2004

Reconstructing Electronic Surveillance Law

Daniel J. Solove
George Washington University Law School, dsolove@law.gwu.edu

Reconstructing Electronic Surveillance Law

Daniel J. Solove*

Table of Contents

Introduction

After the September 11 attacks, Congress hastily passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"),[1] which made several changes to electronic surveillance law. The Act has sparked a fierce debate.[2] The pros and cons of the USA PATRIOT Act,

* Associate Professor, The George Washington University Law School; J.D. Yale Law School. Thanks to Patricia Bellia, Linda Fisher, Chris Hoofnagle, Orin Kerr, Raymond Ku, Peter Raven-Hansen, Stephen Saltzburg, Paul Schwartz, and Peter Swire for helpful comments on the manuscript. I would also like to thank Romana Kaleem for excellent research assistance.

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

[2] *See, e.g.*, Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 637 (2003); Steven A. Osher, *Privacy, Computers, and the Patriot Act: The Fourth Amendment Isn't Dead, but No One Will Insure It*, 54 FLA. L. REV. 521, 542 (2002); Alison A. Bradley, Comment, *Extremism in the Defense of Liberty?: The Foreign Intelligence Surveillance Act and the Significance of the USA Patriot Act*, 77 TUL. L. REV. 465, 467 (2002); Susan W. Dean, Comment, *Government Surveillance of Internet Communications: Pen Register and Trap and Trace Law Under the Patriot Act*, 5 TUL. J. TECH. & INTELL. PROP. 97, 98 (2003); Michael F. Dowley, Note, *Government Surveillance Powers Under the USA Patriot Act: Is It Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War,* 36 SUFFOLK

however, are only one part of a much larger issue: How effective is the law that regulates electronic surveillance?

Today, technology has given the government an unprecedented ability to engage in surveillance. New X-ray devices can see through people's clothing, amounting to what some call a "virtual strip-search."[3] Thermal sensors can detect movement and activity via heat patterns.[4] Telephone calls can be wiretapped; places can be "bugged" with hidden recording devices; and parabolic microphones can record conversations at long distances.[5] A device known as Carnivore developed by the Federal Bureau of Investigation ("FBI") can scan through all of the e-mail traffic of an internet service provider ("ISP").[6] Keystroke logger devices can record every keystroke typed on one's computer,[7] and these devices can be installed into a person's computer by e-mailing a computer virus called "Magic Lantern."[8] Tracking devices can relay information about a person's whereabouts.[9] One can trace cell phone calls to a person's particular location.[10]

Surveillance cameras have become ubiquitous. Britain has erected an elaborate system of video cameras which enable officials to monitor city

U. L. REV. 165, 167 (2002); Jennifer C. Evans, Comment, *Hijacking Civil Liberties: The USA Patriot Act of 2001*, 33 LOY. U. CHI. L.J. 933, 934 (2001); David Hardin, Note, *The Fuss Over Two Small Words: The Unconstitutionality of the USA Patriot Act Amendments to FISA Under the Fourth Amendment*, 71 GEO. WASH. L. REV. 291, 294 (2003); Nathan C. Henderson, Note, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications*, 52 DUKE L.J. 179, 180 (2002); Sharon H. Rackow, Comment, *How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of 'Intelligence' Investigations*, 150 U. PA. L. REV. 1651, 1653 (2002); Anne Uyeda, Note, *The USA Patriot Act May Infringe on Civil Liberties in Cyberspace*, 2002 UCLA J.L. & TECH. NOTES 1, ¶ 4 (2002), *at* http://www.lawtechjournal.com/notes/2002/01_020204_uyeda.php (last visited June 9, 2004).

[3] Ivan Amato, *Future Tech: Beyond X-ray Vision: Can Big Brother See Right Through Your Clothes?*, DISCOVER, July 2002, at 24; Guy Gugliotta, *Tech Companies See Market for Detection; Security Techniques Offer New Precision*, WASH. POST, Sept. 28, 2001, at A8.

[4] *See* Kyllo v. United States, 533 U.S. 27, 29–30 (2001).

[5] The opening to the movie *The Conversation* provides an illustration of the use of parabolic microphones. *See* THE CONVERSATION (Paramount Studio 1974).

[6] *See generally* E. Judson Jennings, *Carnivore: U.S. Government Surveillance of Internet Transmissions*, 6 VA. J.L. & TECH. 10, § 2 (2001), *at* http://www.vjolt.net/vol6/issue2/v6i2-a10-Jennings.html (last visited June 9, 2004).

[7] *See* United States v. Scarfo, 180 F. Supp. 2d 572, 574 (D.N.J. 2001).

[8] Ted Bridis, *FBI Is Building a "Magic Lantern"; Software Would Allow Agency to Monitor Computer Use*, WASH. POST, Nov. 23, 2001, at A15.

[9] *See* United States v. Karo, 468 U.S. 705, 708 (1984); United States v. Knotts, 460 U.S. 276, 277 (1983).

[10] Christine Tatum, *Navigators Hit Road in Digital Quest*, CHI. TRIB., July 29, 2002, § 4 at 3.

streets through closed circuit television.[11] Called CCTV, this system has grown rapidly ever since it was first used in 1994 in response to terrorist bombings.[12] By 2001, according to estimates, Britain had one-half million surveillance cameras, one for every 120 people.[13] The United States has begun moving toward the British model. In 2002, the U.S. National Park Service installed surveillance cameras around national monuments in Washington, D.C.[14]

Surveillance technology can be a useful law enforcement tool, for it provides the government with the power to watch people's activities and listen to their conversations. These profound powers, however, raise difficult problems. As with many countries throughout the world, the United States has enacted a series of laws to balance the benefits and dangers of surveillance.

Electronic surveillance law in the United States is comprised primarily of two statutory regimes: (1) the Electronic Communications Privacy Act ("ECPA"),[15] which is designed to regulate domestic surveillance; and (2) the Foreign Intelligence Surveillance Act of 1978 ("FISA"),[16] which is designed to regulate foreign intelligence gathering. While other statutes provide additional protection, ECPA and FISA are the heart of electronic surveillance law.

The USA PATRIOT Act made a number of changes in electronic surveillance law, but the most fundamental problems with the law did not begin with the USA PATRIOT Act. In this Article, I suggest that electronic surveillance law suffers from significant problems that predate the USA PATRIOT Act. The USA PATRIOT Act indeed worsened some of these problems, but surveillance law had lost its way long before. Surveillance law is thus in need of a radical reconstruction; I aim to provide some guidance to start this endeavor.

In Part II, I discuss the purpose and history of electronic law. In Part III, I analyze several problems with existing surveillance law. I begin by focusing on specific difficulties with the scope, standards, and enforcement mechanisms of the statutes. Next, I examine the more deeply rooted and

---

[11] *See generally* CLIVE NORRIS & GARY ARMSTRONG, THE MAXIMUM SURVEILLANCE SOCIETY: THE RISE OF CCTV (1999); Jeffrey Rosen, *A Cautionary Tale for a New Age of Surveillance*, N.Y. TIMES, Oct. 7, 2001, § 6 (Magazine).

[12] NORRIS & ARMSTRONG, *supra* note 11; Rosen, *supra* note 11, at 41.

[13] Charles Goldsmith et al., *Tuesday's Attack Forces an Agonizing Decision on Americans*, WALL ST. J., Sept. 14, 2001, at A8.

[14] David A. Fahrenthold, *Cameras to Oversee Festivities for Fourth*, WASH. POST, July 3, 2002, at A1; Spencer S. Hsu, *D.C. Police Offer Rules for Video Surveillance*, WASH. POST, Apr. 10, 2002, at B1.

[15] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

[16] The Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1811 (2000)).

systematic problems. I contend that electronic surveillance law is overly intricate and complex, that it has failed to keep pace in adapting to new technologies, and that it provides for insufficient judicial and legislative oversight. In Part IV, I suggest ways in which surveillance law should be reconstructed to address these problems. Specifically, I recommend a rather radical solution: Warrants supported by probable cause should be required for most uses of electronic surveillance. I explain why this solution best resolves the existing problems with electronic surveillance law, and I argue that this approach is flexible and practical. Finally, I recommend that Congress draft a charter regulating the FBI.

I. The Purpose and History of Electronic Surveillance Law

In order to examine the effectiveness of electronic surveillance law and the methods by which to improve it, we must first articulate the goals that we want the law to achieve. At a very general level, the law of electronic surveillance recognizes two things: that government surveillance is good and that it is bad. Surveillance is an important law enforcement tool, and it can be highly effective at solving and preventing crimes. Thus, we want the government to be able to engage in certain forms of surveillance. But surveillance is also a very dangerous tool, with profound implications for our freedom and democracy. Hence, we also want government surveillance to be tightly controlled.

Our electronic surveillance law was created in response to specific problems. It was thus borne out of experience, and it is designed to redress these problems. In this Part, I discuss the animating problems and concerns of surveillance law. I examine the costs and benefits of electronic surveillance as well as the history of how and why surveillance law developed the way it did.

A. Surveillance: The Good and the Bad

Electronic surveillance is one of the central tools of modern law enforcement. It can aid significantly in the investigations of crimes, for it allows the government to watch and listen to people during their unguarded moments, when they may speak about their criminal activity. Video cameras may capture criminals in the act and aid in their identification and arrest. Surveillance can also assist in preventing crimes because it enables the government to learn about criminal activity that is afoot and to halt it before it happens. Few would argue that these are not significant benefits.

