CHAPTER THIRTEEN
Reform of the National Security Surveillance Laws and Procedures

I. The Problem

The Foreign Intelligence Surveillance Act (FISA) as enacted in 1978 permitted targeted surveillance to collect foreign intelligence information and protect national security. The PATRIOT Act upset the balance established in FISA and permitted surveillance to be conducted in criminal investigations without a showing of criminal probable cause to a judge. The PATRIOT Act also permitted roving FISA wiretaps that violate the specificity and nexus requirements of the Fourth Amendment. Roving FISA wiretap orders are not required to specify the target or the communications facility (such as a telephone) to be surveilled. The FISA Amendments Act of 2008 further diminished FISA safeguards. The FAA permits the interception in the U.S. of communications that Americans have with non-citizens who are abroad without adequate judicial supervision of such surveillance. The FAA also permits that surveillance to occur on a massive scale: if resources permit, the FISA Amendments Act allows the NSA to collect in bulk the international communications that Americans have with non-citizens abroad.

Moreover, even with the significant revisions to the FISA, President Bush asserted virtually unlimited authority under Article II of the Constitution, and secretly authorized the NSA to engage in a warrantless wiretapping program that violated FISA and the Constitution. Telecommunications carriers that assisted in that surveillance program were granted immunity from civil liability, thus leaving those whose rights were violated without any legal remedy against the carriers and inviting them to assist with unlawful surveillance in the future.

Further, in the post-9/11 era, federal agencies turned from the traditional Title III authority to conduct electronic surveillance in the United States and made increasing use of FISA to obtain personal information in the possession of third parties. As a consequence, there was less scrutiny and less accountability of the searches undertaken by the government of US citizens.

Strong statutory provisions, including judicial review, clear standards for lawful surveillance, limitations on the scope and duration of surveillance, formal reporting requirements, as well congressional oversight, and a commitment by the President to follow the law are critical to protect the rights of Americans and ensure that the intelligence agencies are acting effectively and within the law. In the absence of meaningful and enforceable Fourth Amendment standards, government intelligence surveillance activity is subject to abuse.

II. Proposed Solutions

A. Guiding Principles

The Fourth Amendment standards articulated in FISA and related federal wiretap laws, such as ECPA, should govern intelligence surveillance conducted in the United States. The President is bound by FISA, and a court order based on probable cause should be required when surveillance is conducted in the U.S. for intelligence purposes. Telecommunications carriers must be expected to comply with statutory standards to prevent misuse of wiretap authority. They can provide a backstop for illegal surveillance because surveillance usually cannot be conducted without their help.

B. **Proposed Measures**

1. Congressional leaders should commence a comprehensive investigation of domestic intelligence activities. The investigation should seek to uncover illegal or inappropriate surveillance and prevent it from recurring, and it should include an assessment of the effectiveness of new authorities granted in the USA PATRIOT Act and the FISA Amendments Act. This review should provide the basis for congressional consideration of the USA PATRIOT Act provisions that would otherwise expire on December 31, 2009. The review may also identify other civil liberties issues that warrant changes to FISA.

2. President-elect Obama should announce early in the first 100 days of his administration that it is the policy of his administration to:

   i. Adhere to FISA's judicial warrant requirements when engaging in surveillance in the United States;
   ii. Comply fully with all intelligence surveillance statutes, and specifically with FISA, and to assert no power under Article II of the Constitution to engage in domestic intelligence gathering that does not fully comply with the law;
   iii. Publicly disclose the government documents, including the opinions of the DOJ Office of Legal Counsel, that provided the legal basis for the NSA's warrantless surveillance program;
   iv. Direct the Attorney General to withdraw the government's motion to dismiss pending privacy litigation brought against telecommunications carriers for assisting with unlawful warrantless surveillance, or seek a stay of those proceedings until such time as the Attorney General, based on review of the Inspectors' General reports required by the FISA Amendments Act, determines that a grant of immunity is appropriate;
   v. Refrain from using the FISA Amendments Act to engage in bulk collection of Americans' communications, whether domestic or international; and
   vi. Cooperate fully with any investigation of post 9-11 warrantless surveillance.

