Electronic Frontier Foundation

Statement of Kevin S. Bankston
Staff Attorney
Electronic Frontier Foundation

before the
Senate Select Committee on Intelligence

on
FISA Modernization

May 1, 2007

Chairman Rockefeller, Vice Chairman Bond, and Members of the Committee, the Electronic Frontier Foundation (EFF) is pleased to have this opportunity to provide its statement on the Administration's current proposal to "modernize" the Foreign Intelligence Surveillance Act (FISA).[1]

EFF is a non-profit, member-supported public interest organization dedicated to protecting privacy and free speech in the digital age. As part of that mission, EFF is representing current and former residential customers of AT&T in a civil action against that company for its alleged cooperation in the National Security Agency's warrantless dragnet surveillance of its customers' telephone calls and Internet communications.[2] Just as Congress' laws prohibiting warrantless electronic surveillance bind the government, so too do they bind those telecommunications carriers that are entrusted with transmitting Americans' private communications. As Congress recognized when it provided civil causes of action against communications providers that violate that trust, the ability to maintain such lawsuits is a key check against illegal collaborations between the Executive and those that control access to our national telecommunications infrastructure.

The amendments to FISA currently proposed by the Administration threaten to deprive our plaintiffs of their day in court, and to deprive all Americans of their right to communicate privately. That proposal, far from "modernizing" the law, would gut the long-standing checks and balances that Congress established to rein in the Executive's ability to spy on Americans. It would shield surveillance conducted in the name of national security from meaningful judicial scrutiny, and unjustifiably provide blanket immunity for illegal surveillance conducted since September 11, 2001—surveillance that

[1] FISA Modernization Provisions of the Proposed Fiscal Year 2008 Intelligence Authorization, Title IV, *available at* http://www.fas.org/irp/news/2007/04/fisa-proposal.pdf (hereinafter "Administration Proposal").
[2] *Hepting v. AT&T*, 439 F.Supp.2d 974 (N.D. Cal. 2006) (on appeal to the Ninth Circuit).

454 Shotwell Street, San Francisco, CA 94110 USA
+1 415 436 9333 (v) +1 415 436 9993 (f) www.eff.org

Congress has not yet even investigated, and which appears to go far beyond the narrow "Terrorist Surveillance Program" admitted to by the President.[3]

Unfortunately, this Administration has squandered the people's trust over the past five years, flagrantly ignoring FISA's requirements by wiretapping Americans without warrants and routinely abusing its authority under the USA PATRIOT Act to obtain Americans' private records.[4] It can no longer be given the benefit of the doubt by Congress in these matters. When a large margin of Americans believe that the President has failed to properly balance the preservation of civil liberties against national security concerns,[5] what is most needed is vigorous investigation and oversight by Congress and the Courts—not a statutory blank check granting the Executive even greater surveillance authority, nor a pardon for government agents and telecommunications companies that have violated the law in the past. The Administration and the telephone companies must understand that they cannot ignore the statutes passed by Congress and then simply demand amnesty when caught in the act.

Other commentators have already explained at length how passage of the Administration's proposal as a whole would dangerously and unjustifiably expand the Executive's surveillance powers.[6] Therefore, this statement will focus on those provisions that would most directly impact pending lawsuits against the government and telecommunications carriers for their illegal collaboration in the surveillance of Americans' private communications. In particular, this statement will address:

- Section 408, "Liability Defense," which would unjustifiably grant broad immunity to those who have illegally spied on American citizens;

---

[3] *See, e.g.*, Eric Lichtblau and James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, The New York Times (December 24, 2005), at A1; Leslie Cauley and John Diamond, *Telecoms Let NSA Spy On Calls*, USA Today (February 6, 2006), at A1.

[4] *See* U.S. Department of Justice Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (March 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf.

[5] *See* Shaun Waterman, *Analysis: Poll Shows Security Imbalance*, United Press International (April 26, 2007), *available at* http://www.upi.com/Zogby/UPI_Polls/2007/04/26/analysis_poll_shows_security_imbalance/.