Surveillance can also prevent crime in another way. In 1791, Jeremy Bentham imagined a new architectural design for a prison which he called the Panopticon.[17] As Michel Foucault describes it:

[17] *See* DAVID LYON, THE ELECTRIC EYE: THE RISE OF THE SURVEILLANCE SOCIETY 62 (1994).

> [A]t the periphery, an annular building; at the centre, a tower; this tower is pierced with wide windows that open onto the inner side of the ring; the peripheric building is divided into cells, each of which extends the whole width of the building . . . . All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy. By the effect of backlighting, one can observe from the tower, standing out precisely against the light, the small captive shadows in the cells of the periphery. They are like so many cages, so many small theatres, in which each actor is alone, perfectly individualized and constantly visible.[18]

The Panopticon achieves obedience and discipline by having all prisoners believe they could be watched at any moment. Their fear of being watched inhibits transgression. Surveillance can thus prevent crime by making people decide not to engage in it at all. More generally, surveillance is good because it is a highly effective tool for maintaining social order. We want to foster a society where people are secure from theft, vandalism, assault, murder, rape, and terrorism. We thus desire social control, and surveillance can help achieve that end.

But surveillance is bad for the very same reason. George Orwell's *Nineteen Eighty-Four* chronicles a totalitarian government called "Big Brother" that aims for total social control.[19] Everyone is under constant fear of being watched or overheard, and everything that people do is rigidly controlled by the government.[20] In contrast to the society depicted in Orwell's novel, our society aims to be free and democratic, and our government is a far cry from Big Brother. The goal is not to suppress all individuality, to force everybody to think and act alike. Our government, however, has some of the same surveillance capabilities as Big Brother. And even when the government does not aim for total social control, surveillance can still impair freedom and democracy.

Surveillance has negative side effects that affect both the observed and the observers. For the observed, surveillance can lead to self-censorship and inhibition.[21] According to Julie Cohen: "Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream."[22] Monitoring constrains the "acceptable spectrum of belief and behavior," and it results in "a subtle yet fundamental shift in the

---

[18] MICHEL FOUCAULT, DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON 200 (Alan Sheridan trans., Vintage Books 1st ed. 1979) (1975).

[19] GEORGE ORWELL, NINETEEN EIGHTY-FOUR 3 (Alfred A. Knopf, Inc. 1992) (1949).

[20] *See id.*

[21] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1260 (1998).

[22] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000).

content of our character, a blunting and blurring of rough edges and sharp lines."[23] Surveillance "threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it."[24] Paul Schwartz argues that surveillance inhibits freedom of choice, impinging upon self-determination.[25] Surveillance rigidifies one's past; it is a means of creating a trail of information about a person. Christopher Slobogin argues that being placed under surveillance impedes one's anonymity, inhibits one's freedom to associate with others, makes one's behavior less spontaneous, and alters one's freedom of movement.[26] Surveillance's inhibitory effects are especially potent when people are engaging in political protest or dissent. People can face persecution, public sanction, and blacklisting for their unpopular political beliefs. Surveillance can make associating with disfavored groups and causes all the more difficult and precarious.

For the observers, surveillance presents a profound array of powers that are susceptible to abuse. As Raymond Ku notes, the Framers of the Constitution were concerned about "unfettered governmental power and discretion."[27] The Framers were deeply opposed to general warrants and writs of assistance.[28] General warrants "resulted in 'ransacking' and seizure of the personal papers of political dissidents, authors, and printers of seditious libel."[29] Writs of assistance authorized "sweeping searches and seizures without any evidentiary basis."[30] As Patrick Henry declared: "They may, unless the general government be restrained by a bill of rights, or some similar restrictions, go into your cellars and rooms, and search, ransack, and measure, every thing you eat, drink, and wear. They ought to be restrained within proper bounds."[31] The problem, in short, is with the

---

[23] *Id.*

[24] *Id.*

[25] *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1656 (1999) ("[P]erfected surveillance of naked thought's digital expression short-circuits the individual's own process of decisionmaking."); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560 (1995).

[26] Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 237–67 (2002).

[27] Raymond Shih Ray Ku, *The Founder's Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1332 (2002).

[28] *See* LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 158 (1999); Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse than the Disease*, 68 S. CAL. L. REV. 1, 8 (1994).

[29] DAVID M. O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY 38 (1979); *see also* William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 406 (1995).

[30] Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 82 (1988).

[31] 3 THE DEBATES IN SEVERAL CONVENTIONS ON THE ADOPTION OF THE FEDERAL

government having too much power.

Electronic surveillance presents additional problems. It is a sweeping form of investigatory power. It extends beyond a search, for it records behavior, social interaction, and everything that a person says and does. Rather than a targeted query for information, surveillance is often akin to casting a giant net, which can ensnare a significant amount of data beyond that which was originally sought. As James Dempsey notes, electronic surveillance captures a wide range of communications, "whether they are relevant to the investigation or not, raising concerns about compliance with the particularity requirement in the Fourth Amendment and posing the risk of general searches."[32] Moreover, unlike a typical search, which is often performed in a short once-and-done fashion, electronic surveillance "continues around-the-clock for days or months."[33] Additionally, in a regular search, the government comes to a suspect's house and often searches while the suspect is present; on the other hand, "the usefulness of electronic surveillance depends on lack of notice to the suspect."[34] As Justice Douglas observed, wiretapping can become "a dragnet, sweeping in all conversations within its scope."[35]

Dissenting from *Lopez v. United States*,[36] where the Court upheld the use of a pocket wire recorder to record a conversation, Justice Brennan observed that surveillance "makes the police omniscient; and police omniscience is one of the most effective tools of tyranny."[37] As Justice Brandeis observed:

> Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded and all conversations between them upon any subject, although proper, confidential and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping.[38]

Furthermore, information collected by electronic surveillance can potentially be abused. Even if abuses are rare or the risk of abuse is low, the existence of legal protection is comforting and freedom-enhancing.

CONSTITUTION 448–49 (Jonathan Elliot ed., 1974).

32 James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 70 (1997).

33 *Id.*

34 *Id.*

35 Berger v. New York, 388 U.S. 41, 65 (1967) (Douglas, J., concurring).

36 Lopez v. United States, 373 U.S. 427 (1963).

37 *Id.* at 466 (Brennan, J., dissenting).

38 Olmstead v. United States, 277 U.S. 438, 475–76 (1928) (Brandeis, J., dissenting).

People need a degree of control over the government in order to feel free. Freedom is not just the absence of restraints; it is a mental state, a felt reality in both structure and sentiment. Like insurance, protections against surveillance provide a sense of security.

Surveillance gives significant power to the watchers. Part of the harm is not simply in being watched, but in the lack of control that people have over the watchers. Surveillance creates the need to worry about the judgment of the watchers. Will our e-mail be misunderstood? Will our confidential information be revealed? What will be done with the information gleaned from surveillance?

Thus, the goal of surveillance law is to ameliorate these problems while at the same time allowing for effective law enforcement. This can be accomplished by providing for the oversight of government surveillance, accountability for abuses and errors, and limits against generalized forms of surveillance.

B. The Story of Surveillance Law

Electronic surveillance emerged as early as the telegraph. After the telegraph was invented in 1844,[39] technology to tap into its communications was developed shortly thereafter. Priscilla Regan notes: "During the Civil War, the Union and Confederate armies tapped each other's telegraph communications to ascertain battle plans and troop movements. Rival press organizations tapped each other's wire communications in order to be the first to report major news items."[40]

Following the Civil War, Congress attempted to obtain telegraph messages maintained by Western Union for various investigations.[41] This raised quite an outcry.[42] Editorials decried the tapping as "an outrage upon the liberties of the citizen";[43] as a practice that "outrages every man's sense of his right to the secrets of his own correspondence";[44] and as "hateful and repulsive to the people in general."[45] In 1880, Congress considered a bill to protect the privacy of telegrams.[46] Although the bill was abandoned, state law responded. Several courts quashed subpoenas for telegrams.[47] As the

---

39 *See* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 123 (2000).

40 PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 111 (1995).

41 *See* DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 30 (1978); ELLIS SMITH, *supra* note 39, at 69.

42 *See* SEIPP, *supra* note 41, at 31.

43 *Id.*

44 *Id.* at 35.

45 *Id.* at 36.

46 *Id.* at 40.

47 *Id.*

Missouri Supreme Court stated in quashing a grand jury subpoena for telegrams: "Such an inquisition, if tolerated, would destroy the usefulness of this most important and valuable mode of communication."[48] More than half of the states passed laws to prohibit the disclosure of telegraph messages by telegraph company employees.[49]

In the twentieth century, the changing nature of the type of criminal activity being prosecuted, the rise of organized police forces, and the development of more sophisticated surveillance technologies led to a profound increase in law enforcement surveillance. The rise of the mafia and large-scale crime organizations required law enforcement to find means to learn about what crimes these groups were planning. The government began to increase prosecution of certain consensual crimes, such as gambling, the use of alcohol during Prohibition, and the trafficking of drugs. Unlike robberies or assaults, which are often reported to the police, these crimes occurred through transactions in an underground market. Infiltration into this underworld (undercover work), as well as surveillance, became key tools to detect these crimes.

