LAWLESS SURVEILLANCE, WARRANTLESS RATIONALES*

CINDY COHN**

In the four years since it was first revealed, the United States National Security Agency's warrantless domestic surveillance programs have been the subject of front page news stories,[1] multiple books,[2] dramatic hospital room confrontations,[3] and a heated Congressional battle culminating in an unprecedented law allowing the Attorney General to grant legal immunity to telecommunications companies for behavior they never admitted doing yet simultaneously claimed was lawful.[4] What it hasn't been subject to is a formal adjudication of whether this plainly ongoing activity is legal or constitutional.

Both former NSA Director Michael Hayden and former Justice Department attorney John Yoo took to the editorial pages of major

---

* This article is adapted from an op-ed, which was published by the American Constitution Society blog: Posting of Cindy Cohn to ACSblog, Lawless Surveillance, Warrantless Rationales, http://www.acslaw.org/node/13922 (Aug. 17, 2009, 10:57).

** Legal Director, Electronic Frontier Foundation. Ms. Cohn and Electronic Frontier Foundation serve as counsel to the plaintiffs in two lawsuits arising out of the warrantless domestic surveillance dragnet, *Hepting v. AT&T Corp.* and *Jewel v. NSA*, both currently pending before the Ninth Circuit Court of Appeals. *See* Hepting v. AT&T Corp., No. 06-CV-00672 (N.D. Cal. July 21, 2009), *appeal docketed*, No. 09-16676 (9th Cir. Aug. 7, 2009); Jewel v. NSA, No. C-06-1791, 2010 WL 235075 (N.D. Cal. Jan. 21, 2010), *appeal docketed*, No. C-08-4373 (9th Cir. Mar. 19, 2010). EFF also serves as co-lead coordinating counsel for all of the plaintiffs in the ongoing multi-district litigation arising out of the various claims of warrantless wiretapping by the National Security Agency.

1. *See, e.g.*, Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at 1A; Eric Lichtblau & James Risen, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1; Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES, Dec. 24, 2005, at A1; Joseph Menn & Josh Meyer, *U.S. Spying is Much Wider, Some Suspect*, L.A. TIMES, Dec. 25, 2005, at A1.

2. *See, e.g.*, BARTON GELLMAN, ANGLER: THE CHENEY VICE PRESIDENCY (2008); JACK L. GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION (2007); ERIC LICHTBLAU, BUSH'S LAW: THE REMAKING OF AMERICAN JUSTICE (2008); JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION (2006).

3. *See* Dan Eggen & Paul Kane, *Gonzales Hospital Episode Detailed: Ailing Ashcroft Pressured on Spy Program, Former Deputy Says*, WASH. POST, May 16, 2007, at A01; *see also* OFFICES OF THE INSPECTORS GENERAL, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 24-26 (2009), *available at* http://www.fas.org/irp/eprint/psp.pdf.

4. *See* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 50 U.S.C. § 1885a (2008).

national newspapers in the summer of 2009 to defend the still-shadowy set of programs that spy on Americans in America without any probable cause or warrant.[5] This campaign to sway public opinion continues, despite the ongoing revelations of the government's activity, because neither the past Bush officials nor the current Obama administration officials dare to defend the wholesale surveillance of millions of Americans on the merits in a court of law. Meanwhile, a new court ruling places judicial review of the spying even further out of reach.[6]

While the exact details are unknown, credible evidence indicates that billions of everyday communications of ordinary Americans are swept up by government computers and run through data-mining or other technical processes, likely culminating in human review of computer-selected communications.[7] That means that even the most personal and private of our electronic communications—between doctors and patients, between husbands and wives, or between children and parents—are subject to review by computer algorithms programmed by government bureaucrats, with some unknown portion reviewed by the bureaucrats themselves.

---

5. *See* Michael Hayden, *Warrantless Criticism*, N.Y. TIMES, July 26, 2009, at A21; John Yoo, *Why We Endorsed Warrantless Wiretaps*, WALL ST. J., July 16, 2009, at A13.

6. *See* Jewel v. NSA, No. C 06-1791, 2010 WL 235075 (N.D. Cal. Jan. 21, 2010), *appeal docketed*, No. C-08-4373 (9th Cir. Mar. 19, 2010).

