1 Data Sec. & Privacy Law § 6:67 (2013)

Data Security and Privacy Law
Database updated June 2013
Chapter 6. Data Security Statutes

Leslie Paul Machado [*] and C. Matthew Haynes [**]

§ 6:67. Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act (FISA) [1] gives the government power to conduct electronic and physical searches and seizures (termed "electronic surveillance" and "physical searches" by the statute) beyond what is normally authorized for criminal investigations for those cases in which national security is at issue. [2] Prior to the enactment of FISA, courts routinely either deferred to the executive or abstained from hearing cases in which a defendant sought to limit the power of the government to conduct searches and seizures to obtain, store, and use information about foreign powers or their agents (e.g., spies). Such surveillance activities were deemed part of national security functions and, therefore, ill suited for judicial review. [3]

In 1978, Congress passed the original version of FISA, which for the first time established a procedure by which the executive branch was required to seek authorization to conduct foreign surveillance activities. [4] FISA also created the Foreign Intelligence Surveillance Court (FISA Court) and the Foreign Intelligence Surveillance Court of Review (FISA Court of Review). [5] These courts are staffed by federal court judges appointed by the Chief Justice of the Supreme Court, and the decisions of the FISA Court of Review are reviewable by the U.S. Supreme Court. [6] The main function of the FISA Court is to issue FISA warrants sought by the Attorney General or by designated federal officials. [7] A FISA Court denial of a warrant request may be appealed to the FISA Court of Review, a process that has occurred only once since the enactment of FISA. [8]

FISA was amended by the USA PATRIOT Act in 2001 to allow for increased cooperation between officials carrying out criminal investigations and foreign intelligence surveillance. [9] Prior to the FISA Court of Review's ruling in *In re Sealed Case*, it was generally held that FISA required a clear separation of criminal investigations from foreign intelligence investigations. [10] Indeed, previous interpretations of FISA had proceeded from the assumption that the statute implicitly mandated the erection of an institutional barrier or "wall" within the U.S. Department of Justice to block intelligence officials and criminal investigators from working together and sharing information. [11] *In re Sealed Case* rejects this stark division, finding that the plain language of FISA does not support the view that FISA searches can only be permitted if the government's objective is primarily directed toward foreign intelligence instead of criminal prosecution. Moreover, even if such a dichotomy between criminal investigations and foreign intelligence investigations existed under FISA, the USA PATRIOT Act statutorily relaxed it and embraced the sharing of the criminal and foreign intelligence procedures by allowing FISA searches in which foreign intelligence collection was merely a "significant"—albeit not primary—purpose of the surveillance. [12]

Criminal investigations are more limited than foreign intelligence investigations in several important respects. For example: (a) criminal investigations have a higher standard for what must be shown to satisfy "probable cause" than foreign intelligence investigations; (b) foreign intelligence investigations may use highly intrusive surveillance techniques which are not allowed in investigating "ordinary crime;" and (c) foreign intelligence investigations may keep confidential (and therefore not discoverable) the records of the surveillance, which in ordinary criminal investigations must be made available to the defendant once the case goes to trial. [13] Thus, for example, FISA searches can reach where searches under the Wiretap Statute would not. [14]

These advantages make a FISA search a desirable tool for criminal investigators. However, the justification for such increased investigative powers lies in the fact that FISA searches seek to obtain information that is related to national security. Searches that are reasonable for national security purposes may be suspect for Fourth Amendment purposes under a lesser governmental interest like criminal prosecution. [15]

The FISA Court of Review found that the original version of FISA passed in 1978 "clearly did not preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution," [16] as long as the government certified that "the purpose" of the surveillance was to obtain foreign intelligence information. [17] The USA PATRIOT Act relaxed this requirement, changing the requirement to a certification "that a significant purpose of the surveillance is to obtain foreign intelligence information." [18] By easing the certification standard, Congress clearly intended to authorize FISA searches for investigations in which foreign intelligence information was not the primary purpose, but rather only a significant purpose. [19] The FISA Court of Review in *In re Sealed Case* clearly viewed the USA PATRIOT Act as going a long way toward breaking down the barriers between criminal law enforcement and foreign intelligence gathering. [20] As the FISA Court of Review explained, "as long as the government entertains a realistic option of dealing with the [object of the surveillance] other than through criminal prosecution, it satisfies the significant purpose test." [21]