In earlier times, policing consisted of amateurs who merely patrolled rather than investigated.[50] But by the twentieth century, police forces transformed into organized units of professionals.[51] The FBI emerged in the early years of the twentieth century, the brainchild of Attorney General Charles Bonaparte. In 1907, Bonaparte asked Congress to authorize the creation of a detective force in the Department of Justice ("DOJ").[52] At the time, the DOJ was borrowing investigators from the Secret Service, and Bonaparte wanted a small permanent set of investigators to work for him in the DOJ.[53] But he was rebuffed by the House Appropriations Committee.[54] Bonaparte again asked Congress in 1908, and members of Congress were very skeptical of the idea.[55] They worried about the detective force becoming a secret police, prying into the privacy of citizens, growing into something larger and more unwieldy, and lacking adequate control.[56] One congressman declared:

> In my reading of history I recall no instance where a government perished because of the absence of a secret-service force, but many there are that perished as a result of the spy system. If

---

48 *Ex parte* Brown, 72 Mo. 83, 95 (1880).

49 SEIPP, *supra* note 41, at 65.

50 Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1105–06 (2002).

51 *Id.* at 1105; Stuntz, *supra* note 29, at 435.

52 CURT GENTRY, J. EDGAR HOOVER: THE MAN AND THE SECRETS 111 (1991).

53 *Id.*

54 *Id.*

55 *Id.* at 111–12.

56 *Id.* at 112.

> Anglo-Saxon civilization stands for anything, it is for a government where the humblest citizen is safeguarded against the secret activities of the executive of the government.[57]

Congress rejected Bonaparte's request and even passed a law prohibiting the DOJ from borrowing Secret Service agents.[58] Before this law became effective, however, Bonaparte used the DOJ's discretionary budget to hire Secret Service agents, and he brought in people from other parts of the DOJ to form a new subdivision.[59] In July 1908, President Theodore Roosevelt issued an executive order authorizing the subdivision, which became known as the Bureau of Investigation.[60] J. Edgar Hoover soon took the helm of the Bureau, which was renamed the Federal Bureau of Investigation ("FBI") in 1935.[61] The FBI grew dramatically throughout the rest of the century. When Franklin Roosevelt became President in 1933, the FBI had 353 agents and 422 support staff.[62] When Roosevelt died in 1945, there were 4,380 agents and 7,422 support staff.[63]

At the time the FBI was being born, the debate over surveillance of communications was entering a new era. Similar to the story of telegraph tapping,[64] telephone wiretapping technology arose soon after the invention of the telephone in 1876.[65] And similar to what occurred earlier with the telegraph, the privacy of phone communications became a public concern. State legislatures responded by passing laws criminalizing wiretapping.[66] For example, in 1905, California expanded its 1862 law against intercepting telegraph messages to include telephone calls.[67]

In 1928, in *Olmstead v. United States*,[68] the Supreme Court held that the Fourth Amendment did not apply to wiretapping.[69] The Court reasoned: "There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[70] Justice Brandeis penned a powerful dissent, arguing that new technologies required rethinking old-

---

57 *Id*. at 112–13 (quoting Rep. J. Swagar Sherley, D-Ky.).

58 *Id.* at 111, 113.

59 GENTRY, *supra* note 52, at 113; RICHARD GID POWERS, SECRECY AND POWER: THE LIFE OF J. EDGAR HOOVER 133 (1987).

60 GENTRY, *supra* note 52, at 113.

61 *Id.*

62 RONALD KESSLER, THE BUREAU: THE SECRET HISTORY OF THE FBI 57 (2002).

63 *Id.*

64 *See supra* notes 39–40 and accompanying text.

65 REGAN, *supra* note 40, at 110–11. Telephone wiretapping began in the 1890s. SAMUEL DASH ET AL., THE EAVESDROPPERS 25 (1959).

66 ELLIS SMITH, *supra* note 39, at 157.

67 *Id.*

68 Olmstead v. United States, 277 U.S. 438 (1928).

69 *Id.* at 469.

70 *Id*. at 464.

fashioned notions of the Fourth Amendment: "Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[71] A year after *Olmstead*, even J. Edgar Hoover testified that "'while it may not be illegal . . . [wiretapping] is unethical and it is not permitted under the regulations by the Attorney General.'"[72] Hoover declared that "'any employee engaged in wire tapping will be dismissed from the service of the bureau.'"[73]

In 1934, six years after *Olmstead*, Congress passed section 605 of the Federal Communications Act.[74] Under section 605, "no person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communications to any person."[75] Section 605, however, was largely ineffective. It was interpreted only to preclude the introduction of wiretapping evidence in court.[76] The FBI could thus wiretap freely so long as it did not seek to use the evidence at trial. Section 605 also did not apply to the states.

Throughout the middle of the twentieth century, the FBI expanded in size and in the scope of its surveillance activities. World War II and the ensuing Cold War enabled the FBI to fortify its powers.[77] Presidents increasingly gave the FBI new authorization to engage in wiretapping.[78] During World War II, the FBI received a profoundly expanded authority to engage in wiretapping and to investigate national security threats.[79] Hoover, who once had promised to fire any FBI employee who wiretapped,[80] lavishly ordered wiretapping of hundreds of people, including

---

[71] *Id*. at 473 (Brandeis, J., dissenting).

[72] Louis Fisher, *Congress and the Fourth Amendment*, 21 GA. L. REV. 107, 127 (1986) (quoting *Department of Justice Appropriations Bill for 1931: Hearings Before the House Subcomm. on Appropriations*, 71st Cong., 2d Sess. 63 (1930) (testimony of J. Edgar Hoover, Director of the Bureau of Investigation)).

[73] *Id.*

[74] Communications Act of 1934, ch. 652, 48 Stat. 1064 (current version at 47 U.S.C. § 605 (2000)).

[75] 47 U.S.C. § 605.

[76] *See* WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE 260 (3d ed. 2000).

[77] *See* Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 797–98 (1989).

[78] *See* WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 155–65 (1998); Cinquegrana, *supra* note 77, at 797–98.

[79] *See* DIFFIE & LANDAU, *supra* note 78, at 161–62; William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 26–27 (2000).

[80] Fisher, *supra* note 72, at 127 (citation omitted).

political enemies, dissidents, Supreme Court Justices, professors, celebrities, writers, and others.[81] Among Hoover's files were dossiers on John Steinbeck, Ernest Hemingway, Charlie Chaplin, Marlon Brando, Muhammad Ali, Albert Einstein, and numerous presidents and members of Congress.[82] Justice William Douglas seemed paranoid when he complained for years that the Supreme Court was being bugged and tapped—but he was right.[83] The FBI aggressively investigated political dissenters in a program known as COINTELPRO (Counter Intelligence Program).[84] The program was designed to gather information about political groups viewed as domestic security threats.[85] The data was used to disrupt the lives of the members of these groups, and the FBI's tactics included secretly attempting to convince employers to fire targeted individuals, anonymously informing spouses of affairs to break up marriages, and trying to induce an IRS investigation to deter individuals from attending meetings and events.[86] Much of COINTELPRO's activities were focused on the American Communist Party, but the program extended to other political groups as well, including members of the Civil Rights Movement and opponents of the Vietnam War.[87] Included among these individuals was Martin Luther King, Jr., whom Hoover had under extensive surveillance.[88] The FBI surveillance recordings revealed that King was having extramarital affairs, and the FBI sent copies of the recordings to King and his wife, threatening that if King failed to commit suicide by a certain date, the recordings would be released publicly.[89]

In the late 1960s, the Court and Congress attempted to rein in the growing power of the executive to engage in electronic surveillance. In *Berger v. New York*, the Court struck down portions of New York's wiretapping statute and outlined the constitutional criteria for electronic surveillance.[90] In 1967, the Supreme Court reversed *Olmstead* in *United States v. Katz*, declaring that wiretapping was covered by the Fourth

---

81 KESSLER, *supra* note 62, at 94, 166, 188.

82 *Id.* For more information about Hoover's files on Albert Einstein, see generally FRED JEROME, THE EINSTEIN FILE: J. EDGAR HOOVER'S SECRET WAR AGAINST THE WORLD'S MOST FAMOUS SCIENTIST (2002).

83 GENTRY, *supra* note 52, at 630.

84 POWERS, *supra* note 59, at 339.

85 *See* 2 *Hearings Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the U.S. Senate*, 94th Cong. vol.2, at 10 (1976) [hereinafter *Church Comm. Report*].

86 *See id.*

87 DAVID COLE & JAMES X. DEMPSEY, TERRORISM AND THE CONSTITUTION 6–7 (1999); POWERS, *supra* note 59, at 339, 422–30.

88 GENTRY, *supra* note 52, at 140–42.

89 *Id*. at 126.

90 Berger v. New York, 388 U.S. 41, 44 (1967).

Amendment.[91]

In 1968, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act.[92] Almost everyone had disliked section 605 of the Federal Communications Act.[93] Attorney General Nicholas Katzenback declared it the "worst of all possible solutions."[94] According to Senate Report 1097, section 605 "serves . . . neither the interests of privacy nor of law enforcement."[95] The problem with section 605 was that it permitted private citizens to wiretap but prohibited law enforcement officials from using evidence of electronic surveillance for even the most serious of crimes.[96] Further, the report stated, "[t]he tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques."[97] The report also noted the need to permit law enforcement to engage in electronic surveillance to combat serious and complex crimes performed by "highly organized, structured and formalized groups of criminal cartels."[98] *Berger* and *Katz* were used "as a guide in drafting Title III."[99] Title III extended the reach of electronic surveillance law beyond federal officials to state officials and even to private parties.[100]

Although Title III was an improvement over section 605, it failed to address national security and foreign intelligence surveillance.[101] In *Katz,* a debate in dicta arose over whether regular Fourth Amendment procedures would apply when national security was at stake.[102] In his concurrence, Justice White opined that if the president authorized electronic surveillance for national security reasons, then the Fourth Amendment should not require a warrant.[103] Justices Douglas and Brennan, in their own concurrence, attacked White's claim: "There is, so far as I understand constitutional history, no distinction under the Fourth Amendment between

---

91 United States v. Katz, 389 U.S. 347, 358 (1967).

92 Omnibus Crime Control & Safe Streets Act of 1968, Pub. L. 90-351, § 802, 82 Stat. 212 (current version at 18 U.S.C. §§ 2510–2520 (2000)).