7. *See* Declaration of Mark Klein in Support of Plaintiffs' Motion for Preliminary Injunction, Hepting v. AT&T, 439 F. Supp. 2d 974 (N.D. Cal. 2006), *available at* http://www.eff.org/files/filenode/att/Mark%20Klein%20Unredacted%20Decl-Including%20Exhibits.PDF (declaration of AT&T whistleblower describing massive NSA spying operation in AT&T San Francisco facility); Declaration of J. Scott Marcus in Support of Plaintiffs' Motion for Preliminary Injunction, *Hepting*, 439 F. Supp. 2d 974, *available at* http://www.eff.org/files/filenode/att/Marcus%20Declaration%20Including%20Exhibits.pdf (expert declaration reviewing whistleblower evidence and concluding it is consistent with a nationwide network of government surveillance hubs attached to key telecommunications switches); *see also*, *e.g.*, Barton Gellman, et al., *Surveillance Net Yields Few Suspects*, WASH. POST, Feb. 5, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/02/04/AR2006020401373.html ("Surveillance takes place in several stages . . . the earliest by machine . . . . Successive stages of filtering grow more intrusive as artificial intelligence systems rank voice and data traffic in order of likeliest interest to human analysts . . . . [T]his kind of filtering intrudes into content, and machines 'listen' to more Americans than humans do."); Shane Harris & Tim Naftali, *Tinker, Tailor, Miner, Spy: Why the NSA's Snooping is Unprecedented in Scale and Scope*, SLATE, Jan. 3, 2006, http://www.slate.com/id/2133564/ ("[Telecommunications] companies have granted the NSA access to their all-important switches, the hubs through which colossal volumes of voice calls and data transmissions move every second . . . . [T]he NSA appears to be vacuuming up all data, generally without a particular phone line, name, or e-mail address as a target."); Lichtblau & Risen, *supra* note 1 (describing how the NSA had obtained "backdoor access to streams of domestic and international communication" via arrangements with "some of the nation's largest telecommunications companies to gain access to [telecommunications] switches," and describing the NSA program as a "large data-mining operation" in which NSA personnel comb through large volumes of phone and Internet traffic in search of patterns that might point to persons of interest).

The scale of the surveillance seems overwhelming, almost impossible. Yet the NSA apparently thinks it can do it. The agency is building a million square foot data storage facility at a cost of $2 billion in Utah and another large facility in San Antonio.[8] Noted author and NSA-watcher James Bamford notes that the NSA is planning to have gathered Yottabytes of data, or 1,000,000,000,000,000,000,000,000 pages of text, by 2015.[9] According to Bamford, the new facilities in Utah and Texas will be used "[t]o house trillions of phone calls, email messages and data trails: Web searches, parking receipts, bookstore visits, and other digital 'pocket litter.'"[10] This massive collection continues despite increasing indications that such data mining is "[n]ot well suited to the terrorist discovery problem."[11]

It's a remarkable turn of events, this shift from the traditional limitations on search and seizure to the wholesale scooping up and storing of our communications, our communications records, and indeed our entire digital lives. The United States was founded on the rejection of such wholesale collection of citizen communications and papers. In the late 1700s, "general warrants" were pieces of paper that gave the Executive (then the King) power to search colonial Americans without cause.[12] These general warrants were routinely used by British customs inspectors to search and seize papers in colonial homes in search of evidence of smuggling.[13] Indeed, John Adams noted that "the child Independence was born" when Boston merchants represented by James Otis unsuccessfully sued to stop these unchecked powers.[14] The Fourth Amendment was adopted in part to stop these "hated writs"[15] and to make sure that searches of the papers of Americans required an individualized, probable cause showing to a court.[16]

8. James Bamford, *Who's in Big Brother's Database?*, 56 N.Y. REV. OF BOOKS 17 (2009) (reviewing MATTHEW M. AID, THE SECRET SENTRY: THE UNTOLD HISTORY OF THE NATIONAL SECURITY AGENCY (2009) (citing MITRE CORP., DATA ANALYSIS CHALLENGES 13 (2008)).

9. Bamford notes that numbers greater than a Yottabyte have yet to be named. *Id.*

10. *Id.*

11. Jeff Jonas & Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, CATO INST. POL'Y ANALYSIS, Dec. 2006, at 1–2; *see also* WILLIAM J. PERRY ET AL., PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENT (2008) (finding that data mining is not very helpful for counterterrorism).

12. Boyd v. United States, 116 U.S. 616, 625 (1886).

13. Payton v. New York, 445 U.S. 573, 608 (1980); Stanford v. Texas, 379 U.S. 476, 484 (1965); United States v. Lefkowitz, 285 U.S. 452, 466 (1932).

