

THE PROTECT AMERICA ACT:

Who will protect us against the protectors?

Stephen Ross Johnson
Anne Passino
RITCHIE, DILLARD, & DAVIES, P.C.

The Latin phrase *quis custodiet ipsos custodiet* (“Who will protect us from the protectors”) is attributed to the Roman poet Juvenal. The essential problem was posed by Plato in *The Republic*, his work on government and morality. Several centuries later, Lord Acton accurately described the nature of governmental power. “Power tends to corrupt and absolute power corrupts absolutely.” J. Acton, *Essays on Freedom and Power*, 364 (H. Finer ed. 1948).

Advancements in telecommunications technology coupled with virtually limitless storage and processing capabilities present modern society with the same questions, albeit on a much larger scale, that have been debated for centuries. The difference in the present era is that at no other time in recorded human history has it been as possible as it is today to invade, memorialize, catalog, and search the spoken and written words that we pass among one another. In the age where virtually all communications – visual, audio, and written – are in digital format and pass through multiple computer systems on the way from sender to receiver, the developments in electronic surveillance have allowed the government to have virtually limitless access to the most intimate portions of our lives, all in the name of protection and security, which invokes Juvenal’s classic question: Who will protect us against the protectors?

The Protect America Act of 2007, Pub. L. 110-55 (Aug. 5, 2007), which has a 180 day sunset provision, amends the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C.A § 1803 *et seq.*, by adding §§ 1803a-c. Section (a) states that nothing under FISA’s definition of “electronic surveillance” shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States.¹

¹ Previously, “electronic surveillance” had been defined as:

- (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
- (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United

By defining electronic surveillance in terms of whether the target is “reasonably believed to be located outside the United States,” surreptitious warrantless surveillance only requires that one of the parties be international (or, more accurately, only that he or she is reasonably believed to be international). This means that electronic communications may be intercepted either when the communication is going to someone outside the U.S. or coming from someone inside the U.S., so long as the person targeted is outside the United States. Court orders are still required under the PAA to conduct electronic or physical searches when the target is inside the United States, *see Hearing on the Foreign Intelligence Surveillance Act and Protect America Act Before the House Judiciary Committee*, (statement of J. Michael McConnell, Director of National Intelligence) (September 18, 2007), but critics of PAA suggest that the court order requirement may be bypassed by engaging in “reverse targeting.” To allay worries, McConnell testified that reverse targeting is illegal, and he dismissed the need to engage in reverse targeting as unnecessary and inefficient. However, because the Intelligence Community is not required to disclose its methods for determining whether the target is reasonably located outside the United States or how the methods are implemented, it is not clear how illegal reverse targeting or purely domestic surveillance are prevented.

Next, section (b) authorizes the Director of National Intelligence and the Attorney General – with no court or independent oversight – to issue year-long warrants for surveillance of individuals reasonably believed to be outside the United States. Although section (c) directs the AG to submit to the FISA Court within 120 days its procedures for ensuring that the information acquisition is not electronic surveillance, some suggest that this will do little to mitigate the dragnet that the newly expanded definition of “electronic surveillance” allows because it does not require the AG to explain how American phone calls or emails are treated when intercepted. The ACLU also suggests that the requirement that the Attorney General report to the Intelligence and Judiciary Committee is meaningless because the Attorney General is only required to disclose activities in violation of the secret guidelines as they relate to targets overseas and does not require the him to disclose how many Americans’ calls were intercepted or how many Americans were targeted.

States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C.A. § 1801.

In response to the PAA, on August 3, 2007, Representative Conyers sponsored a bill called the RESTORE Act (“Responsible Electronic Surveillance that is Overseen, Reviewed, and Effective Act of 2007”). H.R. 3773, 110th Cong. (2007); see also H.R. 3356, 110th Congress (2007). The RESTORE Act, which would establish a procedure for determining what is and is not electronic surveillance and which would re-require oversight by the Foreign Intelligence Surveillance Court, has nonetheless received some of the same criticisms leveled against the PAA, because it still allows for blanket warrants that circumvent traditional warrant requirements. See ACLU October 9, 2007, Press Release available at <http://www.aclu.org/safefree/general/32104prs20071009.html>.

Given that FISA and the PAA now allow warrantless surveillance of some domestic calls, do they also allow warrantless surveillance of calls protected by the attorney client privilege? FISA provides that “No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this title shall lose its privileged character.” 50 U.S.C. § 1806(a). However, Attorney General Gonzales told the Senate Judiciary Committee that “Although the [PAA] Program does not specifically target the communications of attorneys or physicians . . . calls from such sources would not be categorically excluded from interception,” (March 24 letter), and precedent suggests that such calls could be monitored just as if they were not privileged.