93 JAMES G. CARR & PATRICIA L. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE §2.1, at 2–3 (2003).

94 *Hearings on Criminal Laws and Procedures Before a Subcomm. of the Senate Comm. on the Judiciary*, 89th Cong., 2d Sess. 38 (1966) (statement of Nicholas Katzenbach, Attorney General, United States).

95 S. REP. NO. 90-1097, at 2154 (1968).

96 CARR & BELLIA, *supra* note 93, § 2.1 at 2–3.

97 S. REP. NO. 90-1097, at 2154.

98 *Id.* at 2157.

99 *Id.* at 2163.

100 *See generally* DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW: CASES AND MATERIALS (2003).

101 *See* STEPHEN J. SCHULHOFER, THE ENEMY WITHIN: INTELLIGENCE GATHERING, LAW ENFORCEMENT, AND CIVIL LIBERTIES IN THE WAKE OF SEPTEMBER 11, at 37 (2002).

102 Katz v. United States, 389 U.S. 347, 358 n.23 (1967).

103 *Id.* at 364 (White, J., concurring).

types of crimes. . . . [T]he Fourth Amendment draws no lines between various substantive offenses."[104]

In 1972, the Court concluded in *United States v. United States District Court*[105] that, under the Fourth Amendment, the government needed a warrant to engage in electronic surveillance for domestic criminal investigations.[106] This case is often referred to as the "*Keith* case," named after Judge Damon J. Keith, the federal district judge who originally heard the matter. The Court, however, also stated that "domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.'"[107] The Court reasoned that the "gathering of security intelligence" occurs over a long time period and aims to prevent future crises.[108] Because of these aims, security surveillance "may be less precise than that directed against more conventional types of crime."[109] Accordingly:

> Different standards [for gathering domestic security intelligence] may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.[110]

Beyond the "domestic aspects of national security," the Court explicitly declared it was expressing no opinion about surveillance of "foreign powers or their agents," but it noted that warrantless surveillance under these limited circumstances "may be constitutional."[111]

Spurred by the Watergate scandal, Congress formed a special eleven-member committee in 1975 to investigate surveillance abuses over a nearly forty-year span from 1936 to 1975.[112] The committee was led by Senator Frank Church and was called the Church Committee. Publishing fourteen volumes of reports and supporting documents, the Committee concluded that the government had engaged in numerous abuses of surveillance, often

---

104 *Id.* at 360 (Douglas, J., concurring).

105 United States v. United States District Court, 407 U.S. 297 (1972).

106 *Id.* at 323–24.

107 *Id.* at 322.

108 *Id.*

109 *Id.*

110 *Id.* at 322–23.

111 *Id.* at 321–22 & n.20.

112 DIFFIE & LANDAU, *supra* note 78, at 178. Another committee, chaired by Governor Nelson Rockefeller, was created in 1975 to investigate CIA surveillance in the United States. The committee report found numerous abuses. Banks & Bowman, *supra* note 79, at 32–33.

targeting people solely because of their political beliefs.[113] Specifically, the Committee noted:

> Too many people have been spied upon by too many Government agencies and [too] much information has [been] collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power.[114]

Additionally, the Committee reported, every president from Franklin D. Roosevelt to Richard M. Nixon improperly used government surveillance to obtain information about critics and political opponents.[115] The Committee counseled for a strict separation between domestic and foreign intelligence gathering.[116]

FISA[117] emerged as a response to the Church Committee reports and to the *Keith* case. Congress was concerned over surveillance abuses by the executive branch, a concern inspired by Nixon's abuse of surveillance powers under the guise of national security.[118] As Senate Report 604 declared: "This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused."[119] The purpose of FISA was to erect a "secure framework by which the executive branch could conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights."[120] FISA created a distinct regime regulating electronic surveillance for foreign intelligence purposes.

In 1986, Congress amended Title III of the Omnibus Crime Control

---

[113] In addition to electronic surveillance, the Church Committee reported on United States's involvement in the assassination of foreign and military leaders as well as foreign and military intelligence. For the reports and documents relating to surveillance abuses within the United States, see 1–7 *Church Comm. Report*, *supra* note 85. The Church Committee reports are available online at http://www.aarclibrary.org/publib/church/reports/contents.htm. The Committee also produced a number of additional volumes of reports and documents not cited above. For more background about the Church Committee, see DIFFIE & LANDAU, *supra* note 78, at 178–79; SCHULHOFER, *supra* note 101, at 60–61; Cinquegrana, *supra* note 77, at 806–08.

[114] 2 *Church Comm. Report*, *supra* note 85, at 5.

[115] *Id.* at 9–10.

[116] DIFFIE & LANDAU, *supra* note 78, at 121.

[117] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1811 (2000)).

[118] Robert A. Dawson, *Shifting the Balance: The D.C. Circuit and the Foreign Intelligence Surveillance Act of 1978*, 61 GEO. WASH. L. REV. 1380, 1386 (1993).

[119] S. REP. NO. 95-604, at 7 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908.

[120] *Id.* at 15, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3916.

and Safe Streets Act by passing the ECPA.[121] Congress passed ECPA out of a concern that new technologies were posing an increasing threat to privacy.[122] House Report 647 noted that "[l]egal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology."[123] Additionally, Senate Report 541 mentioned that threats to privacy in these new communications media "may unnecessarily discourage potential customers from using innovative communications systems."[124] ECPA extended Title III to cover a greater range of forms of communication, such as e-mail.[125] It also extended protection beyond communications in transmission to those stored in computer systems.[126] Subsequently, ECPA was amended a number of times, although these amendments made relatively minor changes to the structure of ECPA.

The most substantial changes came after September 11. In an extremely short time following the September 11 attacks, Congress passed the USA PATRIOT Act of 2001.[127] The USA PATRIOT Act's changes to surveillance law, however, were not directly linked to September 11. Indeed, when Attorney General John Ashcroft asked the DOJ just a few days after September 11 for recommendations on potential changes in surveillance law, "the DOJ had already prepared a comprehensive proposal for updating the Internet surveillance laws."[128] As Orin Kerr observes, many of the changes the DOJ proposed had been introduced in Congress on numerous previous occasions and had failed.[129] The Act was thus actually a DOJ wish list from before September 11.

The Act made numerous changes to ECPA and FISA. Among other things, the Act created more opportunities for delaying notice of search warrants, increased the types of subscriber records that could be obtained from communications service providers, and permitted a nationwide scope for pen register orders and e-mail search warrants.[130] It provided for roving wiretaps under FISA as well as increased sharing of foreign intelligence information between law enforcement entities.[131] The Act made a number of other changes as well, which will be discussed later. Some of these

---

121 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

122 S. REP. NO. 99-541, at 2–3, 5 (1986); H.R. REP. NO. 99-647, at 16–19 (1986).

123 H.R. REP. NO. 99-647, at 18.

124 S. REP. NO. 99-541, at 5.

125 *See* H.R. REP. NO. 99-647, at 16.

126 *Id.*

127 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

128 Kerr, *supra* note 2, at 637.

129 *Id.*

130 *See* SOLOVE & ROTENBERG, *supra* note 100, at 341–44.

131 *See id*., at 343.

changes will sunset on December 31, 2005.[132]

II. Electronic Surveillance Law and Its Problems

The USA PATRIOT Act has been strongly criticized for making surveillance law less protective of privacy. The Act is certainly troubling,[133] but many of its problems are rooted more deeply in the surveillance law that preceded the Act. The USA PATRIOT Act is therefore just the tip of a much larger iceberg. We thus need to shift the focus of the debate from the USA PATRIOT Act to electronic surveillance law more generally. Engaging in this endeavor requires a basic understanding of the structure of surveillance law, which primarily consists of two statutory frameworks: ECPA and FISA. Whereas ECPA regulates surveillance for domestic purposes (the investigation and prevention of crimes), FISA regulates the surveillance of foreign agents within the United States. Since it regulates foreign intelligence gathering, FISA provides a much looser set of protections than ECPA. In this Part, I examine this two-part regime comprised of ECPA and FISA and assess its problems.

A. The Electronic Communications Privacy Act

Before analyzing the problems with ECPA, it is necessary to discuss the basic architecture of the statute. ECPA restructures Title III into three titles. Title I, known as the Wiretap Act, deals with the interception of communications that are in transmission.[134] Title II, known as the Stored Communications Act, covers the accessing of stored electronic communications and records.[135] Title III of ECPA, known as the Pen Register Act, applies to pen registers and trap and trace devices, which record phone numbers or addressing information (such as the "to" and "from" lines on e-mail).[136]

ECPA covers three types of communications: wire, oral, and electronic. A "wire communication" involves "aural transfer[s]," which are communications containing the human voice, that travel through wire at

---

132 USA PATRIOT Act § 224.

133 Orin Kerr argues that "[t]he Patriot Act did not expand law enforcement powers dramatically, as its critics have alleged. In fact, the Patriot Act made mostly minor amendments to the electronic surveillance laws. . . . Several of the most controversial amendments may actually *increase* privacy protections, rather than decrease them." Kerr, *supra* note 2, at 608. Kerr goes on to conclude: "The Patriot Act is hardly perfect, but it is not the Big Brother law that many have portrayed it to be." *Id.* Kerr makes a convincing case that selected portions of the Patriot Act are not problematic, but there are other parts that Kerr does not examine that are quite troubling. I will discuss some of these parts later.