FISA also provides criteria for "minimization" of the information gathered under FISA searches. [22] The FISA minimization procedures are aimed at limiting the storage, use, and dissemination of information gathered under FISA searches to those functions that justify the searches, or at least the use and storage of the information gathered. [23] The USA PATRIOT Act did not change these criteria, [24] but the FISA Court of Review overruled the FISA Court's attempt to impose minimization procedures that improperly restricted the government's ability to use information discovered during foreign intelligence investigations in the prosecution of ordinary crimes:

> In light of these purposes of the minimization procedures, there is simply no basis for the FISA court's reliance on section 1801(h) to limit criminal prosecutors' ability to advise FBI intelligence officials on the initiation, operation, continuation, or expansion of FISA surveillances to obtain foreign intelligence information, even if such information includes evidence of a foreign intelligence crime. [25]

Computer security and privacy issues generated by *In re Sealed Case* include increased governmental power to conduct electronic surveillance of virtually every computer connected to the Internet, [26] and the likelihood that defendants prosecuted for computer crimes will challenge evidence obtained by FISA searches that are not primarily foreign surveillance investigations on the grounds that they are unreasonable searches and seizures in violation of the Fourth Amendment.

In re Sealed Case gained added significance in 2006 upon discovery of a clandestine domestic wiretapping program carried out by the National Security Agency and authorized by Presidential Order. [27] The Court declared in dictum in *In re Sealed Case* that FISA cannot encroach on the "inherent authority" of the President to conduct warrantless wiretapping to obtain foreign surveillance but did not elaborate at any length on the precise nature and extent of this authority. [28] The Court's conception of inherent executive authority has become a flashpoint in the controversy over the NSA program and domestic and foreign surveillance more generally. [29]

Footnotes

* Les Machado is a Partner in the Washington, D.C. office of LeClairRyan. Mr. Machado co-chairs the firm’s media, Internet and e-commerce team and advises clients on a wide range of areas, including media, technology and intellectual property and communications law. Mr. Machado has extensive experience in complex commercial and technology/Internet related litigation in state and federal courts throughout the United States and has written extensively about media, Internet and technology issues, including

the Communications Decency Act of 1996 and the Computer Fraud & Abuse Act. Mr. Machado received a J.D., cum laude, from the State University of New York at Buffalo in 1996, where he was a member of the Law Review, Moot Court Board, and Jessup Moot Court Board. Mr. Machado received a B.A. in Communications from Fordham University in 1992. Mr. Machado can be reached for comments and questions at (202) 659-6736, leslie.machado@leclairryan.com and http://www.leclairryan.com.

** Matthew Haynes is an Associate in the Alexandria, Virginia office of LeClairRyan. Mr. Haynes focuses his practice primarily on business and intellectual property and technology litigation. Mr. Haynes's experience in complex commercial and technology related litigation extends to the state and federal level, where he has secured outstanding client results in actions relating to, among other things, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act. Mr. Haynes received a J.D., cum laude, from the University of Richmond in 2009, where he was a member of the Trial Advocacy Board and competed successfully in several national advocacy competitions. While in law school, Mr. Haynes was awarded membership in the Order of the Barrister for demonstrating excellence in trial and appellate advocacy. Mr. Haynes received a B.A., cum laude, in Political Science from Virginia Commonwealth University in 2005. Mr. Haynes can be reached for comments and questions at (703) 647-5919, matthew.haynes@leclairryan.com and http://www.leclairryan.com.

1 50 U.S.C.A. §§ 1801 et seq.

