES.—A circumstance described in this subparagraph is a circumstance in which—

“(i) a court or other authority is notified under paragraph (3) or (4);

“(ii) a motion is made under paragraph (5); or

“(iii) any motion or request is made by an aggrieved person under any other statute or rule of the United States or any State before any court or other authority of the United States or any State to—

“(I) discover or obtain materials relating to a National Security Letter issued under subsection (a); or

“(II) discover, obtain, or suppress evidence or information obtained or derived from a National Security Letter issued under subsection (a).
“(C) DISCLOSURE.—In making a determination under subparagraph (A), unless the court finds that disclosure would not assist in determining any legal or factual issue pertinent to the case, the court may disclose to the aggrieved person, the counsel for the aggrieved person, or both, under the procedures and standards provided in the Classified Information Procedures Act (18 U.S.C. App.) or other appropriate security procedures and protective orders, portions of the National Security Letter, or related materials.

“(7) EFFECT OF DETERMINATION OF LAWFULNESS.—

“(A) UNLAWFUL ORDERS.—If a United States district court determines under paragraph (6) that a National Security Letter was not issued in compliance with the Constitution or laws of the United States, the court may suppress the evidence that was unlawfully obtained or derived from the National Security Letter or otherwise grant the motion of the aggrieved person.

“(B) LAWFUL ORDERS.—If a United States district court determines under para-
graph (6) that a National Security Letter was
issued in accordance with the Constitution and
laws of the United States, the court shall deny
the motion of the aggrieved person, except to
the extent that due process requires discovery
or disclosure.

“(8) BINDING FINAL ORDERS.—An order grant-
ing a motion or request under paragraph (6), a deci-
sion under this section that a National Security Let-
ter was not lawful, and an order of a United States
district court requiring review or granting disclosure
of an application, order, or other related materials
shall be a final order and binding upon all courts of
the United States and the several States, except an
appeal or petition to a United States court of ap-
peals or the Supreme Court of the United States.

“(g) DEFINITIONS.—In this section—

“(1) the terms ‘agent of a foreign power’, ‘for-
eign power’, and ‘United States person’ have the
meanings given those terms in section 101 of the
Foreign Intelligence Surveillance Act of 1978 (50
U.S.C. 1801);

“(2) the term ‘aggrieved person’ means a per-
son whose information or records were sought or ob-
tained under this section; and
“(3) the term ‘assessment’ means an assessment, as that term is used in the guidelines entitled ‘The Attorney General’s Guidelines for Domestic FBI Operations’, or any successor thereto.”.

(2) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2709 and inserting the following:

“2709. National Security Letter for communications subscriber records.”.

(b) NATIONAL SECURITY LETTER AUTHORITY FOR CERTAIN FINANCIAL RECORDS.—Section 1114 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414) is amended to read as follows:

“SEC. 1114. NATIONAL SECURITY LETTER FOR CERTAIN FINANCIAL RECORDS.

“(a) AUTHORIZATION.—

“(1) IN GENERAL.—The Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or Special Agent in Charge in a Bureau field office, may issue in writing and cause to be served on a financial institution, a National Security Letter requiring the production of—
“(A) the name of a customer or entity with whom the financial institution has a financial relationship;

“(B) the address of a customer or entity with whom the financial institution has a financial relationship;

“(C) the length of time during which a customer or entity has had an account or other financial relationship with the financial institution (including the start date) and the type of account or other financial relationship; and

“(D) any account number or other unique identifier associated with the financial relationship of a customer or entity to the financial institution.

“(2) LIMITATION.—A National Security Letter issued under this subsection may not require the production of records or information not listed in paragraph (1).

“(b) NATIONAL SECURITY LETTER REQUIREMENTS.—

“(1) IN GENERAL.—A National Security Letter issued under subsection (a) shall be subject to the requirements of subsections (b) through (g) of section 2709 of title 18, United States Code, in the
same manner and to the same extent as those provisions apply with respect to a National Security Letter issued under section 2709(a) of title 18, United States Code, to a wire or electronic communication service provider.

“(2) REPORTING.—For any National Security Letter issued under subsection (a), the semianual reports under section 2709(e) of title 18, United States Code, shall also be submitted to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives.

“(c) DEFINITION OF ‘FINANCIAL INSTITUTION’.—

For purposes of this section (and sections 1115 and 1117, insofar as the sections relate to the operation of this section), the term ‘financial institution’ has the same meaning as in subsections (a)(2) and (c)(1) of section 5312 of title 31, except that the term shall include only a financial institution any part of which is located inside any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or the United States Virgin Islands.”.

(c) NATIONAL SECURITY LETTER AUTHORITY FOR CERTAIN CONSUMER REPORT RECORDS.—
Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) is amended—

(A) by striking the section heading and inserting the following:

§ 626. National Security Letters for certain consumer report records;

(B) by striking subsections (a) through (d) and inserting the following:

(a) Authorization.—

(1) In general.—The Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or Special Agent in Charge in a Bureau field office, may issue in writing and cause to be served on a consumer reporting agency a National Security Letter requiring the production of—

(A) the name of a consumer;

(B) the current and former address of a consumer;

(C) the current and former places of employment of a consumer; and

(D) the name and address of any financial institution (as that term is defined in sec-
tion 1101 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401) at which a consumer maintains or has maintained an account, to the extent that the information is in the files of the consumer reporting agency.

“(2) LIMITATION.—A National Security Letter issued under this subsection may not require the production of a consumer report.

“(b) NATIONAL SECURITY LETTER REQUIREMENTS.—

“(1) IN GENERAL.—A National Security Letter issued under subsection (a) shall be subject to the requirements of subsections (b) through (g) of section 2709 of title 18, United States Code, in the same manner and to the same extent as those provisions apply with respect to a National Security Letter issued under section 2709(a) of title 18, United States Code, to a wire or electronic communication service provider.

“(2) REPORTING.—For any National Security Letter issued under subsection (a), the semiannual reports under section 2709(e) of title 18, United States Code, shall also be submitted to the Committee on Banking, Housing, and Urban Affairs of
the Senate and the Committee on Financial Services of the House of Representatives.”;

(C) by striking subsections (f) through (h);

and

(D) by redesignating subsections (e) and (i) through (m) as subsections (e) through (h), respectively.

(2) REPEAL.—Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) is repealed.

(3) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) is amended by striking the items relating to sections 626 and 627 and inserting the following:


“627. [Repealed].”.

SEC. 102. JUDICIAL REVIEW OF NATIONAL SECURITY LETTERS.

(a) REVIEW OF NONDISCLOSURE ORDERS.—Section 3511(b) of title 18, United States Code, is amended to read as follows:

“(b) NONDISCLOSURE.—

“(1) IN GENERAL.—

“(A) NOTICE.—If a recipient of a National Security Letter under section 2709 of this title, section 626 of the Fair Credit Reporting Act
(15 U.S.C. 1681u), section 1114 of the Right to Financial Privacy Act (12 U.S.C. 3414), or section 802(a) of the National Security Act of 1947 (50 U.S.C. 436(a)), wishes to have a court review a nondisclosure requirement imposed in connection with the National Security Letter, the recipient shall notify the Government not later than 21 days after the date of receipt of the National Security Letter or of notice that an applicable nondisclosure requirement has been extended.

“(B) APPLICATION.—Not later than 21 days after the date of receipt of a notification under subparagraph (A), the Government shall apply for an order prohibiting the disclosure of particular information about the existence or contents of the relevant National Security Letter. An application under this subparagraph may be filed in the district court of the United States for any district within which the authorized investigation that is the basis for the National Security Letter is being conducted. The applicable nondisclosure requirement shall remain in effect during the pendency of proceedings relating to the requirement.
“(C) CONSIDERATION.—A district court of the United States that receives an application under subparagraph (B) should rule expeditiously, and may issue a nondisclosure order for a period of not longer than 1 year, unless the facts justify a longer period of nondisclosure.