134 18 U.S.C. §§ 2510–2522 (2000).

135 18 U.S.C. §§ 2701–2711 (2000).

136 18 U.S.C. §§ 3121–3127 (2000).

some point during their transmission.[137] Another type of communication is an "oral" one—not to be confused with "aural," although an oral communication by definition must also be "aural." This is a communication "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."[138] This definition seemingly applies to communications intercepted through bugs or other recording devices that do not involve a wire transmission. So if the police attempted to place a bug in one's home to record one's dinnertime conversations, this would be an interception of an oral communication. Finally, there are "electronic communications," which are all non-wire and non-oral communications, i.e., signals, images, and data, that can be transmitted through a wide range of transmission mediums (wire, as well as radio, electromagnetic, photoelectronic, etc.).[139] The prime example of an electronic communication is an e-mail message. Each of these types of communications—wire, oral, and electronic—is protected differently, and sometimes, the same type of communication is protected differently in different parts of the statutory regime.

I will evaluate each part of ECPA—the Wiretap Act, Stored Communications Act, and Pen Register Act—by focusing on three main topics. First, I will discuss the *scope* of each act—the applicability of the law to different forms and techniques of surveillance. Second, I will examine the *standards* required for the government to obtain judicial authorization to engage in surveillance. Third, I will look at the *enforcement* provisions of each act.

1. The Wiretap Act

Title I, the Wiretap Act, governs communications intercepted while in transmission. A classic example is a wiretap of a phone conversation. Suppose that Jack and Jill are talking on the telephone. The government taps into the line and listens in on the conversation. Because this occurs while the communication is coursing through the telephone wires, it is covered by the Wiretap Act.

a. Scope

Although the Wiretap Act is quite protective of privacy, it is also very limited in scope, and it makes distinctions in types of surveillance that are quite puzzling. For example, silent video surveillance is not covered under ECPA.[140] Silent video surveillance is not an "aural transfer" because it

---

137 *See* 18 U.S.C. § 2510(1).

138 *Id.* § 2510(2).

139 *See id.* § 2510(12).

140 *See, e.g.*, United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536, 540 (9th Cir. 1992); United States v. Biasuci, 786 F.2d 504, 508

does not involve a human voice.[141] Such surveillance is not covered as an electronic communication under the Wiretap Act because it is not intercepted in transmission.[142] If, however, the government were to intercept video images as they were being transmitted over the Internet, this would be an interception of an electronic communication under the Wiretap Act.[143] But this is a *communication consisting of video images*, not the video surveillance of a communication.

The omission of video surveillance from the Wiretap Act's scope is problematic since silent video surveillance presents similar (and sometimes even greater) dangers and threats to privacy as audio surveillance. As one court noted:

> Television surveillance is identical *in its indiscriminate character* to wiretapping and bugging. It is even more invasive of privacy, just as a strip search is more invasive than a pat-down search, but it is not more indiscriminate: the microphone is as "dumb" as the television camera; both devices pick up anything within their electronic reach, however irrelevant to the investigation.[144]

As another court observed, "video surveillance can be vastly more intrusive [than audio surveillance], as demonstrated by the surveillance in this case that recorded a person masturbating before the hidden camera."[145]

An easy way around ECPA's requirements is thus to install a silent video camera rather than a bug. So long as the camera doesn't pick up audio, all the police need is a skilled lip reader to decipher the conversations.

Ironically, the generally much less stringent protections of FISA cover video surveillance. The government must submit "a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance."[146] Moreover, the government must certify "that such information cannot reasonably be obtained by normal investigative techniques."[147] Foreign agents therefore receive protection against silent video surveillance whereas United States citizens do not.

Another limitation in the Wiretap Act's scope is its narrow definition of "interception." For the Act to apply, a communication must be

(2d Cir. 1986).

141 *See* 18 U.S.C. § 2510(18).

142 *See id.* § 2510(1).

143 *See* SOLOVE & ROTENBERG, *supra* note 100, at 333.

144 United States v. Torres, 751 F.2d 875, 885 (7th Cir. 1984).

145 United States v. Mesa-Rincon, 911 F.2d 1433, 1437 (10th Cir. 1990).

146 50 U.S.C. § 1804(a)(6) (2000).

147 *Id.* § 1804(a)(7).

intercepted while in transit.[148] The government must access it while it is actually in the process of traveling to its destination.[149] For example, suppose Jack calls Jill on the telephone. The FBI listens in on a wiretap. This is clearly covered by the Act. But suppose Jack e-mails Jill a message. The e-mail travels through the phone wires—just like the telephone conversation—although it makes a brief temporary stop at Jill's ISP, where it waits for Jill to download it. The FBI can access it at the ISP, where it is no longer in "flight." It is thus not intercepted and the Wiretap Act does not apply. For example, in *Steve Jackson Games, Inc. v. United States Secret Service*,[150] the Secret Service seized a computer at Steve Jackson Games, Inc., a company that produced role-playing games.[151] The computer was used as an e-mail system for 365 users, and it contained 162 unread e-mail messages.[152] Because the e-mail was temporarily sitting on this computer, it was not intercepted, and the Wiretap Act did not apply.[153]

The Wiretap Act's narrow definition of "interception" thus does not provide much privacy protection for e-mail users. Unlike a telephone conversation, which can only be intercepted while it is actually traveling through wires, an e-mail makes a temporary pit stop at the ISP's server. Even though it is still traveling from the sender to the recipient, it does not fall within the definition of "interception." But this difference seems technical. Phone conversations and e-mail are both very important means of communication today, yet phone conversations receive vastly more protection. E-mail is quickly becoming one of the central modes of communication in the world and is often used in lieu of the telephone. The use of e-mail continues to escalate at a staggering pace. In 2000, there were roughly 505 million e-mail accounts, and the number is expected to reach 1.2 billion by 2005.[154] According to projections, by 2005, over 36 billion e-mails will be sent each day throughout the world.[155] Despite these profound statistics, ECPA treats e-mail like a second-class citizen.

Another problem with the narrow definition of "interception" is demonstrated in *United States v. Scarfo*,[156] where the FBI used a device known as a "Key Logger System," which recorded the defendant's keystrokes on his computer to figure out his password.[157] Scarfo argued

148 18 U.S.C. § 2510 (2000).

149 *Id.*

150 Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994).

151 *Id.* at 458–59.

152 *Id.*

153 *Id.* at 461–62.

154 Cindy M. Rice, *The TCPA: A Justification for the Prohibition of Spam in 2002*, 3 N.C. J.L. & TECH. 375, 376 (2002).

155 *Id.*

156 United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

157 *Id.* at 574.

that the keystroke logger was akin to a wiretap and therefore the Wiretap Act applied.[158] According to the court, however, there was no interception because the key logger did not record keystrokes while Scarfo's modem was operating.[159] Thus, the keystrokes were not intercepted in transit.[160] Indeed, the FBI deliberately programmed the key logger system to stop recording once the modem started transmitting.[161] This seems like an end run around ECPA based on a technicality. For example, suppose a person drafts a letter and then e-mails it to another person. Rather than waiting for the letter to be sent and then intercepting it then, the FBI could simply capture the keystrokes before the letter is sent, thus escaping from the protections of the Wiretap Act.

b. Standards

The Wiretap Act requires the government to meet very high standards in order to obtain authorization to intercept communications. A court order under the Act provides more protection than an ordinary Fourth Amendment search warrant, and Orin Kerr refers to it as a "'super' search warrant."[162] The Wiretap Act only permits certain types of high ranking officials to apply for the warrant.[163] In addition to requiring probable cause, a super warrant requires a specific description of where the communication will be intercepted, the type of communication, and the duration of the interception.[164] The court order must make sure that the interception of nonrelevant communications is minimized and that the surveillance immediately "terminate upon attainment of the authorized objective."[165] In contrast to a Fourth Amendment warrant, which only lasts for a short time, however, a Wiretap Act court order can authorize surveillance for up to thirty days.[166] Moreover, although the standards for authorization are fairly high, they have limited impact because of the Wiretap Act's narrow scope.

c. Enforcement

Generally, enforcement under the Wiretap Act is quite strong. The Wiretap Act provides for high civil penalties—minimum damages of $10,000 per violation.[167] Additionally, wire and oral communications are

158 *Id.* at 581.
159 *Id.* at 581–82.
160 *Id.*
161 *Id.*
162 Kerr, *supra* note 2, at 621.
163 18 U.S.C. § 2516 (2000).
164 *Id.* § 2518.
165 *Id.* § 2518(5).
166 *Id.*
167 *Id.* § 2520(c)(2)(B).

protected with an exclusionary rule,[168] but electronic communications are not.[169] At trial, the result is that a defendant can suppress evidence obtained by the illegal interception of a phone conversation but not an e-mail. Since e-mail has become a central mode of communication, this discrepancy is baseless.