3. As President, Mr. Obama should work with Congress to amend FISA in his first year in office to:

   i. Ensure that surveillance authorized under FISA does not undermine the Fourth Amendment's requirement of probable cause of crime and that it complies with all Fourth Amendment standards;
   ii. Repeal Title II of the FISA Amendments Act:
   iii. Strengthen FISA's exclusivity provisions to ensure that telecommunications firms that provide assistance with surveillance in the future are given immunity only when the surveillance is authorized by the FISA court or is conducted under a specific, articulated statutory exception to the court order requirement;
   iv. Require that applications for roving intelligence wiretaps specify either the target of surveillance or the telephone or other communications facility to be surveilled;
   v. Amend the FISA Amendments Act to require judicial authorization of surveillance and more searching judicial review of such surveillance, and to bar bulk collection of Americans' international communications;
   vi. Implement additional civil liberties safeguards, including possibly, civil liberties recommendations that may be contained in the Inspectors General report on the FISA Amendments Act, due in July 2009; and
   vii. Improve public reporting and transparency so that the effectiveness of FISA surveillance can be evaluated.

4. President Obama should support inclusion of many of these reforms in any legislation that is proposed to reauthorize the FISA provisions that expire at the end of 2009.

III. Allies*

American Association of Law Libraries
Mary Alice Baish, Acting Washington Affairs Representative
baish@law.georgetown.edu
202-662-9200

American Library Association
Lynne E. Bradley, Director
lbradley@alawash.org
202-682-8410
The ALA Policy Manual: The Rights of Library Users and the USA Patriot Act (52.4.5) *available at* http://www.ala.org/ala/aboutala/governance/policymanual/policymanual.31_3.pdf

Association of Research Libraries
Prudence Adler

prue@arl.org
202-296-2296 (ext. 104)

Bill of Rights Defense Committee (BORDC)
Chip Pitts, President
chip.pitts@att.net

Center for Democracy & Technology
Gregory T. Nojeim
gnojeim@cdt.org
202-637-9800 (ext 113)
The Internet in Transition, *available at* http://www.cdt.org/election2008/

Common Cause
Sarah Dufendach, Vice President for Legislative Affairs
www.commoncause.org
202-736-5709

Defending Dissent Foundation
Sue Udry, Director
Sue.udry@defendingdissent.org
202-549-4225
www.defendingdissent.org

Electronic Frontier Foundation (EFF)
Kevin S. Bankston
bankston@eff.org
415-436-9333 (ext.126)
A Privacy Agenda for the New Administration, *available at* http://www.eff.org/deeplinks/2008/11/privacy-agenda

Essential Information
John Richard or Robert Weissman
202-387-8034

Government Accountability Project
Jesselyn Radack, Homeland Security Director
JesselynR@whistleblower.org
202-408-0034 (ext. 107)

Liberty Coalition
Michael D. Ostrolenk, Co-Founder/National Director
www.libertycoalition.net
mostrolenk@libertycoalition.net
301-717-0599

Muslim Advocates
Shahid Buttar
shahid@muslimadvocates.org
415-692-1512

National Coalition Against Censorship
Joan E. Bertin, Esq., Executive Director
bertin@ncac.org
212-807-6222
Fax: 212-807-6245

OMB Watch
Sean Moulton, Director, Federal Information Policy
202-234-8494
Fax: 202- 234-8584

OpenTheGovernment.org
Patrice McDermott
pmcdermott@openthegovernment.org
202-332-6736

South Asian Americans Leading Together
Priya Murthy
priya@saalt.org
301-270-1855

U.S. Bill of Rights Foundation
Dane vonBreichenruchardt, President
usbor@aol.com
202-546-7079

* These groups and individuals support the general principles expressed and the general policy thrust and judgments in the policy proposals described above. The allies listed do not necessarily endorse the specific language in every proposed solution, but they do agree that the proposals reflect the general principles that should govern policy in this area. Please contact the individuals and organizations listed in this section for more information

IV. Counter-Arguments and Rebuttal:

Agencies of the federal government engaged in intelligence surveillance, such as the FBI/Department of Justice, the National Security Agency, and the Office of the Director of National Intelligence will likely oppose measures to require more judicial oversight of their surveillance activities. However, history has shown that in many cases, judicial oversight is the measure most likely to prevent abuse of surveillance powers.

Telecommunications providers will oppose the repeal of the immunity provisions of the FISA Amendments Act because they could be subjected to substantial civil liability. They will argue that they responded to a call from the President at a time of great national concerns and should not be punished for their patriotism. But the purpose of FISA, and other similar privacy laws, is precisely to make clear the circumstances under which private sector entities may disclose customer information to the government. FISA even anticipated the declaration of war and made special allowances. But the President and the telephone companies disregarded this provision and others when they went forward with the warrantless surveillance program. Because national security concerns test the rule of law, it is particularly important that the statutory requirements be observed and the procedures set out by the Congress for surveillance in the United States be followed.