“(D) DENIAL.—If a district court of the United States rejects an application for a nondisclosure order or extension thereof, the nondisclosure requirement shall no longer be in effect.

“(2) APPLICATION CONTENTS.—An application for a nondisclosure order or extension thereof under this subsection shall include—

“(A) a statement of specific and articulable facts giving the applicant reason to believe that disclosure of particular information about the existence or contents of a National Security Letter described in paragraph (1)(A) during the applicable time period will result in—

“(i) endangering the life or physical safety of any person;

“(ii) flight from prosecution;

“(iii) destruction of or tampering with evidence;
“(iv) intimidation of potential witnesses;

“(v) interference with diplomatic relations; or

“(vi) otherwise seriously endangering the national security of the United States by alerting a target, an associate of a target, or the foreign power of which the target is an agent, of the interest of the Government in the target;

“(B) an explanation of how the harm identified under subparagraph (A) relates to the ongoing and authorized national security investigation to which the records sought are relevant;

“(C) an explanation of how the nondisclosure requirement is narrowly tailored to address the specific harm identified under subparagraph (A); and

“(D) the time period during which the Government believes the nondisclosure requirement should apply.

“(3) STANDARD.—A district court of the United States may issue a nondisclosure require-
ment order or extension thereof under this sub-
section if the court determines that—

“(A) there is reason to believe that disclo-
sure of the information subject to the nondisclo-
sure requirement during the applicable time pe-
period will result in—

“(i) endangering the life or physical
safety of any person;
“(ii) flight from prosecution;
“(iii) destruction of or tampering with
evidence;
“(iv) intimidation of potential wit-
tnesses;
“(v) interference with diplomatic rela-
tions; or
“(vi) otherwise seriously endangering
the national security of the United States
by alerting a target, an associate of a tar-
get, or the foreign power of which the tar-
get is an agent, of the interest of the Gov-
ernment in the target;
“(B) the harm identified under subpara-
graph (A) relates to the ongoing and authorized
national security investigation to which the
records sought are relevant; and
“(C) the nondisclosure requirement is narrowly tailored to address the specific harm identified under subparagraph (A).

“(4) RENEWAL.—A nondisclosure order under this subsection may be renewed for additional periods of not longer than 1 year, unless the facts of the case justify a longer period of nondisclosure, upon submission of an application meeting the requirements of paragraph (2), and a determination by the court that the circumstances described in paragraph (3) continue to exist.”.

(b) DISCLOSURE.—Section 3511(d) of title 18, United States Code, is amended to read as follows:

“(d) DISCLOSURE.—In making determinations under this section, unless the district court of the United States finds that disclosure would not assist in determining any legal or factual issue pertinent to the case, the court may disclose to the petitioner, the counsel of the petitioner, or both, under the procedures and standards provided in the Classified Information Procedures Act (18 U.S.C. App.) or other appropriate security procedures and protective orders, portions of the National Security Letter, or related materials.”.

(c) CONFORMING AMENDMENTS.—Section 3511 of title 18, United States Code, is amended—
(1) in subsection (a)—

(A) by inserting after “(a)” the following “REQUEST.—”;

(B) by striking “2709(b)” and inserting “2709”;

(C) by striking “626(a) or (b) or 627(a)” and inserting “626”; and

(D) by striking “1114(a)(5)(A)” and inserting “1114”; and

(2) in subsection (c)—

(A) by inserting after “(c)” the following “FAILURE TO COMPLY.—”;

(B) by striking “2709(b)” and inserting “2709”;

(C) by striking “626(a) or (b) or 627(a)” and inserting “626”; and

(D) by striking “1114(a)(5)(A)” and inserting “1114”.

(d) REPEAL.—Section 3511(e) of title 18, United States Code, is repealed.

SEC. 103. NATIONAL SECURITY LETTER COMPLIANCE PROGRAM AND TRACKING DATABASE.

(a) COMPLIANCE PROGRAM.—The Director of the Federal Bureau of Investigation shall establish a program
to ensure compliance with the amendments made by section 101.

(b) TRACKING DATABASE.—The compliance program required under subsection (a) shall include the establishment of a database, the purpose of which shall be to track all National Security Letters.

(c) INFORMATION.—The database required under this section shall include—

(1) a signed copy of each National Security Letter;

(2) the date the National Security Letter was issued and for what type of information;

(3) whether the National Security Letter seeks information regarding a United States person;

(4) identification of the ongoing and authorized national security investigation (other than an assessment) to which the National Security Letter relates;

(5) whether the National Security Letter seeks information regarding an individual who is the subject of the investigation described in paragraph (4);

(6) the date on which the information requested was received and, if applicable, when the information was destroyed; and

(7) whether the information gathered was disclosed for law enforcement purposes.
(d) DEFINITIONS.—In this section—

(1) the term “assessment” means an assessment, as that term is used in the guidelines entitled “The Attorney General’s Guidelines for Domestic FBI Operations”, or any successor thereto; and


SEC. 104. PUBLIC REPORTING ON NATIONAL SECURITY LETTERS.

Section 118(c) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (18 U.S.C. 3511 note) is amended—

(1) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking “concerning different United States persons”; and

(B) in subparagraph (A), by striking “, excluding the number of requests for subscriber information”;
(2) by redesignating paragraph (2) as paragraph (3); and

(3) by inserting after paragraph (1) the following:

“(2) CONTENT.—

“(A) IN GENERAL.—Except as provided in subparagraph (B), each report required under this subsection shall include the total number of requests described in paragraph (1) requiring disclosure of information concerning—

“(i) United States persons;

“(ii) persons who are not United States persons;

“(iii) persons who are the subjects of authorized national security investigations;

or

“(iv) persons who are not the subjects of authorized national security investigations.

“(B) EXCEPTION.—With respect to the number of requests for subscriber information under section 2709 of title 18, United States Code, a report required under this subsection need not provide information separated into
SEC. 105. EMERGENCY DISCLOSURES.

(a) Enhanced Protections for Emergency Disclosures.—

(1) Stored Communications Act.—Section 2702 of title 18, United States Code is amended—

(A) in subsection (b)(8)—

(i) by striking ‘‘, in good faith,’’ and inserting ‘‘reasonably’’;

(ii) by inserting ‘‘immediate’’ after ‘‘involving’’; and

(iii) by adding before the period: ‘‘and the request is narrowly tailored to address the emergency, subject to the limitations of subsection (d)’’;

(B) in subsection (c)(4)—

(i) by striking ‘‘, in good faith,’’ and inserting ‘‘reasonably’’;

(ii) by inserting ‘‘immediate’’ after ‘‘involving’’; and

(iii) by adding before the period: ‘‘, subject to the limitations of subsection (d)’’;
(C) by redesignating subsection (d) as subsection (e);

(D) by inserting after subsection (c) the following:

“(d) REQUIREMENT.—

“(1) REQUEST.—If a governmental entity requests that a provider divulge information under subsection (b)(8) or (c)(4), the request shall specify that the disclosure is on a voluntary basis and shall document the factual basis for believing that an emergency involving immediate danger of death or serious physical injury to a person requires disclosure without delay of the information relating to the emergency.

“(2) NOTICE TO COURT.—Not later than 5 days after the date on which a governmental entity obtains access to records under subsection (b)(8) or (c)(4), a governmental entity shall file with the appropriate court a signed, sworn statement of a supervisory official of a rank designated by the head of the governmental entity setting forth the grounds for the emergency access.”; and

(E) in subsection (e), as so redesignated, in each of paragraphs (1) and (2), by striking
“subsection (b)(8)” and inserting “subsections (b)(8) and (c)(4)”.