2. The Stored Communications Act

The Stored Communications Act (Title II) regulates communications in "electronic storage."[170] The Stored Communications Act also governs law enforcement access to subscriber records of various communications service providers, such as ISPs.[171] Therefore, if a communication is being transmitted from its origin to a destination, the Wiretap Act applies; if it is stored electronically in a computer, the Stored Communications Act governs. As discussed later, the Stored Communications Act is much less protective than the Wiretap Act.

a. Scope

"Electronic storage" is defined as "any temporary, intermediate storage" that is "incidental" to the communication and "any storage of such communication by an electronic communications service for purpose of backup protection of such communication."[172] This definition significantly limits the scope of the Stored Communications Act. For example, e-mail sitting on the ISP's server waiting to be downloaded is in "electronic storage." After people download and read their messages, however, they often retain copies of them on the ISP's server. For example, I keep many old e-mail messages in my law school e-mail account's inbox. I also keep copies of the messages I send to others in the outbox. Because these messages are now stored indefinitely, according to the DOJ's interpretation (which was drafted by Orin Kerr), the e-mail is no longer in temporary storage and is "simply a remotely stored file."[173] Therefore, under this view, it falls outside of much of the Act's protections.[174] Since many people store their e-mail messages after reading them and the e-mail they send out, this enables the government to access their communications with very minimal limitations.

The Stored Communications Act also regulates the government's

168 *Id.* § 2518 (10)(a).

169 *Id.*

170 *Id.* § 2510(17).

171 *Id.* § 2510(17)(B).

172 *Id.* § 2510(17).

173 COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, U.S. DEP'T OF JUSTICE, MANUAL ON SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § III.B (2001) [hereinafter DOJ MANUAL].

174 *But see* Theofel v. Farey-Jones, 359 F.3d 1066, 1075–76 (9th Cir. 2004).

access to customer records maintained by a service provider. The Stored Communications Act lists certain customer record information that is protected less stringently than stored communications: the customer's name, address, phone numbers, billing records, and types of services the customer utilized.[175] The USA PATRIOT Act expanded the list to include "records of session times and durations," "any temporarily assigned network address," and "any credit card or bank account number" used for payment.[176]

b. Standards

The Stored Communications Act is much less protective than the Wiretap Act. Whereas the Wiretap Act requires a "super warrant,"[177] the Stored Communications Act requires a range of less restrictive orders. Regular warrants are required only to obtain the contents of communications in electronic storage for 180 days or less.[178] If communications are stored over 180 days, the government can access them with an administrative subpoena, a grand jury subpoena, a trial subpoena, or a court order.[179] There is no requirement for probable cause, only "specific and articulable facts showing that there are reasonable grounds" to believe communications are "relevant" to the criminal investigation.[180] For remotely stored files, such as e-mails that have been downloaded and read, the DOJ contends that the government can access them with a mere subpoena,[181] a radically different device than a warrant. Subpoenas do not require probable cause or judicial approval.[182] As William Stuntz notes, federal subpoena power is "akin to a blank check."[183]

The government can obtain customer record information by providing "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and

---

175 18 U.S.C. § 2703(c)(1)(C).

176 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, §210, 115 Stat. 272 (amending 18 U.S.C. § 2703(c)(2)).

177 18 U.S.C. § 2518; *see also* Kerr, *supra* note 2, at 621.

178 18 U.S.C. § 2703(a).

179 *Id.* § 2703(b).

180 *Id.* § 2703(d). If the government does not want to provide prior notice to the subscriber that it is seeking the information, it must obtain a warrant. *Id.* § 2703(b). In a number of circumstances, however, notice can be delayed for up to three months after information has been obtained. *Id.* § 2705.

181 DOJ MANUAL, *supra* note 173, § III.D.1. The government must provide prior or delayed notice to the individual. *See* 18 U.S.C. § 2703(b)(1)(B)(i)–(b)(2).

182 Fisher, *supra* note 72, at 152.

183 William J. Stuntz, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 864 (2001).

material to an ongoing criminal investigation."[184] ISP records are quite important because they contain key information that can identify people using screen names or pseudonyms on the Internet. Thus, a person's First Amendment right to speak anonymously is implicated. As the Court has noted, "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance."[185] Accordingly, when private parties have sought to obtain the identities of anonymous speakers, courts have required heightened standards for subpoenas.[186] Unfortunately, the Stored Communications Act fails to acknowledge that ISP records implicate important constitutional rights. It allows the government to obtain records by merely demonstrating relevance to an ongoing criminal investigation. As previously discussed, this standard does not rise to the level of probable cause. The ease of government access to ISP records creates a host of problems that I have examined elsewhere.[187] For the purposes of this discussion, it suffices to say that the Stored Communications Act goes astray in assuming that ISP records are not important enough to deserve greater protection.

c. Enforcement

The Stored Communications Act is enforced with much less stringent penalties than the Wiretap Act. Whereas Wiretap Act violations have minimum damages of $10,000, Stored Communications Act violations carry minimum damages of only $1000.[188] Another major problem with the Stored Communications Act is that it lacks an exclusionary rule. Even if the police violate the Act blatantly, they can still use surveillance evidence obtained from such misconduct against a defendant in a criminal trial. For example, in *United States v. Hambrick*,[189] the police used an obviously invalid subpoena to obtain ISP records about a pseudonymous person.[190] In *United States v. Kennedy*,[191] the court found that a court order to obtain the defendant's ISP records was deficient because the government failed to articulate the "specific and articulable facts" required to justify the order.[192] Nevertheless, the evidence was admitted in the trial because the Stored Communications Act has no exclusionary rule.[193]

184 18 U.S.C. § 2703(d).

185 Talley v. California, 362 U.S. 60, 65 (1960).

186 *See, e.g.*, Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001); Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

187 *See generally* Solove, *supra* note 50.

188 18 U.S.C. § 2701(b).

189 United States v. Hambrick, 55 F. Supp. 2d 504 (W.D. Va. 1999).

190 *Id.* at 505–06.

191 United States v. Kennedy, 81 F.Supp. 2d 1103 (D. Kan. 2000).

192 *Id.* at 1109–10.

193 *Id.* at 1106; *Hambrick*, 55 F. Supp. 2d at 510.

Orin Kerr contends that the lack of an exclusionary rule is quite problematic because the exclusionary rule is a very effective enforcement device, and without it, "criminal defendants have little incentive to raise challenges to the government's Internet surveillance practices."[194] Kerr notes that when defendants complain about a Stored Communications Act violation, "the courts generally reject [the defendant's complaint] without reaching the merits on the ground that no suppression remedy exists."[195] Due to the lack of an exclusionary rule, violations of the Stored Communications Act do not receive adequate attention in the courts.

3. The Pen Register Act

The Pen Register Act (Title III of ECPA) regulates the government's use of pen registers and trap and trace devices. In *Smith v. Maryland*,[196] the Court held that pen registers are not protected by the Fourth Amendment.[197] A pen register is a device that records the numbers of one's outgoing phone calls.[198] It produces information akin to that on a phone bill—a list of all the numbers a person called, and the date, time, and duration of each call.[199] A trap and trace device records the numbers of one's incoming phone calls.[200] In *Smith*, the Court reasoned that a person has no reasonable expectation of privacy in this information because the telephone company has access to it.[201] Further, the Court noted, "a pen register differs significantly from the listening device employed in *Katz,* for pen registers do not acquire the contents of communications."[202] Therefore, pen registers and trap and trace devices receive no Fourth Amendment protection at all.[203]

The Pen Register Act provides some protection of privacy, although, as I discuss below, the protection is very weak. Under the Act, the government must obtain a court order to use a pen register or trap and trace device.[204]

a. Scope

ECPA largely tracks the distinction made by the Court in *Smith v.*

194 Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 824 (2003).

195 *Id.*

196 Smith v. Maryland, 442 U.S. 735 (1979).

197 *Id.* at 745–46.

198 18 U.S.C. § 3127(3) (2000); *Smith*, 442 U.S. at 736 n.1.

199 *See Smith*, 442 U.S. at 736 n.1.

200 18 U.S.C. § 3127(4).

201 *Smith*, 442 U.S. at 742–43.

202 *Id.* at 741.

203 *Id.* at 745–46.

204 18 U.S.C. § 3121(a).

Maryland, between what Kerr calls "envelope" and "content" information.[205] Analogizing to postal mail, Kerr states that "the content information is the letter itself, stored safely inside its envelope. The envelope information is the information derived from the outside of the envelope, including the mailing and return addresses, the stamp and postmark, and the size and weight of the envelope when sealed."[206] Kerr notes that Congress "has shown little interest in protecting mere envelope information" but has "regulated prospective content information very strictly."[207] Accordingly, only content is regulated under the Wiretap Act and Stored Communications Act. Envelope information is governed by the Pen Register Act's less stringent protections.

This distinction works fine for mail, but it is dubious even in *Smith* with pen registers. As Justice Stewart observed in dissent: "The numbers dialed from a private telephone—although certainly more prosaic than the conversation itself—are not without 'content.'. . . [These numbers] easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[208] As Justice Marshall stated in his dissent:

> Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts. Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society.[209]

As Kerr observes, pen register information can reveal a lot.[210] A lengthy call will suggest that "the two people on opposite ends of the line knew each other, or at least had something substantial to discuss."[211] It reveals "activity from within the suspects' homes that tells the police where they were, at what time, and how long they spoke."[212]

The USA PATRIOT Act expanded the definition of pen registers and trap and trace devices to apply to addressing information on e-mails (e-mail headers) and to Internet Protocol ("IP") addresses.[213] Previously, pen

---

205 Kerr, *supra* note 2, at 611–16.

206 *Id.* at 611.