V. Recommended Documents for Further Information:

a. *Piercing the "Historical Mists" of FISA*, 17 STAN. L. & POL'Y REV. 101 (2006), *available at* http://2009transition.org/liberty-security/administrator/index2.php?option=com_docman&section=documents&task=download&bid=7

b. The Constitution Project, *Statement on the National Security Agency's Domestic Surveillance, available at* http://www.constitutionproject.org/libertyandsecurity/article.cfm?messageID=401&categoryid=6

c. Electronic Privacy Information Center: Foreign Intelligence Surveillance Act http://epic.org/privacy/terrorism/fisa/

d. Electronic Privacy Information Center: FISA Orders 1979-2007 http://epic.org/privacy/wiretap/stats/fisa_stats.html

e. Center for Democracy & Technology: FISA and warrantless snooping: http://www.cdt.org/security/nsa/briefingbook.php

f. Electronic Frontier Foundation: Telecom immunity in the FISA Amendments Act: http://www.eff.org/issues/nsa-spying/archive

g. Electronic Frontier Foundation: NSA spying and litigation related to it: http://www.eff.org/issues/nsa-spying

h. The President's lack of authority under Article II of the Constitution to engage in warrantless surveillance:
   i. Letter from law professors to Congress questioning the legality of the NSA warrantless surveillance program (Jan. 9, 2006)
   ii. DOJ Memorandum in support of the NSA warrantless surveillance program (Jan. 19, 2006)

iii. Second letter from law professors to Congress responding to and questioning DOJ's analysis of the legality of NSA warrantless surveillance (Feb. 2, 2006)

i. Documents that President-elect Obama should consider releasing to the public, with classified information redacted:
   i. List of Most Wanted Surveillance Documents compiled by Center for Democracy & Technology (link to http://www.cdt.org/security/20070620wanteddocs.php)

j. Jim Dempsey, Center for Democracy & Technology, *Does "Targeting" Warrant the Vacuum Cleaner*, (June 25, 2008) *at* http://blog.cdt.org/2008/06/25/does-targeting-authorize-the-vacuum-cleaner/

k. Congressional Research Service reports on FISA:
   i. *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions*, Congressional Research Service Report (Sept. 22, 2004)
   ii. *The Foreign Intelligence Surveillance Act: An Overview of Selected Issues*, Congressional Research Service Report (July 7, 2008)

l. Books about executive power that have information about warrantless wiretapping:
   i. Jack Goldsmith, The Terror President (2007)
   ii. Charlie Savage, The Return of the Imperial Presidency (2007)

m. Text of Foreign Intelligence Surveillance Act – 50 U.S.C. §§ 1801 *et seq.* (current as of Jan. 2, 2006)
   i. 50 U.S.C. § 1801-1811 – Electronic Surveillance
   ii. 50 U.S.C. § 1821-1829 – Physical Searches
   iii. 50 U.S.C. § 1841-1846 – Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes
   iv. 50 U.S.C. § 1861-1863 – Access to Certain Business Records for Foreign Intelligence Purposes
   v. 50 U.S.C. § 1871 – Reporting Requirement

   *These statutory provisions are current as of Jan. 2, 2006, the latest published volume of the U.S. Code. The provisions were amended in the 110th Congress by the FISA Amendments Act of 2008 (H.R. 6304, Pub. L. 110-261), signed into law on July 10, 2008.

APPENDIX
LEGISLATIVE, EXECUTIVE, AND JUDICIAL ACTION
on
REFORM OF NATIONAL SECURITY SURVEILLANCE LAWS AND PROCEDURES

I. Jurisdiction:

A. **Congress**. Congress has the authority to enact the legislation necessary to reform FISA. The intelligence and judiciary committees in both the House and Senate share authority over any such legislation.

B. **Executive Branch**. Even without Congressional action, the President can take a substantial step by simply declaring that he will refrain from exercising any power he might have under Article II of the Constitution to engage in domestic intelligence surveillance outside the standards set by Congress. The Department of Justice and other elements of the Intelligence Community such as the NSA and the Director of National Intelligence would be involved in consideration of the reforms outlined above.

II. Status of Actions in Legislative, Executive and Judicial Branches:

A. **Legislative*:*** The Foreign Intelligence Surveillance Act (FISA) was enacted into law on October 25, 1978 as P.L. 95-511. It has been amended on a number of occasions over the years.