[6] *See, e.g.*, Letter of the American Civil Liberties Union to Chairman Rockefeller and Vice Chairman Bond (April 16, 2007), *available at* http://www.aclu.org/images/general/asset_upload_file827_29385.pdf; Center for Democracy & Technology, *"Modernization" of the Foreign Intelligence Surveillance Act (FISA): Administration Proposes Broad, Warrantless Surveillance of Citizens* (last updated April 18, 2007), *available at* www.cdt.org/security/20070418fisaanalysis.pdf; and Center for National Security Studies, *Fact v. Fiction: The Justice Department's "New" Re-Write of FISA* (April 18, 2007), *available at* http://www.cnss.org/FinalCNSS%20FISA%20Memo%204.19.07.pdf.

- Section 406, "Use of Information," which threatens to create a back door immunity by allowing the Administration to argue that its common law privilege against the disclosure of state secrets overcomes the carefully balanced statutory procedures that Congress established to facilitate litigation over the legality of electronic surveillance; and
- Section 411, "Mandatory Transfer for Review," which would further strengthen the Executive's hand by allowing it to transfer all cases concerning its illegal surveillance to the court most likely to rule in its favor.

Taken together, these provisions represent a concerted attack on the rights of Americans to seek redress when subjected to illegal surveillance, and are an obvious attempt to shield the Administration and its collaborators against judicial inquiry into their illegal surveillance activities since 9/11.

I. Section 408: Blanket Immunity for Illegal Surveillance

The Administration has repeatedly assured Congress and the public that its warrantless surveillance of Americans is fully consistent with the law.[7] Those claims ring hollow, however, when read in conjunction with Section 408 of its proposal. With Section 408, the Administration seeks to provide blanket immunity against liability to any person who has assisted in any government surveillance activity that the Attorney General or his designee claims was undertaken in the name of anti-terrorism. The Administration's bid for such immunity essentially concedes the weakness of its legal arguments in support of warrantless surveillance, arguments that it clearly hopes to insulate from judicial scrutiny.

Specifically, the breathtakingly broad terms of Section 408 provide that:

> Notwithstanding any other law, and in addition to the immunities, privileges, and defenses provided by any other source of law, no action shall lie or be maintained in any court, and no penalty, sanction, or other form of remedy or relief shall be imposed by any court or any other body, against any person for the alleged provision to an element of the intelligence community of any information (including records or other information pertaining to a customer), facilities, or any other form of assistance, during the period of time beginning on September 11, 2001, and ending on the date that is the effective date of this Act, in connection with any alleged classified communications intelligence activity that the Attorney General or a designee of the Attorney General certifies, in a manner consistent with the protection of State secrets, is, was, would be, or would have been

[7] The Administration's legal rationales for its warrantless wiretapping program have been thoroughly refuted by numerous legal scholars. *See, e.g.*, Letter of Law Professors to Congressional Leadership in Response to Department of Justice Memorandum, *available at* http://www.eff.org/Privacy/Surveillance/NSA/FISA_AUMF_replytoDOJ.pdf.

> intended to protect the United States from a terrorist attack. This section shall apply to all actions, claims, or proceedings pending on or after the effective date of this Act.[8]

As an initial matter, this provision does not just protect telecommunications carriers. Rather, it appears designed to also shield *the government itself* against any lawsuit concerning its "classified communications intelligence activit[ies]" since 9/11. In particular, the proposed immunity would reach any "person" as defined at 18 U.S.C. § 2510(6), *i.e.*, "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation."[9]

Furthermore, this provision's language is not expressly limited to immunity from civil liability. Instead, it seeks to prevent the imposition of *any* "penalty, sanction, or other form of remedy or relief" in *any* legal action in *any* court. Such expansive language could be read to preclude even criminal prosecution. Therefore Section 408 could essentially provide the Attorney General with a stack of blank "get out of jail free" cards for both government agents and telecommunications carriers, representing a complete abandonment of the rule of law when it comes to government surveillance conducted in the name of national security.

That Congress might consider such unprecedented blanket immunity for government agents and the telecommunications carriers that illegally assisted them is all the more shocking considering that neither Congress nor the public even knows what conduct it would be immunizing. Senator Arlen Specter has aptly described Section 408 as "a pig in the poke" since "there has never been a statement from the administration as to what these companies have done."[10] Nor has the Administration come clean about its own conduct, publicly admitting only to the purportedly narrow "Terrorist Surveillance Program" described by the President even as news reports[11] and whistle-blower evidence[12] indicate a much broader program.

