CASE COMMENT

ELECTRONIC SURVEILLANCE: NATIONAL SECURITY AND THE PRESERVATION OF THE RIGHTS GUARANTEED BY THE FOURTH AMENDMENT

Jewel v. Nat'l Sec. Agency, 2015 WL 545925 (N.D. Cal. 2015)

Valentín I. Arenas[*]

FACTS

Plaintiffs, California AT&T customers who send Internet communications,[1] alleged that the National Security Agency's (NSA) possible interception of their Internet communications without a warrant violates their Fourth Amendment rights.[2] Defendants, the NSA and other government officials, contended that Plaintiffs lacked standing and raised the state secrets privilege protection.[3] Plaintiffs first filed the case before the U.S. District Court for the Northern District of California, which granted Defendants' motion to dismiss.[4] On appeal, the Ninth Circuit Court of Appeals reversed lower court's judgment.[5] On remand, the District Court rejected Defendants' state secrets privilege defense as per 50 U.S.C. § 1806(f) of the Foreign Intelligence Surveillance Act (FISA)[6] and required that parties submit briefings before ruling on the federal claims.[7] Jurisdiction was proper because the Court had subject matter jurisdiction over the federal claims and personal jurisdiction over Defendants, who had sufficient contacts with the district and events that took place therein, and because Plaintiffs alleged enough stake in the outcome.[8] The Court denied Plaintiffs' motion for partial summary judgment and granted Defendant's cross-motion for partial summary

---

* J.D. Candidate, anticipated May 2017, University of Florida Levin College of Law; B.A., Psychology and Political Science, University of Miami, 2013. I would like to thank my family for their love and support. I would also like to thank the University of Florida Levin College of Law, *Journal of Technology Law & Policy* for selecting my work for publication.

1. Jewel v. Nat'l Sec. Agency, No. 08-CV-04373-JSW, 2015 WL 545925, at *1 (N.D. Cal. Feb. 10, 2015).
2. *Id.* at 2.
3. *Id.*
4. Jewel v. Nat'l Sec. Agency, No. 06-CV-1791-VRW, 2010 WL 235075, at *9 (N.D. Cal. Jan. 21, 2010).
5. Jewel v. Nat'l Sec. Agency, 673 F.3d 902, 913 (9th Cir. 2011).
6. Jewel v. Nat'l Sec. Agency, 965 F. Supp. 2d at 1090, 1112 (N.D. Cal. 2013).
7. *Id.*
8. *Jewel*, 673 F. 3d at 909.

judgment.[9] HELD, Plaintiffs lacked standing to sue under the Fourth Amendment and, even if Plaintiffs established standing, the state secrets privilege will require that their claim be dismissed.[10]

HISTORY

The Fourth Amendment of the U.S. Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[11]

In recent years, the Fourth Amendment's applicability in electronic surveillance has received much attention from the judiciary. The Fourth Amendment's goal is to protect individuals' right to privacy by prohibiting the government from searching through communications without a warrant, probable cause, and particularity.[12] This is especially true in the case of electronic surveillance, where the threat of invasion of privacy is greater and more inconspicuous.

The Federal Code contains numerous sections regarding electronic surveillance and information collection. Relevant to the instant case is FISA. Congress passed FISA in 1988 to prevent the abuse of domestic surveillance and to authorize the use of warrantless foreign surveillance on the grounds that the surveillance is not on United States citizens and is in the interest of national security.[13] Otherwise, FISA requires that the government obtain a warrant to engage in domestic surveillance.[14] Congress intended for FISA to supplant federal common law rules.[15] As a result, 50 U.S.C. § 1806(f),[16] the exclusive procedure for reviewing classified information in FISA challenges,[17] preempts the state secrets privilege by allowing the judiciary to review the information *ex parte* and