For example, Attorney General Ashcroft previously and successfully navigated around the privilege by using anti-terrorism legislation to monitor conversations between attorneys and their clients in prison, 28 C.F.R. §§ 501.3(d) (2002), Prevention of Acts of Violence and Terrorism, 66 Fed. Reg. 55062, (Oct. 31, 2001) 2001 WL 1334043 (citing the crime-fraud exception to the privilege, Attorney General Ashcroft certified that when “reasonable suspicion” exists to believe an inmate “may” use communications with attorneys or their agents to further or facilitate acts of violence or terrorism, the DOJ “shall . . . provide appropriate procedures for the monitoring or review of communications between that inmate and attorneys or attorneys' agents who are traditionally covered by the attorney-client privilege.”), and then using the conversations as evidence to support a criminal conviction. United States v. Ahmed Abdel Sattar et al., No. 02 CRIM. 395 (S.D.N.Y. April 9, 2002) (rejecting argument made by attorney indicted for conspiring to aid terrorist organization based on intercepted phone conversation that possibility that attorney-client communications were under surveillance violated client’s Sixth Amendment right to counsel by chilling communications where indictment).

In addition, reviewing courts may condone PAA-authorized warrantless wiretaps and/or their use in court if, as has been done in cases where FISA was used to record attorney-client communications, privilege or "taint" teams redact material to make it appear that the defendants' right to have privileged communications with his attorney retained its

integrity. United States v. Neill, 952 F. Supp. 834, 841 (D. D.C. 1997) (finding, however, that it was the government's burden to rebut the presumption that tainted material was provided to the prosecution team). Alternatively, it is possible that, as with domestic wiretaps where officials must minimize the interception of non-relevant phone conversations, see United States v. Bennett, 219 F.3d 1117, 1123 (9th Cir. 2000), a court will determine whether agents have properly minimized interception of such conversations by evaluating the facts and circumstances of each case. Id. (citing Scott v. United States, 436 U.S. 128, 14 (1978)).

The loose language of the PAA,² when combined with the ex post facto curative measures traditionally permitted under FISA mean that not only can domestic calls be monitored without a warrant but that privileged calls may also be monitored so long as the purpose is to acquire foreign intelligence information³ and the target is reasonably believed to be outside the United States.

² The expansive definitions of "international terrorism" and "acts of war" set out in the USA Patriot Act, 18 U.S.C.A. § 2331, and "agent of a foreign power" and "foreign intelligence information" set out in FISA, 50 U.S.C.A. § 1801, mean that there are likely increasing numbers of individuals who qualify as targets of surveillance and therefore whose conversations with their attorneys are monitored.

It is also significant that the application for a warrant to intercept (domestic) electronic communications requires only a showing of probable cause to believe that the conversations will reveal evidence of an ongoing or planned crime. 18 U.S.C. § 2518(3)(a); see also, e.g., United States v. Carneiro, 861 F.2d 1171, 1179 (9th Cir. 1998); United States v. Tehfe, 722 F.2d 1114, 1118 (3d Cir. 1983). By comparison, FISA requires a weaker showing of probable cause, since the government need only demonstrate that there is probable cause to believe that the person targeted for the surveillance is an agent of a foreign power or an international terrorist group; it is not even necessary for the government to demonstrate probable cause to believe that the target is currently committing, or planning to commit, a crime. 50 U.S.C. §§ 1801(b)(2) & 1805(a)(3); see also, e.g., United States v. Cavanaugh, 807 F.2d 787, 790-91 (9th Cir. 1987); United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980); United States v. Falvey, 540 F. Supp. 1306, 1313 (E.D.N.Y. 1982).

³ "Foreign intelligence information" means— (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against-- (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to-- (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States.

50 U.S.C.A. § 1801 (2007).

In today's world, anything you say or write can be, and often is, recorded in some fashion – whether it is intended to be or not. That begs the question of whether privacy as we know it is lost. Since many privileges, such as the attorney-client privilege, are premised upon the reasonable expectation of privacy, can any expectation of privacy be reasonable when we're constantly being recorded by the government and we know it? For example, in London, U.K., there are security video cameras on every street corner, recording, saving, and cataloguing audio and video of the activities of the general public. It has proven to be a tremendous investigative tool, yet the privacy historically inherent with public anonymity has been lost in exchange for security. The PAA presents the same Orwellian problem. With the government capable of gathering so much material in the name of protecting us, who will protect us from our protectors?