



STATEMENT ON
THE PROTECT AMERICA ACT

By the Constitution Project's
Liberty and Security Committee

October 4, 2007

The Constitution Project
1025 Vermont Avenue, NW
Third Floor
Washington, DC 20005

202-580-6920 [phone]
202-580-6929 [fax]

info@constitutionproject.org
www.constitutionproject.org

We, the undersigned members of the Constitution Project's Liberty and Security Committee, are deeply concerned that many of the amendments to the Foreign Intelligence Surveillance Act (FISA) contained in the recently enacted Protect America Act (Pub. L. 110-55) are unnecessarily overbroad, undermine our constitutional system of checks and balances, and fail to sufficiently protect the privacy of the communications of Americans. The Protect America Act (PAA) will sunset in February, and we urge Congress not to reauthorize these provisions as written.

In seeking these amendments to FISA, Director of National Intelligence Michael McConnell cited a need to address a technological development that had forced the National Security Agency to seek approval from the Foreign Intelligence Surveillance Court to intercept purely foreign-to-foreign communications. We agree that FISA was not originally intended to cover purely foreign-to-foreign communications, and that an amendment to preserve that understanding is sensible. However, the rush to legislate prior to the August recess led to a law that goes far beyond what was necessary to fix this problem. The broad language of the PAA appears to allow for extensive, untargeted collection of international (and perhaps even wholly domestic) communications of ordinary Americans without a court order or meaningful oversight by Congress.

The major problematic changes the Protect America Act makes to FISA are:

- 1. Section 105A alters the definition of “electronic surveillance” so that the protections that FISA previously provided to Americans will not apply, so long as the surveillance is “directed at” persons “reasonably believed” to be located outside of the U.S.**

Thus, surveillance of emails and phone calls between a foreign person and a person in the United States can be intercepted by the NSA *in the United States* without a court order, and without adequate regard to the privacy rights of the Americans whose communications are intercepted, so long as the surveillance is “directed at” the person outside the U.S. Whether they are targeted or not, Americans’ phone calls and emails with people targeted because they are abroad can be recorded by our government without any suspicion of wrongdoing by the American or by the foreign target. Moreover, because government agents only need to have a “reasonable belief” that the person they are targeting is outside the U.S., there remains the possibility that purely domestic calls could be inadvertently intercepted without any court oversight. This provision allows much more unfettered authority than DNI McConnell claimed he needed to intercept foreign-to-foreign communications.

- 2. Section 105B (a) permits the DNI and the Attorney General to authorize “the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States” for periods of up to one year without prior judicial authorization.**

The term “concerning” is extremely broad and vague. By authorizing the collection of communications “concerning” foreign persons, this provision could be interpreted to allow the government to collect electronic communications stored domestically without obtaining prior court authorization, and without having any suspicion that either party is an agent of a foreign power or otherwise acting improperly. The DNI and Attorney General instead simply have to certify that the surveillance is directed at a person reasonably believed to be abroad and that a “significant purpose” of the surveillance is to obtain foreign intelligence information, which is defined broadly under FISA to include any matter relevant to foreign relations. This provision also goes much further than the problem identified by DNI McConnell, and this unnecessarily broad language should be rewritten.

- 3. Subsection 105B(e) could allow the government to directly tap into telecommunications facilities.**

Our privacy laws have always demanded a strict separation between our government and private sector communications providers. Until now, those who hold access to our personal communications had an independent duty to protect our privacy and only release communications in response to a lawful order, and then only respond with what was precisely asked for. The Protect America Act, for the first time, could permit the government to have direct, unfettered access to U.S. communications without any filter by private industry.