(2) RIGHT TO FINANCIAL PRIVACY ACT.—

(A) EMERGENCY DISCLOSURES.—The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.) is amended by inserting after section 1120 the following:

“SEC. 1121. EMERGENCY DISCLOSURES.

“(a) IN GENERAL.—

“(1) STANDARD.—A financial institution may divulge a record described in section 1114(a) pertaining to a customer to a Government authority, if the financial institution reasonably believes that an emergency involving immediate danger of death or serious physical injury to a person requires disclosure without delay of information relating to the emergency and the request is narrowly tailored to address the emergency.

“(2) NOTICE IN REQUEST.—If a Government authority requests that a financial institution divulge information under this section, the request shall specify that the disclosure is on a voluntary basis, and shall document the factual basis for believing that an emergency involving immediate danger of
death or serious physical injury to a person requires disclosure without delay of the information.

“(b) CERTIFICATE.—In the instances described in subsection (a), the Government authority shall submit to the financial institution the certificate required in section 1103(b), signed by a supervisory official of a rank designated by the head of the Government authority.

“(c) NOTICE TO COURT.—Not later than 5 days after the date on which a Government authority obtains access to financial records under this section, the Government authority shall file with the appropriate court a signed, sworn statement of a supervisory official of a rank designated by the head of the Government authority setting forth the grounds for the emergency access. After filing a statement under this subsection, a Government authority shall provide notice to the customer in accordance with section 1109.

“(d) REPORTING OF EMERGENCY DISCLOSURES.—On an annual basis, the Attorney General of the United States shall submit to the Committee on the Judiciary and the Committee on Financial Services of the House of Representatives and the Committee on the Judiciary and the Committee on Banking, Housing, and Urban Affairs of the Senate a report containing—
“(1) the number of individuals for whom the Department of Justice has received voluntary disclosures under this section; and

“(2) a summary of the bases for disclosure in those instances where—

“(A) voluntary disclosures under this section were made to the Department of Justice; and

“(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

“(e) DEFINITION.—In this section, the term ‘financial institution’ has the meaning given that term in section 1114(c).”.

(B) CONFORMING AMENDMENTS.—The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.) is amended—

(i) in section 1102 (12 U.S.C. 3402), by striking “or 1114” and inserting “1114, or 1121”; and

(ii) in section 1109(c) (12 U.S.C. 3409(c)), by striking “1114(b)” and inserting “1121”.
(b) Clarification Regarding Data Retention.—Subsection 2703(f) of title 18, United States Code, is amended by adding at the end the following:

“(3) No disclosure without court order.—A provider of wire or electronic communications services or a remote computing service who has received a request under this subsection shall not disclose the records referred to in paragraph (1) until the provider has received a court order or other process.”.

SEC. 106. LEAST INTRUSIVE MEANS.

(a) Guidelines.—

(1) In general.—The Attorney General shall issue guidelines (consistent with Executive Order 12333 or any successor order) providing that, in national security investigations, the least intrusive collection techniques feasible shall be used if there is a choice between the use of more or less intrusive information collection methods.

(2) Specific collection techniques.—The guidelines required under this section shall provide guidance with regard to specific collection techniques, including the use of National Security Letters, considering such factors as—

(A) the effect on the privacy of individuals;
(B) the potential damage to reputation of individuals; and

(C) any special concerns under the first amendment to the Constitution of the United States relating to a potential recipient of a National Security Letter or other legal process, including a direction that prior to issuing a National Security Letter or other legal process to a library or bookseller, investigative procedures aimed at obtaining the relevant information from entities other than a library or bookseller be used and have failed, or reasonably appear to be unlikely to succeed if tried or endanger lives if tried.

(b) DEFINITIONS.—In this section:

(1) BOOKSELLER.—The term “bookseller” means a person or entity engaged in the sale, rental, or delivery of books, journals, magazines, or other similar forms of communication in print or digitally.

(2) LIBRARY.—The term “library” means a library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1))) whose services include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or
digitally to patrons for their use, review, examination, or circulation.


SEC. 107. PRIVACY PROTECTIONS FOR SECTION 215 BUSINESS RECORDS ORDERS.

(a) Privacy Protections for Section 215 Business Records Orders.—

(1) In general.—Section 501(b) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861(b)(2)) is amended—

(A) in paragraph (1)(B), by striking “and” after the semicolon;

(B) in paragraph (2)—

(i) in subparagraph (A), by striking “, such things being presumptively” and all that follows through the end of the subparagraph and inserting a semicolon; and
(ii) by striking subparagraph (B) and inserting the following:

“(B) a statement of specific and articulable facts providing reason to believe that the tangible things sought—

“(i) pertain to a suspected agent of a foreign power or an individual who is the subject of an ongoing and authorized national security investigation (other than an assessment (as defined in section 2709 of title 18, United States Code));

“(ii) pertain to an individual who has been in contact with, or otherwise directly linked to, a suspected agent of a foreign power or an individual who is the subject of an ongoing and authorized national security investigation (other than an assessment); or

“(iii) pertain to the activities of a suspected agent of a foreign power, where those activities are the subject of an ongoing and authorized national security investigation (other than an assessment), and obtaining the records is the least intrusive means that could be used to identify per-
sons believed to be involved in the activities; and

“(C) a statement of proposed minimization procedures; and”;

(C) by adding at the end the following:

“(3) if the applicant is seeking a nondisclosure requirement described in subsection (d), shall include—

“(A) a statement of specific and articulable facts providing reason to believe that disclosure of particular information about the existence or contents of the order requiring the production of tangible things under this section during the applicable time period will result in—

“(i) endangering the life or physical safety of any person;

“(ii) flight from prosecution;

“(iii) destruction of or tampering with evidence;

“(iv) intimidation of potential witnesses;

“(v) interference with diplomatic relations; or

“(vi) otherwise seriously endangering the national security of the United States
by alerting a target, an associate of a target, or the foreign power of which the target is an agent, of the interest of the Government in the target;

“(B) an explanation of how the harm identified under subparagraph (A) is related to the authorized investigation to which the tangible things sought are relevant;

“(C) an explanation of how the nondisclosure requirement is narrowly tailored to address the specific harm identified under subparagraph (A); and

“(D) the time period during which the Government believes the nondisclosure requirement should apply.”.

(2) ORDER.—Section 501(c) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861(c)) is amended—

(A) in paragraph (1)—

(i) by striking “subsections (a) and (b)” and inserting “subsection (a) and paragraphs (1) and (2) of subsection (b) and that the proposed minimization procedures meet the definition of minimization procedures under subsection (g)”; and
(ii) by striking the last sentence and inserting the following: “If the judge finds that the requirements of subsection (b)(3) have been met, such order shall include a nondisclosure requirement, which may apply for not longer than 1 year, unless the facts justify a longer period of nondisclosure, subject to the principles and procedures described in subsection (d).”;

and

(B) in paragraph (2)—

(i) in subparagraph (C), by inserting before the semicolon “, if applicable”;

(ii) in subparagraph (D), by striking “and” at the end;

(iii) in subparagraph (E), by striking the period at the end and inserting “; and”;

(iv) by adding at the end the following:

“(F) shall direct that the minimization procedures be followed.”.

(3) NONDISCLOSURE.—Section 501(d) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861(d)) is amended to read as follows:
“(d) NONDISCLOSURE.—

“(1) IN GENERAL.—No person who receives an order under subsection (c) that contains a nondisclosure requirement shall disclose to any person the particular information specified in the nondisclosure requirement during the time period to which the requirement applies.

“(2) EXCEPTION.—

“(A) DISCLOSURE.—A person who receives an order under subsection (c) that contains a nondisclosure requirement may disclose information otherwise subject to any applicable nondisclosure requirement to—

“(i) those persons to whom disclosure is necessary in order to comply with an order under this section;

“(ii) an attorney in order to obtain legal advice or assistance regarding the order; or

“(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

“(B) APPLICATION.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure require-
ments applicable to a person to whom an order is directed under this section in the same manner as the person to whom the order is directed.