14. Founders of America, Otis Was a Flame of Fire, http://www.foundersofamerica.org/jotis.html (last visited Jan. 24, 2010).

15. *Stanford*, 379 U.S. at 481.

16. *Id.*; *see also generally* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547 (1999) (exhaustively surveying history of Fourth Amendment and concluding that Framers' primary intent was to condemn general warrants).

The wholesale collection of American "papers" as part of the warrantless surveillance programs then returns us to the policies of King George III—only with a digital boost. The programs collect our emails, phone calls, Internet searches, website visits, Facebook posts, and other Internet data and subject them to computer review to pick out what will be reviewed by human analysts. This first step can lead to even more intrusive review by faceless government computers and bureaucrats when the computer programs written by the bureaucrats determine that our communications or communications patterns merit further scrutiny.[17]

So how is this digital return to general warrants being defended outside the courts? Both Yoo and Hayden draw from a similar bag of tricks. First, they claim that there was a "gap" between our domestic security and our foreign intelligence surveillance.[18] What they appear to be referencing is the fact that there are more barriers to NSA surveillance inside of the United States than outside of the United States. But this is because those outside of the United States do not enjoy the protections of the U.S. Constitution and our longstanding privacy laws and so can be freely surveilled. It has long been known, including through a report by the European Parliament, that the NSA has set up "listening stations" outside of the United States to sweep up foreign-to-foreign communications on a wholesale basis.[19] So what Yoo and Hayden are calling a "gap" appears to arise from the fact that longstanding constitutional and statutory privacy protections prevent the NSA from engaging in the same kind of wholesale listening in on Americans in America that the agency routinely engages in abroad. Yet far from being a problem or a "gap," these are some of the crucial limitations on the power of government that safeguard our freedoms.[20]

Second, Yoo and Hayden cite briefings given to a few, select members of Congress as demonstrating that the surveillance programs

17. *See supra* notes 1 & 7.

18. Hayden, *supra* note 5; *see* Yoo, *supra* note 5.

19. STEVE WRIGHT, EUROPEAN PARLIAMENT, DIRECTORATE GENERAL FOR RESEARCH, AN APPRAISAL OF TECHNOLOGIES OF POLITICAL CONTROL (1998), *available at* http://cryptome.org/stoa-atpc.htm (European Parliament report describing "a global surveillance system that stretches around the world to form a targeting system on all of the key Intelsat satellites used to convey most of the world's satellite phone calls, internet, email, faxes and telexes," called Echelon); Jason Leopold, *Revisiting Echelon: The NSA's Clandestine Data Mining Program*, THE PUB. REC., Jul. 15, 2009, http://pubrecord.org/nation/2290/revisiting-echelon-nsas/ (describing relationship between NSA program and Echelon).

20. Another theory for the "gap" reference is that the NSA wishes to be able to intercept from inside the United States foreign to foreign or one-end foreign communications that transit through the United States. But the NSA has never explained why those communications, which by definition travel *outside* the United States for some part of their journeys, could not be intercepted at its foreign listening stations.

are not to be feared.[21] Yet neither the full Congress, nor even the full intelligence committees were informed, and those who participated have long complained that the briefings were often incomplete and even possibly misleading.[22]

Third, Yoo and Hayden defend the warrantless surveillance by claiming that it was approved by the hand-picked Bush administration political appointee attorneys.[23] But as the Constitution's careful separation of powers requirements attest, the Executive branch simply cannot be relied upon to police itself, nor should its own secret, internal justifications for its behavior replace formal, external judicial review. Political appointees answer to the President; and the Fourth Amendment's requirement that a court, not the Executive, review and approve surveillance requests is no accident. As the Supreme Court has noted, the Constitution protects us by "divid[ing] power . . . among branches of government precisely so that we may resist the temptation to concentrate power in one location as an expedient solution to the crisis of the day."[24]

Moreover, even on its own terms, the claim that Executive branch officials signed off on the warrantless wiretapping program is weak. Jack Goldsmith, one of those hand-picked Bush administration lawyers, pronounced the wiretapping program "the biggest legal mess" he had seen in his life.[25]

Aside from the attempted justifications of Yoo and Hayden, the Bush Administration's central view was that, when taking steps that it deemed necessary for national security, the Executive branch was somehow above the niceties of the Constitution.[26] As a result, it is unsurprising that they believed the President could ignore the