- 4. The Protect America Act undermines constitutional principles of checks and balances.**

The FISA Court’s oversight role is confined under the PAA to determining only whether the *procedures* by which the new program will operate are “reasonably designed” to ensure that acquisitions are “directed at” people outside the U.S. The FISA Court can only stop an authorized program if the Attorney General’s certification that the procedures governing the program will result in acquisition of information from targeted people reasonably believed to be outside of the United States is found to be “clearly erroneous.” Since its creation, the FISA Court has served as an important check to ensure that privacy concerns are adequately protected in the acquisition of

foreign intelligence information. A highly deferential “clearly erroneous” review standard fails to respect the important role that judicial review can play in this regard.

Congressional reporting under the PAA is likewise insufficient to provide the necessary oversight of such intrusive authority. Congress will not be told how many Americans are having their conversations intercepted, or how those communications are being used.

The lack of prior judicial authorization, the very restricted court review of procedures, and the limited congressional reporting required under the Act make clear that only the executive branch will ever know the extent to which Americans are being subjected to electronic surveillance by their government. This result runs contrary to the tripartite balance of power the Framers envisioned for our constitutional democracy, and poses a serious threat to the very notion of government of the people, by the people and for the people.

We urge Congress not to reauthorize these overbroad and harmful provisions of the PAA.

Members of the Constitution Project’s Liberty and Security Committee Endorsing the Statement on the Protect America Act*

Co-Chairs

David Cole, Professor of Law, Georgetown University Law Center

David Keene, Chairman, American Conservative Union

Members

Azizah Y. al-Hibri, Professor, The T.C. Williams School of Law, University of Richmond; President, Karamah: Muslim Women Lawyers for Human Rights

Bob Barr, Former Member of Congress (R-GA); CEO, Liberty Strategies, LLC; the 21st Century Liberties Chair for Freedom and Privacy at the American Conservative Union; Chairman of Patriots to Restore Checks and Balances; practicing attorney

Mickey Edwards, Lecturer at the Woodrow Wilson School of Public and International Affairs, Princeton University; former Member of Congress (R-OK) and Chairman of the House Republican Policy Committee

Michael German, Policy Counsel, American Civil Liberties Union; Adjunct Professor, National Defense University School for National Security Executive Education; Special Agent, Federal Bureau of Investigation, 1988-2004

Dr. Morton H. Halperin, Director of U.S. Advocacy, Open Society Institute; Senior Vice President, Center for American Progress; Director of the Policy Planning Staff, Department of State, Clinton administration

David Lawrence, Jr., President, Early Childhood Initiative Foundation; former Publisher, *Miami Herald* and *Detroit Free Press*

Robert A. Levy, Constitutional lawyer

Joseph Margulies, Assistant Director, MacArthur Justice Center; Clinical Associate Professor of Law, Northwestern University School of Law

Thomas R. Pickering, Undersecretary of State for Political Affairs, 1997-2000; United States Ambassador and Representative to the United Nations, 1989-1992

John Seigenthaler, Chairman and Founder, The Freedom Forum First Amendment Center at Vanderbilt University; former President, American Society of Newspaper Editors; former Administrative Assistant to Attorney General Robert F. Kennedy; former Founding Editorial Director, USA Today

William S. Sessions, Partner, Holland & Knight, LLP; former Director, Federal Bureau of Investigation; former Chief Judge, United States District Court for the Western District of Texas

John Shore, Founder and President, noborg LLC; former Senior Advisor for Science and Technology to Senator Patrick Leahy

Geoffrey R. Stone, Harry Kalven, Jr., Distinguished Service Professor of Law, University of Chicago

John F. Terzano, Vice President, Veterans for America

Lawrence B. Wilkerson, Col, USA (Ret), Visiting Pamela C. Harriman Professor of Government at the College of William and Mary; Professorial Lecturer in the University

Honors Program at the George Washington University; former Chief of Staff to Secretary of State Colin Powell

John W. Whitehead, President, The Rutherford Institute

Roger Wilkins, Clarence J. Robinson Professor of History and American Culture, George Mason University; Director of U.S. Community Relations Service, Johnson administration

** Affiliations are listed for identification purposes only*