“(C) NOTIFICATION.—Any person who discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall notify the person of the applicable nondisclosure requirement.

“(3) EXTENSION.—The Director of the Federal Bureau of Investigation, or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge), may apply for renewals for the prohibition on disclosure of particular information about the existence or contents of an order requiring the production of tangible things under this section for additional periods of not longer than 1 year, unless the facts justify a longer period of nondisclosure. A nondisclosure requirement shall be renewed if a court having jurisdiction under paragraph (4) determines that the application meets the requirements of subsection (b)(3).

“(4) JURISDICTION.—An application for a renewal under this subsection shall be made to—

“(A) a judge of the court established under section 103(a); or
“(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of the court established under section 103(a).”.

(4) MINIMIZATION.—Section 501(g) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861(g)) is amended—

(A) in paragraph (1), by striking “Not later than” and all that follows and inserting “At or before the end of the period of time for the production of tangible things under an order approved under this section or at any time after the production of tangible things under an order approved under this section, a judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.”; and

(B) in paragraph (2)(A), by inserting “acquisition and” after “to minimize the”.
(5) USE OF INFORMATION.—Section 501(h) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861(h)) is amended to read as follows:

“(h) USE OF INFORMATION.—

“(1) IN GENERAL.—

“(A) CONSENT.—Any tangible things or information acquired from an order under this section concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required under this section.

“(B) USE AND DISCLOSURE.—No tangible things or information acquired under an order under this section may be used or disclosed by Federal officers or employees except for lawful purposes.

“(2) DISCLOSURE FOR LAW ENFORCEMENT PURPOSES.—No tangible things or information acquired from an order under this section shall be disclosed for law enforcement purposes unless the disclosure is accompanied by a statement that the tangible things or information, or any information derived therefrom, may only be used in a criminal pro-
ceeding with the advance authorization of the Attorney General.

“(3) NOTIFICATION OF INTENDED DISCLOSURE BY THE UNITED STATES.—Whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States against an aggrieved person any tangible things or information obtained or derived from an order under this section, the United States shall, before the trial, hearing, or other proceeding or at a reasonable time before an effort to so disclose or so use the tangible things or information or submit them in evidence, notify the aggrieved person and the court or other authority in which the tangible things or information are to be disclosed or used that the United States intends to so disclose or so use the tangible things or information.

“(4) NOTIFICATION OF INTENDED DISCLOSURE BY STATE OR POLITICAL SUBDIVISION.—Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory
body, or other authority of the State or political sub-
division thereof against an aggrieved person any tan-
gible things or information obtained or derived from
an order issued under this section, the State or po-
litical subdivision thereof shall notify the aggrieved
person, the court or other authority in which the
tangible things or information are to be disclosed or
used, and the Attorney General that the State or po-
litical subdivision thereof intends to so disclose or so
use the tangible things or information.

“(5) MOTION TO SUPPRESS.—

“(A) IN GENERAL.—Any aggrieved person
against whom evidence obtained or derived from
an order issued under this section is to be, or
has been, introduced or otherwise used or dis-
closed in any trial, hearing, or other proceeding
in or before any court, department, officer,
agency, regulatory body, or other authority of
the United States, or a State or political sub-
division thereof, may move to suppress the evi-
dence obtained or derived from the order, as the
case may be, on the grounds that—

“(i) the tangible things or information
were acquired in violation of the Constitu-
tion or laws of the United States; or
“(ii) the order was not issued in accordance with the requirements of this section.

“(B) Timing.—A motion under subparagraph (A) shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the aggrieved person concerned was not aware of the grounds of the motion.

“(6) Judicial review.—

“(A) In general.—In a circumstance described in subparagraph (B), a United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority shall, if the Attorney General files an affidavit under oath that disclosure would harm the national security of the United States, review in camera the application, order, and such other related materials relating to the order issued under this section as may be necessary to determine whether the order was lawfully authorized and served.
“(B) CIRCUMSTANCES.—A circumstance described in this subparagraph is a circumstance in which—

“(i) a court or other authority is notified under paragraph (3) or (4); 

“(ii) a motion is made under paragraph (5); or 

“(iii) any motion or request is made by an aggrieved person under any other statute or rule of the United States or any State before any court or other authority of the United States or any State to—

“(I) discover or obtain applications, orders, or other materials relating to an order issued under this section; or 

“(II) discover, obtain, or suppress evidence or information obtained or derived from an order issued under this section.

“(C) DISCLOSURE.—In making a determination under subparagraph (A), unless the United States district court finds that disclosure would not assist in determining any legal or factual issue pertinent to the case, the court
may disclose to the aggrieved person, the counsel for the aggrieved person, or both, under the procedures and standards provided in the Classified Information Procedures Act (18 U.S.C. App.) or other appropriate security procedures and protective orders, portions of the application, order, or other related materials, or evidence or information obtained or derived from the order.

“(7) Effect of determination of lawfulness.—

“(A) Unlawful orders.—If a United States district court determines under paragraph (6) that an order was not authorized or served in compliance with the Constitution or laws of the United States, the court may suppress the evidence which was unlawfully obtained or derived from the order or otherwise grant the motion of the aggrieved person.

“(B) Lawful orders.—If the court determines that an order issued under this section was lawfully authorized and served, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.
“(8) BINDING FINAL ORDERS.—An order granting a motion or request under paragraph (6), a decision under this section that an order issued under this section was not lawful, and an order of a United States district court requiring review or granting disclosure of an application, order, or other materials relating to an order issued under this section shall be a final order and binding upon all courts of the United States and the several States, except an appeal or petition to a United States court of appeals or the Supreme Court of the United States.”.

(6) DEFINITION.—

(A) IN GENERAL.—Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by adding at the end the following:

“SEC. 503. DEFINITIONS.

“In this title, the following definitions apply:

“(1) IN GENERAL.—Except as provided in this section, terms used in this title that are also used in title I shall have the meanings given those terms by section 101.

“(2) AGGRIEVED PERSON.—The term ‘aggrieved person’ means any person whose tangible
things or information were acquired under an order issued under this title.”.

(B) Technical and Conforming Amendment.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by inserting after the item relating to section 502 the following:

“Sec. 503. Definitions.”.

(b) Judicial Review of Section 215 Orders.—
Section 501(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) is amended to read as follows:

“(f) Judicial Review.—
“(1) Order for Production.—Not later than the earlier of 21 days after the date of service upon any person of an order issued under subsection (c) and the return date specified in the order, the person may file, in the court established under section 103(a) or in the United States district court for the judicial district within which the person resides, is found, or transacts business, a petition for the court to modify or set aside the order. The period for compliance with an order issued under subsection (c), or any portion of the order, shall be tolled while a petition under this paragraph is pending in the court. A petition under this paragraph shall specify each
ground upon which the petitioner relies in seeking relief, and may be based upon any failure of the order issued under subsection (c) to comply with this section or upon any constitutional or other legal right or privilege of the person.

“(2) NONDISCLOSURE ORDER.—

“(A) IN GENERAL.—A person prohibited from disclosing information under subsection (d) may file, in the court established under section 103(a) or in the United States district court for the judicial district within which the person resides, is found, or transacts business, a petition for the court to set aside the nondisclosure requirement. A petition under this subparagraph shall specify each ground upon which the petitioner relies in seeking relief, and may be based upon any failure of the nondisclosure requirement to comply with this section or upon any constitutional or other legal right or privilege of the person.