2 See 50 U.S.C.A. §§ 1801(f) (definition of electronic surveillance), 1821(5) (definition of physical searches). See also In re Sealed Case, 310 F.3d 717, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam).

3 Chagnon v. Bell, 642 F.2d 1248, 1259–62, 29 Fed. R. Serv. 2d 1245 (D.C. Cir. 1980) (explaining pre-FISA Supreme Court precedent on searches conducted for foreign intelligence purposes).

4 Chagnon v. Bell, 642 F.2d 1248, 1259–62, 29 Fed. R. Serv. 2d 1245 (D.C. Cir. 1980)

5 See 50 U.S.C.A. § 1803(a), (b).

6 See 50 U.S.C.A. § 1803(a), (b).

7 50 U.S.C.A. § 1803(a).

8 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272; In re Sealed Case, 310 F.3d 717, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam).

9 In re Sealed Case, 310 F.3d 717, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam).

10 See, e.g., U.S. v. Johnson, 952 F.2d 565, 572, 34 Fed. R. Evid. Serv. 1117 (1st Cir. 1991); U.S. v. Pelton, 835 F.2d 1067, 1075-76 (4th Cir. 1987); U.S. v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); U.S. v. Duggan, 743 F.2d 59 (2d Cir. 1984). See also In re All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (Foreign Intel. Surv. Ct. 2002) (per curiam). But see U.S. v. Sarkissian, 841 F.2d 959, 964 (9th Cir. 1988).

11 In re Sealed Case, 310 F.3d 717, 721, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam).

12 Cf. In re Sealed Case, 310 F.3d 717, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam).

13 See In re All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (Foreign Intel. Surv. Ct. 2002) (abrogated on other grounds by, In re Sealed Case, 310 F.3d 717, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002)), In re Sealed Case, 310 F.3d 717, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002).

14 In re Sealed Case, 310 F.3d 717, 738-42, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam) (given the secrecy of the FISA proceedings, it is more difficult to draw a factual example; but, generally, FISA searches allow for more intrusive technological measures and a lesser showing of probable cause than Wiretap Statute searches).

15 See In re Sealed Case, 310 F.3d 717, 737-42, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam). See also U.S. v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987); U.S. v. Cavanagh, 807 F.2d 787, 86 A.L.R. Fed. 771 (9th Cir. 1987).

16 In re Sealed Case, 310 F.3d 717, 727, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam).

17 In re Sealed Case, 310 F.3d 717, 723, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam).

18 In re Sealed Case, 310 F.3d 717, 732, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam).

19 In re Sealed Case, 310 F.3d 717, 732, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam).

20 See also discussions of 50 U.S.C.A. § 1806(k); In re Sealed Case, 310 F.3d 717, 733, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam).

21 In re Sealed Case, 310 F.3d 717, 735, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam).

22 See 50 U.S.C.A. § 1806.

23 In re Sealed Case, 310 F.3d 717, 731, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam).

24 In re Sealed Case, 310 F.3d 717, 729, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam) (referring to the emphasis the FISA Court put on this fact in reaching its decision).

25 In re Sealed Case, 310 F.3d 717, 731, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002) (per curiam).

26 See ACLU, In First Ever Ruling, Secret Appeals Court Allows Expanded Government Spying on U.S. Citizens, Nov. 18, 2002, available at http://www.aclu.org//privacy/spying/15189prs20021118.html (last visited March 19, 2006).

27 See James Risen & Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, N.Y. Times, Dec. 16, 2005, at A1.

28 In re Sealed Case, 310 F.3d 717, 742, 190 A.L.R. Fed. 725 (Foreign Intel. Surv. Ct. Rev. 2002).

29 Compare U.S. Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006), available at http://epic.org/features/surveillance.html (last visited March 18, 2006), with Letter from Scholars of Constitutional Law and Former Government Officials to Members of Congress (Jan. 9, 2006), available at http://www.aclu.org/safefree/nsaspying/index.html (last visited March 18, 2006).

End of Document