Congress must not legislate in the dark, particularly when the rights of so many are at stake. Indeed, it would be unwise for Congress to consider *any* kind of immunity when it has yet to investigate the scope and legality of the Administration's conduct. How many

---

[8] Administration Proposal at § 408(a).
[9] *Id*. at § 408(c)(2).
[10] *See* James Risen, *Legislation Seeks to Ease Rules on Domestic Spying*, The New York Times (April 14, 2007), *available at* http://www.nytimes.com/2007/04/14/us/14fisa.html?ex=1334203200&en=6ce04a0c3e2e2046&ei=5124&partner=permalink&exprod=permalink.
[11] *See supra* note 3.
[12] *See Hepting v. AT&T*, 439 F.Supp.2d at 989 (describing whistle-blower's account of AT&T's dragnet surveillance of Internet communications for the National Security Agency).

Americans have had their privacy violated? How did telecommunications carriers assist in those violations of privacy, and what were they given in return? Congress must conduct a full investigation to uncover the answers to those questions. The public and its elected representatives deserve a full accounting of the Administration's illegal surveillance activities and the telecommunications carriers' participation in that surveillance. Such a full accounting is unlikely ever to occur if every person involved has already been granted a no-strings-attached legislative pardon.

In addition to doing its job by investigating how the Administration has abused its surveillance power since 9/11, Congress should allow the courts to do *their* job by allowing them to adjudicate the legality of that surveillance and the telephone companies' participation in it. The telecommunications industry appears to have assisted the Administration in the greatest mass privacy invasion ever perpetrated on the American people. Americans are entitled to discover the extent to which their privacy was violated and to have a court decide whether the law was broken. Immunity would short-circuit this judicial process, potentially eliminating the courts as a meaningful check on illegal collaboration between telecommunications carriers and the Executive Branch.

Not only is Section 408 designed to ensure that past surveillance by the Administration and its collaborators in the telecommunications industry remains shrouded in secrecy and shielded from judicial review, it would also dangerously increase the risk of *future* illegal collaborations between government and communications providers. Telecommunications carriers' adherence to the law is the biggest practical check that we have against illegal government surveillance. Giving blanket immunity to those carriers, which are the only entities standing between the privacy of countless innocent Americans and government overreaching, sets a dangerous precedent. Section 408 threatens to make Congress' laws a dead letter, eliminated by secret meetings between telecommunications executives and government agents, greased by the promise of similar grants of immunity in the future. There is no reason for Congress to take that risk, as federal law already provides legal protections that adequately protect carriers' good faith cooperation in response to lawful requests by the government.[13]

Instead, in order to fully hold accountable those telecommunications carriers that broke the law and to protect against future law-breaking, Congress should allow those customers whose privacy has been violated to press for the remedies to which they are entitled under statute. Congress rightly established strong civil penalties for violation of FISA and its fellow surveillance statutes,[14] and EFF strongly opposes any legislation that would deprive its clients or any other Americans of the remedies to which they are entitled. Congress' carefully crafted penalties were meant to serve as a strong disincentive against illegal assistance in government surveillance, and to cast them aside now would send a dangerous message: that when the government comes calling and uses

[13] *See, e.g.*, 18 U.S.C. §§ 2511(2)(a)(ii) and 2520(d), and 50 U.S.C. § 1805(i).
[14] *See, e.g.*, 50 U.S.C. § 1810 and 18 U.S.C. § 2520(b).

the magic words "national security" or "terrorism," communications providers should feel free to ignore the law.

Finally, to the extent that Congress is concerned by the potential economic impact of such liability on America's telecommunications industry, such concern is wholly premature. Although EFF is confident that its clients will prevail in their current lawsuit against AT&T, that case and other lawsuits against those companies accused of assisting in the Administration's illegal surveillance are still in their early stages. Assuming that the plaintiffs in those suits will ultimately prevail, any award of money damages is likely many years away. Congress should at least allow those cases to continue so that the full scope and legality of the companies' conduct may be discovered and litigated. Then, when the final day of reckoning for the phone companies at last approaches, Congress will have the benefit of a fully developed judicial record to assist it in considering whether the damages to be imposed would be too much—or not nearly enough.