In the 110th Congress, on August 5, 2007, Congress passed and the President signed the Protect America Act (S. 1927, Pub. L. 110-55), which construed the term "electronic surveillance" under FISA not to include surveillance directed at a person reasonably believed to be located outside the U.S. regardless of the extent to which that person communicated with people in the U.S. It provided for warrantless surveillance of such persons if certain requirements were met. The bill was scheduled to sunset on February 1, 2008. In the face of that sunset, Congress passed and the President signed H.R. 5104, Pub. L. 110-182, which extended the Protect America Act by 15 days. On February 17, 2008, Congress allowed the Protect America Act to expire, but PAA surveillance continued under year-long orders did not begin to expire until August 2008.

Many of the provisions of the Protect America Act were incorporated into the FISA Amendments Act of 2008 (H.R. 6304, Pub. L. 110-261), signed into law on July 10, 2008. Initially, on November 15, 2007, the House passed the Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective (RESTORE) Act (H.R. 3773). On February 12, 2008, the Senate passed its own version of the bill, S. 2248, in the nature of a substitute to H.R. 3773. The House then passed its own amendments to the Senate bill on March 14, 2008. Ultimately, after extensive negotiations, a compromise bill was passed as H.R.

6304, which became law as the FISA Amendments Act of 2008 on July 10, 2008. Unlike the PAA, the FISA Amendments Act did not exclude surveillance targeting people reasonably believed to be abroad from FISA by construing the term "electronic surveillance" to omit it. However, the bill did permit the executive branch, as opposed to the judicial branch, to authorize such surveillance even though it was conducted in the U.S., and to conduct the surveillance with fewer safeguards than FISA requires for surveillance targeting people in the U.S. It also provided immunity to telecommunications carriers that assisted with unlawful warrantless surveillance.

The following are a list and summary of the amendments to FISA that were enacted from 1994 to 2006 provided by the Congressional Research Service:

1. P.L. 103-359 – Counterintelligence and Security Enhancements Act (enacted Oct. 14, 1994)
2. P.L. 105-272 – Intelligence Authorization Act for Fiscal Year 1999 (enacted Oct. 20, 1998)
3. P.L. 106-120 – Intelligence Authorization Act for Fiscal Year 2000 (enacted Dec. 3, 1999)
4. P.L. 106-567 - Counterintelligence Reform Act of 2000 (passed as Title VI of the Intelligence Authorization Act for Fiscal Year 2001; enacted Dec. 27, 2000)
5. P.L. 107-56 – USA PATRIOT Act (enacted Oct. 26, 2001)
6. P.L. 107-108 – Intelligence Authorization Act for Fiscal Year 2002 (enacted Dec. 28, 2001)
7. P.L. 107-296 – Homeland Security Act of 2002 (enacted Nov. 25, 2002)
8. P.L. 108-458 – Intelligence Reform and Terrorism Prevention Act of 2004 (enacted Dec. 17, 2004)
9. P.L. 109-160 – Extension of Sunset of Certain Provisions of the USA PATRIOT ACT until Feb. 3, 2006(enacted Dec. 30, 2005)
10. P.L. 109-170 - Extension of Sunset of Certain Provisions of the USA PATRIOT ACT until Mar. 10, 2006 (enacted Feb. 3, 2006)
11. P.L. 109-177 – USA PATRIOT Improvement and Reauthorization Act of 2005 (enacted Mar. 9, 2006)
12. P.L. 109-178 – USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 (enacted Mar. 9, 2006)

The most extensive post-1993 changes to FISA were made in the Counterintelligence and Security Enhancements Act of 1994, which extended FISA to physical searches, in the USA PATRIOT Act and in the FISA Amendments Act.

Bills that would require that roving intelligence surveillance orders specify either the target of surveillance or the facility to be surveilled:

1. SAFE Act of 2005 (S. 737, 109th Congress) – Introduced by Sens. Larry Craig (R-ID) and Dick Durbin (D-IL); referred to Committee on the Judiciary; no committee action; House companion bill H.R. 2715
2. Protecting the Rights of Individuals Act of 2003 (S. 1552, 108th Congress) – Introduced by Sen. Lisa Murkowski (R-AK); referred to Committee on the Judiciary; no committee action; House companion bill H.R. 3352

In addition, a number of other FISA bills were introduced in the 110th and a partial list of them follows:

1. NSA Oversight Act of 2007 (H.R. 11; 110th Congress) – reiterates that FISA the exclusive means of conducting domestic electronic surveillance, among other provisions – Introduced by Rep. Adam Schiff (D-CA); referred to Committee on the Judiciary; no action taken
2. Foreign Intelligence Surveillance Improvement and Enhancement Act of 2007 (S. 1114, 110th Congress) - A bill to reiterate the exclusivity of the Foreign Intelligence Surveillance Act of 1978 as the sole authority to permit the conduct of electronic surveillance, to modernize surveillance authorities, and for other purposes – Introduced by Sen. Dianne Feinstein (D-CA); referred to Senate Committee on the Judiciary; no action
3. H.R. 3138, 110th Congress - Amends FISA to redefine "electronic surveillance" as: (1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing surveillance at a particular person believed to be in the United States when that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or (2) the intentional acquisition of the contents of any communication when that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are believed to be in the United States. – Introduced by Rep. Heather Wilson (D-NM); Referred to House Committee on the Judiciary and Select Committee on Intelligence; no action
4. Foreign Intelligence Surveillance Modernization Act (H.R. 3782, 110th Congress), which would require a judge to authorized emergency FISA surveillance and physical searches – Introduced by Rep. Rush Holt (D-NJ); referred to House Committee on the Judiciary; no committee action

Hearings in the 110th Congress:

1. *"FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability"*: *Hearing Before the S. Comm. on the Judiciary* (Oct. 24, 2007) *at* http://judiciary.senate.gov/hearings/hearing.cfm?id=3009
2. *Markup of H.R. 3773 (RESTORE Act)*: *Markup Before the House Committee on the Judiciary* (Oct. 10, 2007) *at* http://judiciary.house.gov/hearings/hear_101007.html
3. *"Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?": Hearing Before the S. Comm. on the*

Judiciary (Sept. 25, 2007) *at* http://judiciary.senate.gov/hearings/hearing.cfm?id=2942

4. *Administration Views of FISA Authorities*: *Hearing Before the Permanent Select Committee on Intelligence* (Sept. 20, 2007)
5. *Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II)*: *Hearing Before the House Committee on the Judiciary* (Sept. 18, 2007)
6. *FISA for the Future: Balancing Security and Liberty*: *Hearing Before the Permanent Select Committee on Intelligence* (Sept. 18, 2007)
7. *Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part I)*: *Hearing Before the House Committee on the Judiciary* (Sept. 6, 2007)
8. *"Return of subpoenas regarding the legal justifications for the President's warrantless wiretapping program from 2001 to 2007"*: *Hearing Before the S. Comm. on the Judiciary* (Aug. 20, 2007) *at* http://judiciary.senate.gov/hearings/hearing.cfm?id=2907

B. Executive

The main executive order governing "United States Intelligence Activities," including FISA, is E.O. 12333:

1. E.O. 12333 – U.S. Intelligence Activities (enacted Dec. 4, 1981 – As amended by E.O. 13284 (2003), E.O. 13355 (2004), and E.O. 13470 (2008))

Several other Executive Orders impact implementation of the legislation as well:

1. E.O. 12139 (enacted May 23,1979) – Exercise of Certain Authority Respecting Electronic Surveillance
2. E.O. 12949 (enacted Feb. 9, 1995) – Foreign Intelligence Physical Searches
3. E.O. 13383 (enacted July 15, 2005) - Amending Executive Orders 12139 and 12949 in Light of the Establishment of the Office of Director of National Intelligence

C. Judicial

FISA orders are issued by the U.S. Foreign Intelligence Surveillance Court (FISC). Decisions of the FISC are reviewable in the U.S. Foreign Intelligence Court of Review (Court of Review). The following published rules apply to these court proceedings:

1. Rules of the U.S. Foreign Intelligence Surveillance Court (as of Feb. 17, 2006)
2. FISA Court Procedures for Review of Section 501(f) Petitions (as of May 5, 2006)

3. Draft FISA Court Procedures for Review of Section 105B(h) Petitions (Oct. 2007)

The FISA Court of Review spoke approvingly of the PATRIOT Act "significant purpose" test in dicta in *In re Sealed Case* No. 02-001(Decided Nov. 18, 2002). A federal district court subsequently struck down the "significant purpose" test in *Mayfield v. U.S.*, 504 F. Supp. 2d 1023 (D. Or. 2007) (holding that §§ 1804 and 1823 of FISA, as amended by Patriot Act are unconstitutional for violating the Fourth Amendment)

- See also Case and Law Review citations to *Mayfield* (from Westlaw)

In *Hepting v. AT&T*, No. C-06-0672-JCS (Complaint, N.D. Cal., filed Feb. 22, 2006) plaintiffs sued AT&T for assisting with illegal warrantless surveillance. This case was later consolidated with other cases making similar allegations against telecommunications carriers, and they are the subject of on-going court proceedings in which the immunity provisions of the FISA Amendments Act are being considered.