“(B) STANDARD.—The court shall modify or set aside a nondisclosure requirement unless the court determines that—

“(i) there is reason to believe that disclosure of the information subject to the
nondisclosure requirement during the applicable time period will result in—

“(I) endangering the life or physical safety of any person;

“(II) flight from prosecution;

“(III) destruction of or tampering with evidence;

“(IV) intimidation of potential witnesses;

“(V) interference with diplomatic relations; or

“(VI) otherwise seriously endangering the national security of the United States by alerting a target, an associate of a target, or the foreign power of which the target is an agent, of the interest of the Government in the target;

“(ii) the harm identified under clause (i) relates to the authorized investigation to which the tangible things sought are relevant; and

“(iii) the nondisclosure requirement is narrowly tailored to address the specific harm identified under clause (i).
“(3) Rulemaking.—

“(A) In general.—Not later than 180 days after the date of enactment of the JUSTICE Act, the court established under section 103(a) shall comply with section 103(g) by establishing any rules and procedures and taking any actions as are reasonably necessary to administer the responsibilities of the court under this subsection.

“(B) Reporting.—Not later than 30 days after the date on which the court promulgates rules and procedures under subparagraph (A), the court established under section 103(a) shall transmit a copy of the rules and procedures, in an unclassified form to the greatest extent possible (with a classified annex, if necessary), to the persons and entities listed in section 103(g)(2).

“(4) Disclosures to petitioners.—In making determinations under this subsection, unless the court finds that disclosure would not assist in determining any legal or factual issue pertinent to the case, the court may disclose to the petitioner, the counsel for the petitioner, or both, under the procedures and standards provided in the Classified Infor-
mation Procedures Act (18 U.S.C. App.) or other appropriate security procedures and protective orders, portions of the application, order, or other related materials.”.

(c) SUNSET REPEAL.—Section 102(b) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (Public Law 109–177; 50 U.S.C. 1805 note, 50 U.S.C. 1861 note, and 50 U.S.C. 1862 note) is repealed.

SEC. 108. TECHNICAL AND CONFORMING AMENDMENTS.

(a) TITLE 18.—Section 1510(e) of title 18, United States Code, is amended by striking “Whoever,” and all that follows through “knowingly” and inserting “Whoever, having been notified of the applicable disclosure prohibitions or confidentiality requirements of section 2709 of this title, section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u), section 1114 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414), or section 802 of the National Security Act of 1947 (50 U.S.C. 436), knowingly”.

(b) OTHER LAW.—Section 507(b) of the National Security Act of 1947 (50 U.S.C. 415b(b)) is amended—

(1) by striking paragraphs (4) and (5); and

(2) by redesignating paragraph (6) as paragraph (4).
TITLE II—REASONABLE SAFEGUARDS TO PROTECT THE PRIVACY OF AMERICANS’ HOMES

SEC. 201. LIMITATION ON AUTHORITY TO DELAY NOTICE OF SEARCH WARRANTS.

Section 3103a of title 18, United States Code, is amended—

(1) in subsection (b)—

(A) in paragraph (1), by striking “may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial)” and inserting “will endanger the life or physical safety of an individual, result in flight from prosecution, result in the destruction of or tampering with the evidence sought under the warrant, or result in intimidation of potential witnesses”; and

(B) in paragraph (3), by striking “30 days” and all that follows and inserting “7 days after the date of its execution.”;

(2) in subsection (c), by striking “for good cause shown” and all that follows and inserting “upon application of the Attorney General, the Deputy Attorney General, or an Associate Attorney Gen-
eral, for additional periods of not more than 21 days
for each application, if the court finds, for each ap-
application, reasonable cause to believe that notice of
the execution of the warrant will endanger the life
or physical safety of an individual, result in flight
from prosecution, result in the destruction of or
tampering with the evidence sought under the war-
rant, or result in intimidation of potential wit-
nesses.”;

(3) by redesignating subsection (d) as sub-
section (e); and

(4) by inserting after subsection (e) the fol-
lowing:

“(d) PROHIBITION ON USE AS EVIDENCE.—If any
property or material has been seized under subsection (b)
and notice has been delayed, the property or material and
any evidence derived therefrom may not be received in evi-
dence in any trial, hearing, or other proceeding in or be-
fore any court, grand jury, department, officer, agency,
regulatory body, legislative committee, or other authority
of the United States, a State, or a political subdivision
thereof if the property or material was obtained in viola-
tion of this section, or if notice required by this section
or by a warrant issued under this section was not provided
or was not timely provided.”.
TITLE III—REASONABLE SAFEGUARDS TO PROTECT THE PRIVACY OF AMERICANS’ COMMUNICATIONS

SEC. 301. LIMITATIONS ON ROVING WIRETAPS UNDER FOREIGN INTELLIGENCE SURVEILLANCE ACT.

Section 105(c) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(c)) is amended—

(1) in paragraph (1), by striking subparagraphs (A) and (B) and inserting the following:

“(A)(i) the identity of the target of the electronic surveillance, if known; or

“(ii) if the identity of the target is not known, a description of the specific target and the nature and location of the facilities and places at which the electronic surveillance will be directed;

“(B)(i) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known; or

“(ii) if any of the facilities or places are not known, the identity of the target;”; and

(2) in paragraph (2)—

(A) by redesignating subparagraphs (B) through (D) as subparagraphs (C) through (E), respectively; and
(B) by inserting after subparagraph (A) the following:

“(B) in cases where the facility or place at which the electronic surveillance will be directed is not known at the time the order is issued, that the electronic surveillance be conducted only for such time as it is reasonable to presume that the target of the surveillance is or was reasonably proximate to the particular facility or place;”.

SEC. 302. PRIVACY PROTECTIONS FOR PEN REGISTERS AND TRAP AND TRACE DEVICES.

(a) CRIMINAL AUTHORITY.—

(1) APPLICATION FOR AN ORDER.—Section 3122(b) of title 18, United States Code, is amended by striking paragraph (2) and inserting the following:

“(2) a statement by the applicant that the information likely to be obtained is—

“(A) relevant to an ongoing criminal investigation being conducted by that agency; and

“(B) there are specific and articulable facts providing reason to believe that the information—
“(i) pertains to an individual who is
the subject of an ongoing criminal inves-
tigation;
“(ii) pertains to an individual who has
been in contact with, or otherwise directly
linked to, an individual who is the subject
of an ongoing criminal investigation; or
“(iii) pertain to the activities of an in-
dividual who is the subject of an ongoing
criminal investigation, where those activi-
ties are the subject of an ongoing criminal
investigation, and obtaining the records is
the least intrusive means that could be
used to identify persons believed to be in-
volved in the activities.”.

(2) Issuance of an order.—Section 3123(a)
of title 18, United States Code, is amended—

(A) in paragraph (1), by striking “the at-
torney for the Government has certified to the
court that the information likely to be obtained
by such installation and use is relevant to an
ongoing criminal investigation.” and inserting
“the application meets the requirements of sec-
tion 3122.”; and
(B) in paragraph (2), by striking “the State law enforcement or investigative officer” and all that follows and inserting “the application meets the requirements of section 3122.”.

(3) REPORTING.—Section 3126 of title 18, United States Code, is amended—

(A) in the matter preceding paragraph (1), by striking “law enforcement agencies of the Department of Justice” and inserting “attorneys for the Government”; 

(B) in paragraph (4), by striking “and” at the end; 

(C) in paragraph (5), by striking the period and inserting a semicolon; 

(D) in the matter preceding paragraph (1), by striking “The Attorney General” and inserting the following: 

“(a) REPORT TO CONGRESS.—The Attorney General”; and 

(E) by adding at the end the following: 

“(6) whether the application for the order and the applications for any extensions were granted as applied for, modified, or denied;
“(7) the specific types of dialing, routing, addressing, or signaling information sought in the application and obtained with the order; and

“(8) a summary of any litigation to which the Government is or was a party regarding the interpretation of this chapter.