In conclusion, rather than bowing to the Administration's wholly unjustified proposal of blanket immunity, Congress should instead stick to the law that is already on the books. Existing law already strikes a reasonable and bright-line balance between the government's need for industry cooperation in lawful surveillance and the public's need for accountability when industry fails to demand appropriate legal process. The Administration is correct that "[c]ompanies that cooperate with the Government in the war on terror" deserve "our appreciation and protection"[15]—when they do so lawfully. But they deserve neither appreciation nor protection when they break the law and violate the trust of their customers, whether under the claim of national security or otherwise. To the contrary, they deserve to be held to account for their conduct, and indeed must be held to account if we are to prevent secret and unchecked access to the telecommunications networks that carry all of our most private communications.

II. Section 406: Back Door Immunity Through Secrecy

In addition to seeking explicit immunity under Section 408 for government agents and telephone companies that have illegally surveilled Americans, the Administration's proposal also contains provisions, most notably Section 406, that are designed to strengthen the government's argument for a *de facto*, back door immunity based on the so-called state secrets privilege.

Relying on this common law evidentiary privilege, intended to protect from disclosure evidence that will harm national security, the Administration has asserted an astonishingly broad claim: that any lawsuit concerning its warrantless surveillance or the telecommunications industry's participation in such surveillance must be dismissed at the outset. Indeed, it has gone so far as to argue that even if the state secrets privilege did not wholly prevent the cases from being litigated, "[a] court—*even if it were to find unlawfulness* upon *in camera*, *ex parte* review—could not then proceed to adjudicate the

[15] Administration Proposal, Sectional Analysis, p. 60.

very question of awarding damages because to do so would confirm Plaintiffs' allegations."[16] The government argues, essentially, that the state secrets privilege provides complete immunity from suit for any surveillance related to national security. And now, via Section 406 and other provisions of its "modernization" proposal, the Administration is asking Congress to facilitate its attempt to turn this common law evidentiary privilege into a shield against any judicial inquiry into its wrongdoing.

However, Congress has already considered the issue of state secrets in the context of litigation over illegal surveillance, and when passing FISA in 1978 correctly chose not to allow the Executive to use the state secrets privilege as a shield against litigation. In particular, FISA already contains a specific procedure to be followed when the Executive asserts that the disclosure of information concerning electronic surveillance would harm national security. And while that procedure strongly protects national security, it rightly does not contemplate immediate dismissal based on the state secrets privilege.

Instead, FISA provides that if during litigation the Attorney General files a sworn affidavit with the court that disclosure of materials related to electronic surveillance would harm the national security, then the court "*shall*, notwithstanding any other law," review those materials *in camera* and *ex parte*.[17] Furthermore, when reviewing those materials to determine whether the surveillance was lawfully authorized and conducted, the court may if it deems necessary disclose information about the surveillance to the aggrieved person seeking discovery.

This procedure, codified at 50 U.S.C. § 1806(f), reflects several key judgments made by Congress when crafting FISA. First, it reflects Congress' recognition that the legality of surveillance *must be litigable* in order for any of its laws on the subject to have teeth, a recognition bolstered by its creation of a civil remedy in FISA for those who have been illegally surveilled.[18] Second, it reflects Congress' intent to carefully balance that need for accountability with the Executive's interest in avoiding disclosure of information that may harm the national security, and to achieve a "fair and just balance between protection of national security and protection of personal liberties."[19] Finally, it reflects Congress' recognition that the final decision as to what information should be disclosed cannot be left to the Executive's unilateral discretion, but must instead be made by the

---

[16] United States' Reply in Support of the Assertion of the Military and State Secrets Privilege and Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States (*Hepting v. AT&T*, N.D. Cal. Case No. 06-672-VRW, Dkt. No. 245) at p. 20:19-20 (emphasis added), *available at* http://www.eff.org/legal/cases/att/gov_MTD_reply.pdf.

[17] *See* 50 U.S.C. § 1806(f) (emphasis added).

[18] *See* 50 U.S.C. § 1810.

[19] S. Rep. No. 94-1035, at 9 (1976) (discussing § 1806(f)).

courts[20]—courts that both Congress and the Executive trusted could handle sensitive national security information in a reasonable and secure manner.[21]

Now, however, the Administration is unjustifiably asking this Congress to cast aside those carefully considered legislative judgments so it may avoid the judicial scrutiny that FISA demands. Specifically, in Section 406 of its proposal, the Administration asks for the insertion of a new subsection into 50 U.S.C. § 1806, the same section that contains Congress' reasoned procedure for court review and disclosure of secret evidence:

> (l) PROTECTIVE ORDERS AND PRIVILEGES.—Nothing in this section shall prevent the United States from seeking protective orders or asserting privileges ordinarily available to the United States to protect against the disclosure of classified information.[22]