9. *Jewel*, 2015 WL 545925, at *5.
10. *Id.* at *7.
11. U.S. CONST. amend. IV.
12. *Jewel*, 2015 WL 545925, at *2.
13. *Electronic Surveillance*, CORNELL UNIV. LAW SCHOOL WEX LEGAL ENCYCLOPEDIA, https://www.law.cornell.edu/wex/electronic_surveillance (last visited July 28, 2015).
14. *Id.*
15. Jewel v. Nat'l Sec. Agency, 965 F. Supp. 2d at 1090, 1105 (N.D. Cal. 2013).
16. 50 U.S.C. § 1806(f) (2015).
17. *Jewel*, 965 F. Supp. 2d at 1105.

in camera.[18] This, in turn, permits the judiciary to determine whether the surveillance was "lawfully authorized and executed."[19]

Similarly, section 702 of FISA outlines the process by which the government is to collect communications. Pursuant to Section 702, government surveillance aims to "[i]dentify non-U.S. persons located outside of the United States who are reasonably believed to possess or receive, or likely to communicate, foreign intelligence information" relevant to national security.[20] Once the government identifies the target's means of communications, known as "selectors," the government may then compel service providers to disclose all information necessary, to acquire the communications related to the selector, known as "tasking."[21]

A section 702 directive that has been subject to recent litigation is the Upstream collection program. The program compels service providers to release the tasked selectors' communications that transit the domestic Internet backbone and to filter the results.[22] Once the communications pass both screens, they enter governmental databases for further surveillance.[23]

Generally, to have standing on a Fourth Amendment claim, Plaintiffs must establish a reasonable expectation of privacy and show that a violation of that constitutionally protected right is "certainly impending."[24] In *Clapper*, the Court found that plaintiffs' reliance on a "speculative chain of possibilities" was insufficient to establish standing.[25] The Court reasoned that one cannot establish that an injury is certainly impending if it is based on a "potential future surveillance."[26] In other words, allegations and speculations are not enough to challenge NSA surveillance under FISA.[27]

Furthermore, *Klayman* sheds light on the role service providers may play in establishing standing. In *Klayman*, the District Court granted standing to Verizon customers after finding that the NSA had been

---

18. *Id.* at 1106; *see also* 50 U.S.C. § 1806(f) (2015).

19. *Id.* at 1105.

20. Jewel v. Nat'l Sec. Agency, No. 08-CV-04373-JSW, 2015 WL 545925 at *1 (N.D. Cal. Feb. 10, 2015).

21. *Id.*

22. *Id.* at *2.

23. *Id.* (citing to *Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, July 2, 2014, at 35).

24. Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992); *see also* Whitmore v. Arkansas, 495 U.S. 149, 158 (1990).

25. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 (2013).

26. *Id.* at 1150.

27. *See Whitmore*, 495 U.S. at 158.

collecting Verizon metadata.[28] It reasoned that the fact that plaintiffs are Verizon customers sufficiently shows that an injury is certainly impending.[29] On appeal, the Court reversed after finding that plaintiffs subscribed to Verizon Wireless instead of Verizon Business Network Services, Inc., whose data the government acknowledged collecting.[30] Thus, once it is known that a service provider collaborates with the government in the mass collection of Internet communications, individuals only have to show that they are its customers and that they send Internet communications to establish that the collection program has potentially stored their communications.[31]

Celotex set the standard of proof required at the summary judgment stage.[32] In *Celotex*, the Court held that the burden of proof at the summary judgment stage and at trial is the same.[33] Therefore, individuals moving for summary judgment must show sufficient evidence in establishing an essential element of their claim to allow a rational trier of fact to find in their favor. Once the moving party meets its burden of proof, the judiciary must address whether Fourth Amendment violations can be litigated without risking disclosure of classified information critical to national security. The judiciary's main concerns when it comes to litigating the constitutionality of electronic surveillance are national security and a fair and full adjudication of the parties' arguments.[34] These concerns, coupled with protection under the state secrets privilege, may at times require the Court to dismiss a case.[35] History has shown that the judiciary has protected the government's use of the state secrets privilege in the name of national security at the expense of full disclosure to the public.

INSTANT CASE

The instant case follows this pattern of judiciary support for the government's use of the state secrets privilege in the name of national security. The Court based its decision on the risks that litigating this claim poses on national security and on the impossibility of a fair and full

28. Klayman v. Clapper, 957 F. Supp. 2d 1, 26-28 (D.D.C. 2013), *vacated*, Obama v. Klayman, 800 F. 3d 559 (D.C. Cir. 2015).