207 *Id.* at 630.

208 *Smith*, 442 U.S. at 748 (Stewart, J., dissenting).

209 *Id.* at 751 (Marshall, J., dissenting).

210 Kerr, *supra* note 2, at 643.

211 *See id.*

212 *Id.*

213 *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, §216, 115 Stat. 272, 288-290 (amending 18 U.S.C. § 3127(3)–(4) (2000)).

registers were defined as devices that recorded "the numbers dialed . . . on the telephone line."[214] Now, the definition extends to all "dialing, routing, addressing, or signaling information" beyond telephone lines to numerous forms of transmission.[215] The effect of this change is that e-mail headers (the addressing information on e-mail messages), IP addresses, and Uniform Resource Locators ("URLs") fall under this definition.

When applied to IP addresses and URLs, the envelope/content distinction becomes even more fuzzy. An IP address is a unique number that is assigned to each computer connected to the Internet. Each website, therefore, has an IP address. On the surface, a list of IP addresses is simply a list of numbers; but it is actually much more. With a complete listing of IP addresses, the government can learn quite a lot about a person because it can trace how that person surfs the Internet. The government can learn the names of stores at which a person shops, the political organizations a person finds interesting, a person's sexual fetishes and fantasies, her health concerns, and so on.

Perhaps even more revealing are URLs. A URL is a pointer—it points to the location of particular information on the Internet. In other words, it indicates where something is located. When we cite to something on the Web, we are citing to its URL. For example, the following is the URL to Orin Kerr's webpage: http://www.law.gwu.edu/faculty/profile.asp?ID=3568.

One can visit Kerr's webpage by typing the above URL into one's web browser and clicking the "Go" button. Therefore, URLs can reveal the specific information that people are viewing on the Web. URLs can also contain search terms. So if one does a search on Google for Orin Kerr, she will be directed to a URL that reads: http://www.google.com/search?hl=en&ie=UTF-8&oe=UTF-8&q=orin+kerr. Note that the URL reveals her search: "orin+kerr." As Kerr notes, "[w]hether URLs that include search terms and other websurfing addresses can contain 'contents' presents a surprisingly difficult question."[216] The question is difficult because the envelope/content distinction is not always clear. In many circumstances, to adapt Marshall McLuhan, the "envelope" *is* the "content."[217] Envelope information can reveal a lot about a person's private activities, sometimes as much (and even more) than can content information. Yet, as discussed below, envelope information receives very little protection in contrast to content information.[218]

---

214 18 U.S.C. § 3127(3) (2000).

215 18 U.S.C. § 3127(3), *amended by* USA PATRIOT Act § 216.

216 Kerr, *supra* note 2, at 645.

217 I am referring to McLuhan's famous phrase, "the medium is the message." MARSHALL MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN 7 (1964).

218 *See infra* Part II.A.3.b.

Kerr, however, argues that envelope information should receive lesser privacy protection because it "is quite rare for noncontent information to yield the equivalent of content information."[219] Kerr contends that the example of Internet search terms in URLs is "misleading," since "Internet search terms very well may be contents."[220] Kerr, however, overlooks the great difficulty in making the envelope/content distinction. Kerr assumes that a compilation of envelope information is generally less revealing than content information. However, a person may care more about protecting the identities of people with whom she communicates than the content of those communications. Indeed, the identities of the people one communicates with implicates freedom of association under the First Amendment. The difficulty is that the distinction between content and envelope information does not correlate well to the distinction between sensitive and innocuous information. Envelope information can be quite sensitive; content information can be quite innocuous. Admittedly, in many cases, people do not care very much about maintaining privacy over the identities of their friends and associates. But it is also true that in many cases, the contents of communications are not very revealing. Many e-mails are short messages which do not reveal any deep secrets, and even Kerr would agree that this should not lessen their protection under the law. This is because content information has the potential to be quite sensitive—but this is also the case with envelope information.

b. Standards

The Pen Register Act does not provide much in the way of protection for envelope information. The standard to obtain a pen register order is remarkably low. All the government needs to do is certify that "the information likely to be obtained by such installation and use is relevant to an ongoing investigation."[221] Courts do not even review the evidence to back up the government's claim. The court must take the government's word without question. One court has even called the judicial role "ministerial in nature."[222] Orders can last up to 60 days.[223]

Moreover, there are no particularization or minimization requirements.[224] The Act does not specify the nature of the investigation.[225]

---

219 **Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. __, manuscript 49 n.86 (2004).**

220 ***Id.* at manuscript 50 n.86.**

221 18 U.S.C. § 3123(a) (2000).

222 United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995); *see also* DOJ MANUAL, *supra* note 173, § IV.B.

223 18 U.S.C. § 3123(c).

224 *See id.* § 3123(b).

225 *See id.* § 3122.

The investigation could be a large scale dragnet or COINTELPRO, but it does not matter. Furthermore, the use of the pen register must only be "relevant" to an investigation.[226] It is hard to imagine how the government could fail to make this showing regardless of how illegitimate its desired use of the pen register might be. In fact, Kerr agrees that the pen register provision is not protective enough and argues for a "higher threshold to obtain the court order" and "judicial review of the government's application."[227] Kerr also notes, however, that because the Pen Register Act provides protection where the Fourth Amendment provides none, it is "primarily a privacy law."[228] Title II is thus actually increasing the protection, because without Title II, these records could be entirely unprotected. This is certainly true, but giving limited and ineffective protection is not necessarily improving the situation in a meaningful way. Instead, it assigns a legislative stamp of legitimacy on the government's obtaining such information. It also gives an illusory judicial stamp of legitimacy by providing for court orders without even minimal judicial supervisory power.

c. Enforcement

As with the Stored Communications Act, the Pen Register Act does not contain an exclusionary rule. Thus, like the Stored Communications Act, the Pen Register Act does not provide recourse to defendants on whom the government has illegally collected information.

B. The Foreign Intelligence Surveillance Act

FISA creates a different regime for surveillance to obtain "foreign intelligence" information than the ECPA regime that governs regular government surveillance.[229] The regime created by FISA is designed primarily for intelligence gathering agencies to regulate how they gain general intelligence about foreign powers within the borders of the United States. FISA is very permissive; it provides for expansive surveillance powers with little judicial supervision. FISA permits electronic surveillance and covert searches pursuant to court orders, which are reviewed by a special court of eleven federal district court judges known as the Foreign Intelligence Surveillance Court ("FISC").[230] The court meets in secret,

---

[226] *Id.* § 3122(b)(2).

[227] Kerr, *supra* note 2, at 639. Kerr suggests "specific and articulable facts" as the threshold, but this is only one step above the existing standard. *Id.* In contrast, I believe that a warrant should be required.

[228] *Id.* at 638.

[229] **For a more thorough background about the FISA, see Peter P. Swire, *The System of Foreign Intelligence Surveillance*, 72 GEO. WASH. L. REV. ___ (2004).**

[230] Originally, there were seven judges on the court, but the USA PATRIOT Act raised the number to eleven. *See* Uniting and Strengthening America by Providing Appropriate

with the government presenting applications for orders *ex parte*.[231] If the government receives an adverse decision, it can appeal to a three-judge panel.[232]

FISA's protections against surveillance are much looser than those of the ECPA. Under the ECPA and the Fourth Amendment, surveillance is only authorized if there is a showing of probable cause that the surveillance will uncover evidence of criminal activity; under FISA, however, orders are granted if there is probable cause to believe that the monitored party is a "foreign power" or "an agent of a foreign power."[233] Unlike the ECPA, FISA surveillance is therefore not tied to any required showing of a connection to a criminal investigation. FISA does not have this safeguard since it is about gathering general intelligence about other countries and their activities within the United States. FISA orders can last for ninety days[234] as opposed to thirty days for an ECPA order.[235]

The problem with FISA is its secrecy. Of course, monitoring foreign agents on United States soil is difficult without secrecy. But as William Banks and M.E. Bowman observe, "[t]he secrecy that attends FISC proceedings, and the limitations imposed on judicial review of FISA surveillance, may insulate unconstitutional surveillance from any effective sanction."[236] Under FISA, the entire proceedings are held *ex parte*, with nobody permitted to argue the opposing side.[237] Only the government has the opportunity to appeal.[238] The government thus gets two bites at the apple, and the courts only hear the government's side.

This procedure is problematic because there is little to ensure against abuses of power. Compounding this problem is the fact that FISA intelligence can be used in domestic criminal trials.[239] Ordinarily, in a domestic criminal trial, surveillance evidence must be obtained through the procedures of ECPA. But if information is obtained under the less stringent FISA provisions, it can still be used for the prosecution of domestic crimes.

Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 208, 115 Stat. 272, 283 (codified at 50 U.S.C. § 1803(a) (2000)). For more details about the workings of the FISC, see generally Benjamin Wittes, *Inside America's Most Secretive Court*, 143 N.J. L.J. 777 (1996).

231 50 U.S.C. § 1093(a) (2000).

232 *Id.* § 1803(b).

233 *Id.* § 1805(a).

234 *Id.* § 1805(e).

235 18 U.S.C. § 2518(5).

236 Banks & Bowman, *supra* note 79, at 87; *see also* Nola K. Breglio, Note, *Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 Yale L.J. 179, 188 (2003).