“(b) PUBLIC REPORT.—The Attorney General shall annually make public a full and complete report concerning the number of applications for pen register orders and orders for trap and trace devices applied for under this chapter and the number of the orders and extensions of the orders granted or denied under this chapter during the preceding calendar year. Each report under this subsection shall include a summary and analysis of the data required to be reported to Congress under subsection (a).”.

(4) NOTICE.—Section 3123 of title 18, United States Code, is amended by adding at the end the following:

“(e) NOTICE.—

“(1) INVENTORY.—A court that receives an application for an order or extension under section 3122(a) shall cause to be served on the persons named in the application, and any other party to communications the court determines should receive
notice in the interest of justice, an inventory, including—

“(A) the fact of the application for an order or extension under section 3122(a) and whether the court granted or denied the application; and

“(B) if the order or extension was granted—

“(i) the date of the entry of the order or extension and the period of authorized, approved, or disapproved use of the pen register or trap and trace device;

“(ii) whether a pen register or trap and trace device was installed or used during the period authorized; and

“(iii) the specific types of dialing, routing, addressing, or signaling information sought in the application and collected by the pen register or trap and trace device.

“(2) Timing.—The court shall serve notice under paragraph (1) within a reasonable time, but not later than 90 days after—
“(A) the date of the filing of the application for an order or extension under section 3122(a) that is denied; or

“(B) the date on which an order, or extensions thereof, that is granted terminates.

“(3) Delay.—The court may issue an ex parte order postponing the service of the inventory required under paragraph (1) upon a showing of good cause by an attorney for the Government.

“(4) Inspection.—Upon the filing of a motion, the court may make available for inspection by a person served under paragraph (1), or counsel for the person, such portions of the collected communications, applications, and orders as the court determines to be in the interest of justice.”.

(b) Foreign Intelligence Authority.—

(1) Application.—Section 402(c) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842(c)) is amended—

(A) in paragraph (1), by striking “and” at the end; and

(B) by striking paragraph (2) and inserting the following:

“(2) a statement by the applicant that—
“(A) the records sought are relevant to an ongoing and authorized national security investigation (other than an assessment (as defined in section 2709 of title 18, United States Code)); and

“(B) there are specific and articulable facts providing reason to believe that the records—

“(i) pertain to a suspected agent of a foreign power or an individual who is the subject of an ongoing and authorized national security investigation (other than an assessment);

“(ii) pertain to an individual who has been in contact with, or otherwise directly linked to, a suspected agent of a foreign power or an individual who is the subject of an ongoing and authorized national security investigation (other than an assessment); or

“(iii) pertain to the activities of a suspected agent of a foreign power, where those activities are the subject of an ongoing and authorized national security investigation (other than an assessment), and
obtaining the records is the least intrusive means that could be used to identify persons believed to be involved in the activities; and

“(3) a statement of proposed minimization procedures.”.

(2) **MINIMIZATION.**—

(A) **DEFINITION.**—Section 401 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1841) is amended by adding at the end the following:

“(4) The term ‘minimization procedures’ means—

“(A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the installation and use of a pen register or trap and trace device, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

“(B) procedures that require that nonpublicly available information, which is not foreign
intelligence information, as defined in section 101(e)(1), shall not be disseminated in a manner that identifies any United States person, without such person’s consent, unless such person’s identity is necessary to understand foreign intelligence information or assess its importance; and

“(C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.”.

(B) **Pen registers and trap and trace devices.**—Section 402 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842) is amended—

(i) in subsection (d)—

(I) in paragraph (1), by inserting “, and that the proposed minimization procedures meet the definition of minimization procedures under this title” before the period at the end; and
(II) in paragraph (2)(B)—

(aa) in clause (ii)(II), by striking “and” after the semi-colon; and

(bb) by adding at the end the following:

“(iv) the minimization procedures be followed; and”; and

(ii) by adding at the end the following:

“(h) At or before the end of the period of time for which the installation and use of a pen register or trap and trace device is approved under an order or an extension under this section, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.”.

(C) EMERGENCIES.—Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended—

(i) by redesignating subsection (c) as (d); and

(ii) by inserting after subsection (b) the following:
“(c) If the Attorney General authorizes the emergency installation and use of a pen register or trap and trace device under this section, the Attorney General shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.”.

(D) USE OF INFORMATION.—Section 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1845(a)) is amended by striking “provisions of” and inserting “minimization procedures required under”.

SEC. 303. REPEAL OF TELECOMMUNICATIONS IMMUNITY.

(a) IN GENERAL.—The Foreign Intelligence Surveillance Act of 1978 is amended by striking title VIII (50 U.S.C. 1885 et seq.).

(b) RULE OF CONSTRUCTION.—Nothing in the amendments made by this section shall be construed to affect any limitation on liability otherwise provided under titles I through VII of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), title 18, United States Code, or the Protect America Act of 2007 (Public Law 110–55; 121 Stat. 552) or the amendments made by that Act.

(e) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et
seq.) is amended by striking the items relating to title VIII and sections 801, 802, 803, and 804.

SEC. 304. PROHIBITION ON BULK COLLECTION UNDER FISA AMENDMENTS ACT.

Section 702(g)(2)(A) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(g)(2)(A)) is amended—

(1) in clause (vi), by striking “and” at the end;

(2) by redesignating clause (vii) as clause (viii);

and

(3) by inserting after clause (vi) the following:

“(vii) the acquisition of the contents (as that term is defined in section 2510(8) of title 18, United States Code)) of any communication is limited to communications to which any party is an individual target (which shall not be limited to known or named individuals) who is reasonably believed to be located outside of the United States, and a significant purpose of the acquisition of the communications of the target is to obtain foreign intelligence information; and”.


SEC. 305. PROHIBITION ON REVERSE TARGETING UNDER FISA AMENDMENTS ACT.

Section 702 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a) is amended—

(1) in subsection (b)(2), by striking “the purpose” and all that follows and inserting the following: “a significant purpose of the acquisition is to acquire the communications of a particular, known person reasonably believed to be located in the United States, except in accordance with title I;”;

(2) in subsection (d)(1)(A)—

(A) by striking “ensure that” and insert the following: “ensure—

“(i) that”; and

(B) by adding at the end the following:

“(ii) that an application is filed under title I, if otherwise required, when a significant purpose of an acquisition authorized under subsection (a) is to acquire the communications of a particular, known person reasonably believed to be located in the United States; and’’;

(3) in subsection (g)(2)(A)(i)(I)—

(A) by striking “ensure that” and insert the following: “ensure—

“(aa) that”; and
(B) by adding at the end the following:

“(bb) that an application is filed under title I, if otherwise required, when a significant purpose of an acquisition authorized under subsection (a) is to acquire the communications of a particular, known person reasonably believed to be located in the United States; and”;

and

(4) in subsection (i)(2)(B)(i)—

(A) by striking “ensure that” and insert the following: “ensure—

“(I) that”; and

(B) by adding at the end the following:

“(II) that an application is filed under title I, if otherwise required, when a significant purpose of an acquisition authorized under subsection (a) is to acquire the communications of a particular, known person reasonably believed to be located in the United States; and”.
SEC. 306. LIMITS ON USE OF UNLAWFULLY OBTAINED INFORMATION UNDER FISA AMENDMENTS ACT.

Section 702(i)(3) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(i)(3)) is amended by striking subparagraph (B) and inserting the following:

"(B) CORRECTION OF DEFICIENCIES.—

"(i) IN GENERAL.—If the Court finds that a certification required by subsection (g) does not contain all of the required elements, or that the procedures required by subsections (d) and (e) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government’s election and to the extent required by the order of the Court—

"(I) correct any deficiency identified by the order of the Court not later than 30 days after the date on which the Court issues the order; or

"(II) cease the acquisition authorized under subsection (a).