21. Hayden, *supra* note 5; *see* JOHN YOO, WAR BY OTHER MEANS: AN INSIDER'S ACCOUNT OF THE WAR ON TERROR 115–18 (2006).

22. *See* OFFICES OF THE INSPECTORS GENERAL, *supra* note 3, at 23 n. 16 (describing how U.S. Senators and Representatives dispute the Administration's characterization of Congressional briefings on the NSA program); *see also* Letter from Harry Reid, Democratic Leader, U.S. Senate, John D. Rockefeller IV, Vice Chairman of the Select Comm. on Intelligence, U.S. Senate, & Patrick Leahy, Ranking Democrat of the Comm. on the Judiciary, U.S. Senate to George W. Bush, U.S. President (Dec. 20, 2005), http://democrats.senate.gov/newsroom/record.cfm?id=250189 (letter from Democratic leaders in Senate to President demanding information on NSA program and noting that "public statements by several of the handful of Members of Congress who were provided a briefing on this program indicate that insufficient information was provided to them under ground rules that did not enable Congress to conduct satisfactory oversight.").

23. Hayden, *supra* note 5; Yoo, *supra* note 5.

24. Printz v. United States, 521 U.S. 898, 933 (1997) (quoting New York v. United States, 505 U.S. 144, 187 (1992)).

25. Dan Eggen, *White House Secrecy On Wiretaps Described*, WASH. POST, Oct. 3, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/10/02/AR2007100201083.html.

26. *See* Yoo, *supra* note 5.

constitutional and statutory provisions that had long prevented the NSA from engaging in wholesale spying on Americans on American soil. What's clear now, and deeply distressing, is President Obama's embrace of this radical view, rejecting the bedrock principle that the Constitution and the rule of law place limits on Executive power.[27] Despite running on promises to return the country to the proper constitutional balance, President Obama's Justice Department has been pulling out all the stops to block the courts from reviewing the domestic surveillance programs while giving no indication that the surveillance itself has ceased.[28]

Unfortunately, the District Court faced with these arguments ducked them altogether, and instead blazed its own, equally dangerous path.[29] The Court dismissed the cases on the incorrect conclusion that, because so many individuals were impacted by the widespread surveillance, the plaintiffs had no standing.[30] This argument, which was not raised by either party in the case, mischaracterizes the claims as presenting a "generalized grievance" akin to a mere policy dispute, rather than "particularized injury" suffered by the plaintiffs necessary for standing. Aside from ignoring the actual concrete harm to each individual whose conversations and emails were illegally intercepted and reviewed or processed, this holding would have the courts blind themselves to statutory and constitutional violations on the grounds that they impact too many people. Such a finding, if upheld on appeal, would grant the government the ability to conduct whatever surveillance it likes, so long as it violates the privacy of many, many Americans rather than just a few. Even if reversed on appeal, the ruling threatens to place actual judicial consideration of the merits of the surveillance years away.

Thus, the core constitutional crisis caused by the domestic surveillance programs remains. While we can expect to see more attempts to shape public opinion by powerful current and former Executive branch figures, no amount of op-ed window dressing can hide the central fact that the domestic surveillance programs are a digital version of general warrants and a return to the "hated writs" of the Founders. The failure of the Executive to submit these programs to the judiciary for a true constitutional and legal review speaks far louder than

27. *See* Press Release, Electronic Frontier Foundation, Obama Administration Embraces Bush Position on Warrantless Wiretapping and Secrecy: Says Court Must Dismiss *Jewel v. NSA* to Protect 'State Secrets' (Apr. 6, 2009), http://www.eff.org/press/archives/2009/04/05; *see also* Zachary Roth, *Expert Consensus: Obama Mimics Bush on State Secrets*, TPMMUCKRACKER, Apr. 9, 2009, http://tpmmuckraker.talkingpointsmemo.com/2009/04/expert_consensus_obama_aping_bush_on_state_secrets.php.

28. Opinion, *Obama Channels Cheney: Obama Adopts Bush View on the Powers of the Presidency*, WALL ST. J., Mar. 7, 2009, at A10.

29. *See* Jewel v. NSA, No. C 06-1791, 2010 WL 235075 at *2–3 (N.D. Cal. Jan. 21, 2010)), *appeal docketed*, No. C-08-4373 (9th Cir. Mar. 19, 2010).

30. *Id.*

the self-serving justifications of former officials, even when they are published in our nation's leading newspapers.