29. *Id.* at 26.

30. Obama v. Klayman, 800 F.3d 559, 565-66 (D.C. Cir. 2015) (Williams, J., concurring).

31. *Jewel*, 2015 WL 545925, at *4.

32. Celotex Corp. v. Catrett, 477 U.S. 317, 322 (1986).

33. *Id.*

34. *Jewel*, 2015 WL 545925, at *5.

35. Mohamed v. Jeppesen DataPlan, Inc., 614 F.3d 1070, 1083 (9th Cir. 2010); *see also* Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 991-92 (N.D. Cal. 2006) (holding that AT&T aids the government in the collection of Internet communications).

adjudication due to the necessity of classified information.[36]

The instant case was before the Court on Plaintiffs' motion for partial summary judgment and Defendants' cross-motion for partial summary judgment following the Court's order for briefings on the subject.[37] Plaintiffs alleged that Defendants received copies of their Internet communications from their service provider, AT&T, filtered them to remove domestic communications, and then searched the remaining communications for "potentially terrorist-related foreign intelligence information."[38] At issue is a FISA section 702 directive called the Upstream collection program. Plaintiffs contended that the possible interception of their Internet communications by the NSA without a warrant or "individualized suspicion" violates their Fourth Amendment protection.[39] In response, Defendants contended that Plaintiffs lacked standing and that, even if Plaintiffs established standing, the state secrets privilege requires dismissal of Plaintiffs' claim.[40]

The Court found that Plaintiffs sufficiently established that, as AT&T customers and Internet users, their communications were likely to be captured under the wide net casted by the Upstream collection program.[41] However, the Court was persuaded by Defendants' arguments. The Court held that Plaintiffs' witness testimony was "substantially inaccurate" because it was speculative and based on insufficient facts.[42] Moreover, the Court reviewed the classified portions of the Defendants' brief and found that they must remain classified in the interest of national security.[43] The Court reasoned that because a fair and full adjudication of the Defendant's arguments was not possible without the privileged information, the Court was forced to deny Plaintiffs' motion for partial summary judgment and grant Defendants' cross-motion for partial summary judgment.[44] The Court did not rule on the substantive issue: the constitutionality of the NSA's Upstream collection program.[45] Plaintiffs have since appealed the Court's decision.[46]

---

36. *Jewel*, 2015 WL 545925, at *5.
37. *Id.* at *1.
38. *Id.*
39. *Id.* at *2.
40. *Id.*
41. *Id.* at *4.
42. *Id.*
43. *Id.* at *5.
44. *Id.*
45. *Id.*
46. Jewel v. Nat'l Sec. Agency, 810 F.3d 622 (9th Cir. 2015).

ANALYSIS

The instant case was decided incorrectly because the Court did not rule on the constitutionality of the NSA's Upstream collection program. The Court properly found that Plaintiffs had sufficiently proven to have stake in the outcome of the case because AT&T, Plaintiffs' service provider, aided the government in the collection of Internet communications.[47] However, the Court disregarded FISA's procedure for reviewing classified information, 50 U.S.C. § 1806(f).[48] Consequently, the Court improperly held that individuals lacked standing to challenge the constitutionality of the NSA surveillance program under FISA, contradicting its previous ruling.[49]

At first glance, one might argue that the Court decided the instant case correctly because, as Defendants contended, Plaintiffs failed to prove that the surveillance occurred as Plaintiffs alleged.[50] It is true that Plaintiffs relied on the declarations of a former AT&T technician who did not have actual knowledge of the program's operation and, as a result, Plaintiffs did not meet the burden of proof necessary to survive a motion for summary judgment. However, the Court ignored the case law it cited.