"(ii) LIMITATION ON USE OF INFORMATION.—
“(I) IN GENERAL.—Except as provided in subclause (II), no information obtained or evidence derived from an acquisition under clause (i)(I) concerning any United States person shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from the acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of the United States person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

“(II) EXCEPTION.—If the Government corrects any deficiency iden-
tified by the order of the Court under clause (i), the Court may permit the use or disclosure of information acquired before the date of the correction under such minimization procedures as the Court shall establish for purposes of this clause.”.

SEC. 307. PRIVACY PROTECTIONS FOR INTERNATIONAL COMMUNICATIONS OF AMERICANS COLLECTED UNDER FISA AMENDMENTS ACT.

(a) In General.—Title VII of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881) is amended by adding at the end the following:

“SEC. 709. ADDITIONAL SAFEGUARDS FOR COMMUNICATIONS OF PERSONS IN THE UNITED STATES.

“(a) Limitations on Acquisition of Communications.—

“(1) Limitation.—Except as authorized under title I or paragraph (2), no communication shall be acquired under this title if the Government knows before or at the time of acquisition that the communication is to or from a person reasonably believed to be located in the United States.

“(2) Exception.—
“(A) IN GENERAL.—In addition to any authority under title I to acquire communications described in paragraph (1), the communications may be acquired if—

“(i) there is reason to believe that the communication concerns international terrorist activities directed against the United States, or activities in preparation therefore;

“(ii) there is probable cause to believe that the target reasonably believed to be located outside the United States is an agent of a foreign power and the foreign power is a group engaged in international terrorism or activities in preparation therefore; or

“(iii) there is reason to believe that the acquisition is necessary to prevent death or serious bodily harm.

“(B) ACCESS TO COMMUNICATIONS.—Communications acquired under this paragraph shall be treated in accordance with subsection (b).

“(3) PROCEDURES FOR DETERMINATIONS BEFORE OR AT THE TIME OF ACQUISITION.—
“(A) Submission.—Not later than 120 days after the date of enactment of the JU- TICE Act, the Attorney General, in consulta- tion with the Director of National Intelligence, shall submit to the Foreign Intelligence Surveil- lance Court for approval procedures for deter- mining before or at the time of acquisition, where reasonably practicable, whether a com- munication is to or from a person reasonably believed to be located in the United States and whether the exception under paragraph (2) ap- plies to that communication.

“(B) Review.—The Foreign Intelligence Surveillance Court shall approve the procedures submitted under subparagraph (A) if the proce- dures are reasonably designed to determine be- fore or at the time of acquisition, where reason- ably practicable, whether a communication is to or from a person reasonably believed to be lo- cated in the United States and whether the ex- ception under paragraph (2) applies to that communication.

“(C) Procedures do not meet re- quirements.—If the Foreign Intelligence Sur- veillance Court concludes that the procedures
submitted under subparagraph (A) do not meet the requirements of subparagraph (B), the Court shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph to the Foreign Intelligence Surveillance Court of Review.

“(D) USE OF PROCEDURES.—If the Foreign Intelligence Surveillance Court approves procedures under this paragraph, the Government shall use the procedures in any acquisition of communications under this title.

“(E) REVISIONS.—The Attorney General, in consultation with the Director of National Intelligence, may submit new or amended procedures to the Foreign Intelligence Surveillance Court for review under this paragraph.

“(F) RELIABILITY.—If the Government obtains new information relating to the reliability of procedures approved under this paragraph or the availability of more reliable procedures, the Attorney General shall submit to the Foreign Intelligence Surveillance Court the information.
“(b) LIMITATIONS ON ACCESS TO COMMUNICATIONS.—

“(1) IN GENERAL.—At such time as the Government can reasonably determine that a communication acquired under this title (including a communication acquired under subsection (a)(2)) is to or from a person reasonably believed to be located in the United States, the communication shall be segregated or specifically designated and no person shall access the communication, except in accordance with title I or this section.

“(2) EXCEPTIONS.—In addition to any authority under title I, including the emergency provision in section 105(f), a communication described in paragraph (1) may be accessed and disseminated for a period of not longer than 7 days if—

“(A)(i) there is reason to believe that the communication concerns international terrorist activities directed against the United States, or activities in preparation therefor;

“(ii) there is probable cause to believe that the target reasonably believed to be located outside the United States is an agent of a foreign power and the foreign power is a group engaged
in international terrorism or activities in preparation therefor; or

“(iii) there is reason to believe that the access is necessary to prevent death or serious bodily harm;

“(B) the Attorney General notifies the Foreign Intelligence Surveillance Court immediately of the access; and

“(C) not later than 7 days after the date the access is initiated, the Attorney General—

“(i) makes an application for an order under title I; or

“(ii) submits to the Foreign Intelligence Surveillance Court a document that—

“(I) certifies that—

“(aa) there is reason to believe that the communication concerns international terrorist activities directed against the United States, or activities in preparation therefor;

“(bb) there is probable cause to believe that the target reasonably believed to be located
outside the United States is an
agent of a foreign power and the
foreign power is a group engaged
in international terrorism or ac-
tivities in preparation therefor; or

“(cc) there is reason to be-
lieve that the access is necessary
to prevent death or serious bodily
harm; and

“(II) identifies the target of the
collection, the party to the commu-
ication who is in the United States if
known, and the extent to which infor-
mation relating to the communication
has been disseminated.

“(3) DENIAL OF COURT ORDER.—If an applica-
tion for a court order described in paragraph
(2)(C)(i) is made and is not approved, the Attorney
General shall submit to the Foreign Intelligence Sur-
veillance Court, not later than 7 days after the date
of the denial of the application, the document de-
scribed in paragraph (2)(C)(ii).

“(4) ADDITIONAL COURT AUTHORITIES.—

“(A) IN GENERAL.—The Foreign Intel-
ligence Surveillance Court may—
“(i) limit access to communications described in paragraph (1) relating to a particular target if the Court determines that any certification submitted under paragraph (2)(C)(ii)(I) with respect to that target is clearly erroneous; and

“(ii) require the Attorney General to provide the factual basis for a certification submitted under paragraph (2)(C)(ii)(I), if the Court determines it would aid the Court in conducting review under this subsection.

“(B) FISC ACCESS.—The Foreign Intelligence Surveillance Court shall have access to any communications that have been segregated or specifically designated under paragraph (1) and any information the use of which has been limited under paragraph (5).

“(5) FAILURE TO NOTIFY.—

“(A) IN GENERAL.—In the circumstances described in subparagraph (B), access to a communication shall terminate, and no information obtained or evidence derived from the access concerning any United States person shall be received in evidence or otherwise disclosed in
any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from the access shall subsequently be used or disclosed in any manner by Federal officers or employees without the consent of the person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person, or if a court order is obtained under title I.

“(B) CIRCUMSTANCES.—The circumstances described in this subparagraph are circumstances in which—

“(i) as of the date that is 7 days after the date on which access to a communication is initiated under paragraph (2), a court order described in paragraph (2)(C)(i) has not been sought and the document described in paragraph (2)(C)(ii) has not been submitted; or
“(ii) as of the date that is 7 days after an application for a court order described in paragraph (2)(C)(i) is denied, the document described in paragraph (2)(C)(ii) is not submitted in accordance with paragraph (3).

“(6) EVIDENCE OF A CRIME.—Information or communications subject to this subsection may be disseminated for law enforcement purposes if it is evidence that a crime has been, is being, or is about to be committed, if dissemination is made in accordance with section 106(b).

“(7) PROCEDURES FOR DETERMINATIONS AFTER ACQUISITION.—

“(A) IN GENERAL.—Not later than 120 days after the date of enactment of the JUSTICE Act, the Attorney General, in consultation with the Director of National Intelligence, shall submit to the Foreign Intelligence Surveillance Court for approval procedures for determining, where reasonably practicable, whether a communication acquired under this title is to or from a person reasonably believed to be in the United States.
“(B) REVIEW.—The Foreign Intelligence Surveillance Court shall approve the procedures submitted under subparagraph (A) if the procedures are reasonably designed to determine, where reasonably practicable, whether a communication acquired under this title is a communication to or from a person reasonably believed to be located in the United States.