In addition to this provision, other sections of the Administration's proposal are also littered with similar language targeted at bolstering the Executive's assertions of the state secrets privilege.[23] Taken together, these proposed changes represent a bald-faced attempt to avoid the balanced discovery procedure that Congress has previously established, and shield the Administration and those that have cooperated with it from any and all litigation. Yet the Administration has failed to offer any reason why the reasoned judgments made by Congress in 1978 do not still apply with full force. Therefore, and for the same reasons that Congress should reject the immunity proposed in Section 408, it should also reject the Administration's attempt to create a back door immunity based on the state secrets privilege.

III. Section 411: Forum Shopping Through Legislation

Section 411 of the Administration's proposal is the third and final prong in its concerted attempt to stack the deck against Americans seeking redress for being subjected to illegal surveillance. That section would require, *at the Attorney General's discretion*, the transfer "of any case before any court challenging the legality of a classified communications intelligence activity relating to a foreign threat, or in which the legality of any such activity is in issue" to the Foreign Intelligence Surveillance Court

---

[20] Congress explicitly stated that the appropriateness of disclosure is a "decision ... *for the Court to make*[.]" S. Rep. No. 95-701, at 64 (emphasis added); *accord* S. Rep. No. 95-604(I), at 58.

[21] *See* Foreign Intelligence Surveillance Act of 1977: Hearings Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary 95th Cong., at 26 (1977) (Attorney General Bell asserting that "[t]he most leakproof branch of the Government is the judiciary . . . I have seen intelligence matters in the courts. . . I have great confidence in the courts," to which Senator Hatch replied, "I do also").

[22] Administration Proposal § 406(2).

[23] *See* Administration Proposal §§ 402, 408(a), and 411(e).

(FISC).[24] By this provision, the Administration obviously seeks for Congress to legislatively enable it to "forum shop" and shuttle all cases regarding its surveillance activities into the court most likely to approve of its conduct. Indeed, the sole role of that court for nearly thirty years has been to routinely approve the Executive's applications for authorization to conduct foreign intelligence surveillance.

The Administration justifies this forum-shopping provision by arguing that only the FISC can be trusted to handle sensitive national security information. Yet as already discussed, Congress and previous administrations have long trusted the regular court system to handle such information responsibly,[25] and the Administration has been unable to point to a single instance in which the judiciary has failed to do so. The Administration's baseless rhetoric about maintaining security therefore cannot justify the diversion of properly maintained lawsuits into a court staffed by judges that are hand-picked by the Chief Justice of the Supreme Court and are accustomed to considering such matters in completely secret and non-adverserial proceedings. Rather, such cases should remain before the fairly and randomly selected state and federal judges that would otherwise adjudicate those disputes in open court—subject, of course, to the carefully balanced FISA procedures discussed previously.

Furthermore, even if the Administration's unfounded security concerns were valid, they would not provide any justification for Section 411's granting of jurisdiction to the Supreme Court for review "by writ of certiori granted upon the petition of the *United States*," while failing to explicitly grant such jurisdiction based upon petitions by the United States' opponents.[26]

Finally, Section 411 would go even further than Section 406 when it comes to strengthening the Administration's ability to abuse the state secrets privilege and bypass FISA's existing procedures, by allowing the *Attorney General and the Director of National Intelligence* to make the final determination as to whether information relating to the national security may be disclosed by the court.[27] Considering the Administration's claims that the FISC—the most secretive judicial venue in the nation—is the most trustworthy court when it comes to responsibly handling such information, this final insult only adds to the grievous injury the Administration's proposal would inflict on the rule of law and the separation of powers.

IV. Conclusion

The Administration's proposal, if passed, will significantly hinder the judiciary's ability to enforce Congress' laws concerning electronic surveillance, giving the Administration brand new excuses in its attempt to avoid judicial scrutiny of its illegal

---

[24] Administration Proposal § 411(a).
[25] *See supra* note 21 and accompanying text.
[26] Administration Proposal § 411(c) (emphasis added).
[27] Administration Proposal § 411(b).

surveillance of Americans in collaboration with telecommunications carriers. For all the foregoing reasons, the Electronic Frontier Foundation respectfully urges this Committee to reject the Administration's current proposal to amend the Foreign Intelligence Surveillance Act.