Plaintiffs did not intend to show the Court how the NSA surveillance program operates and this should not have prevented Plaintiffs' from establishing standing. Together, *Clapper* and *Klayman*, cases on which the court relied, support Plaintiffs' contention that as customers of a service provider that aids in the collection of Internet communications, Plaintiffs have standing to challenge the statute's constitutionality.[51]

Moreover, the Court may have taken their analysis one step too far when it required that Plaintiffs also establish exactly how the program works. The process outlined by NSA Director of Signals Intelligence Directorate, Teresa H. Shea, comments on the NSA's vast and all-inclusive surveillance.[52] Similarly, Section 702 of FISA is sufficient to establish how the program operates, as it outlines the NSA's surveillance procedures.[53] Standing alone should have been sufficient for the Court to rule on the program's constitutionality.

Furthermore, FISA's legislative history and a plain reading of the

47. *See* Hepting v. AT & T Corp., 439 F. Supp. at 991-92 (N.D. Cal 2006).
48. 50 U.S.C. § 1806(f) (2015).
49. *Jewel*, 965 F. Supp. 2d at 1105-06.
50. *Jewel*, 2015 WL 545925 at *5.
51. *Klayman*, 957 F. Supp. at 26-28; *see also Clapper*, 133 S. Ct. 1150.
52. *Id.* at 28.
53. Jewel v. Nat'l Sec. Agency, No. 08-CV-04373-JSW, 2015 WL 545925 at *1 (N.D. Cal. Feb. 10, 2015).

provisions in question demonstrate that it was written to supplant federal common law rules.[54] Specifically, FISA was written to preempt the state secrets privilege.[55] Thus, the Court incorrectly permitted the government's use of the state secrets privilege. FISA provides a method of review that permits the Court to competently weigh both parties' arguments without disclosing classified information.[56] Adoption of this method would have permitted the Court to rule on the constitutionality of the surveillance program without risking damage to national security. Case law and Congress intended for this to be the case.

An unforeseen ramification is that while allowing the government to raise the state secrets privilege did not affect the Court's disposition, it will likely serve as precedent on future challenges. This decision has the potential to function as an extra layer of protection for the government from constitutional challenges, permitting it to keep stretching the scope of its powers in electronic surveillance.

This case is a result of the nation's war on terror. History shows that, in a time of war, the judiciary constantly justifies the government's actions in the name of national security, even if they stretch beyond the scope of the government's powers.[57] The problem may lie in how the judiciary views possible threats to national security. The judiciary may have to choose between upholding the laws and values of the Constitution and interpreting them to benefit the government at the expense of the people. Another approach altogether may be useful to the judiciary and preserve individuals' constitutionally protected rights. Thus, Plaintiffs' appeal will likely be a step in the right direction.

CONCLUSION

The Fourth Amendment of the U.S. Constitution protects individuals from "unreasonable searches and seizures,"[58] but what that means remains unclear. However, this ambiguity does not permit the government to act beyond the scope of its powers and arbitrarily intrude on individuals' constitutionally protected right to privacy.

Following the 2001 terrorist attacks on the World Trade Center, the government's focus on preventing future attacks opened a floodgate of litigation about the collaboration between the NSA and service providers.

54. 50 U.S.C. § 1806(f) (2015).
55. *Jewel*, 965 F. Supp. 2d at 1105-06.
56. 50 U.S.C. § 1806(f) (2015).
57. *See* Korematsu v. United States, 323 U.S. 214 (1944)
58. U.S. CONST. amend. IV.

In the instant case, the Court contradicted itself to protect the government under the guise of national security's best interest. After previously ruling that FISA preempts the state secrets privilege and outlines procedures by which the Court can review classified information without disclosing it to determine if the surveillance is lawful,[59] the Court decided to disregard the statutory procedure available.[60]

The judiciary was created to provide consistency and uniformity in the law. In this case, it has done the opposite. While national security is certainly a priority, it is not enough to deprive individuals of their constitutionally protected right to privacy and relief, especially when the statute in question provided a way to maintain secrecy while allowing a fair and full adjudication of the claim. Simply put, the Court protected its own with this ruling, which will likely affect future parties intending to pursue similar claims.

59. Jewel v. Nat'l Sec. Agency, 965 F. Supp. 2d at 1105-06 (N.D. Cal. 2013).
60. 50 U.S.C. § 1806(f) (2015).