“(C) PROCEDURES DO NOT MEET REQUIREMENTS.—If the Foreign Intelligence Surveillance Court concludes that the procedures submitted under subparagraph (A) do not meet the requirements of subparagraph (B), the Court shall enter an order so stating and provide a written statement for the record of the reasons for the determination. The Government may appeal an order under this subparagraph to the Foreign Intelligence Surveillance Court of Review.

“(D) USE OF PROCEDURES.—If the Foreign Intelligence Surveillance Court approves procedures under this paragraph, the Government shall use the procedures for any communication acquired under this title.
“(E) Revisions.—The Attorney General, in consultation with the Director of National Intelligence, may submit new or amended procedures to the Foreign Intelligence Surveillance Court for review under this paragraph.

“(F) Reliability.—If the Government obtains new information relating to the reliability of procedures approved under this paragraph or the availability of more reliable procedures, the Attorney General shall submit to the Foreign Intelligence Surveillance Court the information.

“(c) Title I Court Order.—If the Government obtains a court order under title I relating to a target of an acquisition under this title, the Government may access and disseminate, under the terms of that court order and any applicable minimization requirements, any communications of that target that have been acquired and segregated or specifically designated under subsection (b)(1).

“(d) Inspector General Audit.—

“(1) Audit.—Not less than once each year, the Inspector General of the Department of Defense and the Inspector General of the Department of Justice shall complete an audit of the implementation of and compliance with this section. For purposes of an
audit under this paragraph, the Inspectors General shall have access to any communications that have been segregated or specifically designated under subsection (b)(1) and any information the use of which has been limited under subsection (b)(5). An audit under this paragraph shall include an accounting of any segregated or specifically designated communications that have been disseminated.

“(2) REPORT.—Not later than 30 days after the completion of each audit under paragraph (1), the Inspectors General shall jointly submit to the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives and the Select Committee on Intelligence and the Committee on the Judiciary of the Senate a report containing the results of the audit.

“(3) EXPEDITED SECURITY CLEARANCE.—The Director of National Intelligence shall ensure that the process for the investigation and adjudication of an application by an Inspector General or any appropriate staff of an Inspector General for a security clearance necessary for the conduct of the audits under this subsection is conducted as expeditiously as possible.
“(e) APPLICABILITY.—Subsections (a) and (b) shall apply to any communication acquired under this title on or after the earlier of—

“(1) the date that the Foreign Intelligence Surveillance Court approves the procedures described in subsection (a)(3) and the procedures described in subsection (b)(7); and

“(2) 1 year after the date of enactment of the JUSTICE Act.”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—

The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by inserting after the item relating to section 708 the following:

“Sec. 709. Additional safeguards for communications of persons in the United States.”.

SEC. 308. CLARIFICATION OF COMPUTER TRESPASS AUTHORITY.

(a) DEFINITIONS.—Section 2510(21)(B) of title 18, United States Code, is amended—

(1) by inserting “or other” after “contractual”; and

(2) by striking “for access” and inserting “permitting access”.

(b) INTERCEPTION AND DISCLOSURE.—Section 2511(2)(i) of title 18, United States Code, is amended—
(1) in subclause (I), by striking “protected computer authorizes” and inserting the following: “protected computer—

“(aa) is attempting to respond to communications activity that threatens the integrity or operation of the protected computer and requests assistance to protect the rights and property of the owner or operator; and

“(bb) authorizes”; and

(2) in clause (IV), by striking “interception does not” and inserting the following: “interception—

“(aa) ceases as soon as the communications sought are obtained or after 96 hours, whichever is earlier (unless an order authorizing or approving the interception is obtained under this chapter); and

“(bb) does not”.

(c) REPORT.—Not later than 60 days after the date of enactment of this Act, and annually thereafter, the Attorney General shall submit a report to the Committee on the Judiciary of the Senate and the Committee on the Ju-
diciary of the House of Representatives on the use of section 2511 of title 18, United States Code, relating to computer trespass provisions, as amended by subsection (b), during the year before the year of that report.

**TITLE IV—IMPROVEMENTS TO FURTHER CONGRESSIONAL AND JUDICIAL OVERSIGHT**

**SEC. 401. PUBLIC REPORTING ON THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.**

Section 601 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871) is amended—

(1) by redesignating subsections (b) through (e) as subsections (c) through (f), respectively;

(2) by inserting after subsection (a) the following:

“(b) PUBLIC REPORT.—The Attorney General shall make publicly available the portion of each report under subsection (a) relating to paragraphs (1) and (2) of subsection (a).”; and

(3) in subsection (c), as so redesignated, by striking “subsection (c)” and inserting “subsection (d)”. 
SEC. 402. USE OF FOREIGN INTELLIGENCE SURVEILLANCE ACT MATERIALS.

(a) ELECTRONIC SURVEILLANCE.—Section 106(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1806(f)) is amended by striking the last sentence and inserting “In making this determination, unless the court finds that disclosure would not assist in determining any legal or factual issue pertinent to the case, the court may disclose to the aggrieved person, the counsel for the aggrieved person, or both, under the procedures and standards provided in the Classified Information Procedures Act (18 U.S.C. App.) or other appropriate security procedures and protective orders, portions of the application, order, or other related materials, or evidence or information obtained or derived from the order.”.

(b) PHYSICAL SEARCHES.—Section 305(g) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1825(g)) is amended by striking the last sentence and inserting “In making this determination, unless the court finds that disclosure would not assist in determining any legal or factual issue pertinent to the case, the court may disclose to the aggrieved person, the counsel for the aggrieved person, or both, under the procedures and standards provided in the Classified Information Procedures Act (18 U.S.C. App.) or other appropriate security procedures and protective orders, portions of the application,
order, or other related materials, or evidence or information obtained or derived from the order.”.

(c) Pen Registers and Trap and Trace Devices.—Section 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1845(f)) is amended by striking paragraph (2) and inserting the following:

“(2) In making a determination under paragraph (1), unless the court finds that disclosure would not assist in determining any legal or factual issue pertinent to the case, the court may disclose to the aggrieved person, the counsel for the aggrieved person, or both, under the procedures and standards provided in the Classified Information Procedures Act (18 U.S.C. App.) or other appropriate security procedures and protective orders, portions of the application, order, or other related materials, or evidence or information obtained or derived from the order.”.

SEC. 403. CHALLENGES TO NATIONWIDE ORDERS FOR ELECTRONIC EVIDENCE.

Section 2703 of title 18, United States Code, is amended by adding at the end the following:

“(h) Judicial Review.—A provider of electronic communication service or remote computing service may challenge a subpoena, order, or warrant requiring disclosure of customer communications or records under this section in—
“(1) the United States district court for the district in which the order was issued; or
“(2) the United States district court for the district in which the order was served.”.

TITLE V—IMPROVEMENTS TO FURTHER EFFECTIVE, FOCUSED INVESTIGATIONS

SEC. 501. MODIFICATION OF DEFINITION OF DOMESTIC TERRORISM.

Section 2331(5) of title 18, United States Code, is amended—

(1) by striking subparagraphs (A) and (B) and inserting the following:

“(A) involve acts dangerous to human life that constitute a Federal crime of terrorism (as that term is defined in section 2332b(g)(5)); and”;

(2) by redesignating subparagraph (C) as subparagraph (B).

SEC. 502. CLARIFICATION OF INTENT REQUIREMENT.

Section 2339B(a)(1) of title 18, United States Code, is amended by inserting “knowing or intending that the material support or resources will be used in carrying out terrorist activity (as defined in section 212(a)(3)(B)(iii)

1

2