237 50 U.S.C. § 1805(a).

238 *See* 18 U.S.C. § 1803(b).

239 *See* SOLOVE & ROTENBERG, *supra* note 100, (manuscript at 341).

Because FISA surveillance power is much broader and more loosely regulated than the ECPA, what prevents the government from using it in lieu of ECPA to prosecute regular crimes? The bulwark against such uses is FISA's limited applicability, for FISA applies only when the government aims to gather foreign intelligence, not when the government is investigating a domestic crime.

The USA PATRIOT Act, however, expanded FISA's applicability. Previously, FISA applied only when "the purpose" of the investigation was to gather foreign intelligence; the USA PATRIOT Act enlarged FISA's scope to apply when foreign intelligence gathering was "a significant purpose" of the investigation.[240] This seemingly subtle change has potentially dramatic ramifications. By changing the language from "*the* purpose" to "*a significant* purpose," foreign intelligence gathering no longer needs to be the primary purpose of the surveillance.[241] The government can now rely on loose FISA protections even when foreign intelligence gathering is only one of many goals.

In light of this change, Ashcroft altered the minimization procedures of FISA. FISA requires that when conducting foreign intelligence gathering, the government must implement procedures to minimize the gathering of information about United States citizens.[242] These procedures prevent the broad powers of FISA from being used for ordinary domestic criminal investigations. In one type of minimization procedure, investigators establish an "information screening wall," in which officials not involved in the criminal investigation review FISA surveillance and pass along only information that will be relevant to the criminal investigation. In 2002, Ashcroft revised the minimization procedures, virtually eliminating the screening walls. The FISC reviewed these procedures and rejected them.[243] According to the court, the "2002 procedures appear to be designed to amend the law and substitute the FISA for Title III electronic surveillance."[244] But the three-judge FISA review court reversed.[245] In the first case ever appealed from the FISC, the review court declared that by changing FISA by using the words "a significant purpose," the USA PATRIOT Act "eliminated any justification for the FISC to balance the relative weight the government places on criminal prosecution as compared

---

240 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 204, 115 Stat. 272 (codified at 50 U.S.C. § 1804(a)(7)(B) (2000)).

241 *Id.* (emphasis added).

242 50 U.S.C. § 1801(h)(1) (2000).

243 *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 625 (Foreign Intell. Surv. Ct. 2002).

244 *Id.* at 623.

245 *In re* Sealed Case, 310 F.3d 717, 720 (Foreign Intell. Surv. Ct. 2002).

to other counterintelligence responses."[246] Therefore, if the government "articulates a broader objective than criminal prosecution—such as stopping an ongoing conspiracy—and includes other potential non-prosecutorial responses, the government meets the statutory test."[247] Only if the "government's sole objective [is] merely to gain evidence of past criminal conduct . . . the application should be denied."[248]

This ruling underscores the problematic nature of the USA PATRIOT Act's amendments to FISA. Government investigations can have a large scope and multiple purposes. Especially in cases involving terrorism, the line between foreign intelligence gathering and domestic law enforcement is often blurred. Since FISA surveillance information can be used in domestic criminal trials, FISA increasingly can become a tool for domestic law enforcement and an end run around the protections of ECPA.[249] Expanding the scope of FISA makes it more likely that government will use the FISA regime to conduct widespread surveillance with very scant legal protections.

C. The Overarching Problems

The problems discussed above consist of gaps, lapses in protection, inadequate standards for obtaining authorization to engage in surveillance, and weak enforcement devices. Some contend that electronic surveillance law will work quite effectively if its glitches are repaired. Orin Kerr, for example, gives the Stored Communications Act a grade of "B" and suggests a few modifications to the statute.[250] While some problems with could be patched, this would merely be a temporary fix because electronic surveillance law has some larger, more overarching difficulties. There are three general problems that should be addressed in order to reach a more long-lasting and far-reaching solution: (1) surveillance law is overly complex and confusing; (2) it fails to quickly respond and adapt to new technology; and (3) it fails to provide sufficient oversight of the executive branch from both the judicial and legislative branches.

---

246 *Id*. at 735.

247 *Id*.

248 *Id*.

249 The USA PATRIOT Act's expansion of FISA brings into question Kerr's assertion that the Act is not much of a Big Brother law. Kerr, *supra* note 2, at 608. Kerr focuses on only a few specific parts of the USA PATRIOT Act that are not as problematic as some critics contend; the fact that some provisions are nonproblematic cannot counterbalance the rather dangerous change in FISA—indeed, Kerr even concedes in a footnote that "some provisions of the Patriot Act may prove to have serious negative consequences for privacy and civil liberties." *Id.* at 625 n.75. Kerr mentions the FISA changes as "particularly notable in this regard." *Id.* Unfortunately, these provisions are notable enough to refute Kerr's general conclusion that the Patriot Act is relatively benign.

250 **See Orin S. Kerr, *A User's Guide to the Stored Communications Act—And a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. ___, manuscript 85 (2004).**

1. Rocket Science

A central problem with surveillance law is its profound complexity. When reprinted in Marc Rotenberg's *Privacy Law Sourcebook*, in a normal font and page size, the ECPA weighs in at fifty-seven pages.[251] The FISA extends for more than forty pages.[252] There are a myriad of different terms with complicated definitions. The statute zigzags with dozens of cross-references. As cataloged by Orin Kerr, it contains at least seven different legal threshold requirements for government surveillance, including subpoenas, different types of court orders, and different kinds of warrants.[253]

ECPA also provides different protections depending upon how the government accesses a particular communication. The Wiretap Act covers communications intercepted in transmission. The Stored Communications Act provides different protection for communications accessed in computer storage. Communications are also protected differently depending upon how long they are stored. Accessing the customer records of a communications service presents another set of rules. Yet another group of rules governs the accessing of routing information about a communication. And so on.

Kerr, who can probably recite the ECPA by memory, and perhaps even in verse, admits that it is "surprisingly difficult to understand."[254] Kerr notes that "courts, legislators, and even legal scholars have had a very hard time understanding the method behind the madness of the [Stored Communications Act of ECPA]."[255] He states that the "law of electronic surveillance is famously complex, if not entirely impenetrable."[256] In numerous articles, Kerr has elucidated the complexities of the law, giving us countless charts and tables. But alas, all the exegesis Kerr can produce will only help us so much. The intricacy of electronic surveillance law is remarkable because it is supposed to apply not just to the FBI, but to state and local police—and even to private citizens. Given its complexity, however, it is unfair to expect these varying groups to comprehend what they can and cannot do. Indeed, even courts have struggled with understanding the statute. Courts have described surveillance law as caught up in a "fog,"[257] "convoluted,"[258] "fraught with trip wires,"[259] and

---

251 MARC ROTENBERG, PRIVACY LAW SOURCEBOOK 162–219 (2002).

252 *Id.* at 88–128.

253 *See* Kerr, *supra* note 2, at 620–21.

254 **Kerr, *supra* note 250, at manuscript 1.**

255 ***Id.* at manuscript 2.**

256 Kerr, *supra* note 194, at 820.

257 Briggs v. Am. Air Filter, 630 F.2d 414, 415 (5th Cir. 1980).

258 United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998).

259 Forsyth v. Barr, 19 F.3d 1527, 1543 (5th Cir. 1994).

"confusing and uncertain."[260] If one is not willing to study ECPA like a biblical scholar studies the Bible, there is little hope of figuring out ECPA.

2. Difficulty in Adapting to New Technology

Electronic surveillance law has not kept pace with the staggering growth of technology. As discussed earlier, the law currently makes antiquated distinctions that often do not protect what is most important. Electronic surveillance law has lagged behind technological developments and has not been responsive to new surveillance technologies.

Despite the development of the Internet, e-mail, and the dizzying array of other twentieth century technologies, there have only been five major attempts at shaping electronic surveillance law—in 1934 with section 605 of the Federal Communications Act,[261] in 1968 with Title III of the Omnibus Crime Control and Safe Streets Act,[262] in 1978 with FISA,[263] in 1986 with ECPA,[264] and in 2001 with the USA PATRIOT Act.[265] While ECPA has been amended between 1986 and 2001, Kerr notes that these "subsequent changes have merely nibbled around the edges of the law."[266] Thus, major revisions to the law occur in fifteen to forty year intervals. Even with foresight, the law is bound to be lagging behind technological developments, especially given the profound specificity and detail of the current statutory regime.

The most notable problem in this regard is the law's failure to keep pace with the breathtaking development of the Internet. In 1989, less than 90,000 computers were connected to the Internet.[267] The number increased to one million by 1993 and to over nine million by 1996.[268] According to projections, there will be over 720 million Internet users by 2005.[269]

---

260 Konop v. Hawaiian Airlines, 302 F.3d 868, 874 (9th Cir. 2002).

261 Communications Act of 1934, ch. 652, 48 Stat. 1064 (current version at 47 U.S.C. § 605 (2000)).

262 Omnibus Crime Control & Safe Streets Act of 1968, Pub. L. 90-351, § 802, 82 Stat. 212 (current version at 18 U.S.C. §§ 2510–2520 (2000)).

263 Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1811 (2000)).

264 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

265 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

266 Kerr, *supra* note 194, at 814.

267 ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Pa. 1996)

268 *Id.*; *see also* Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 930 (2001).

269 *See* Louis U. Gasparini, *The Internet and Personal Jurisdiction: Traditional Jurisprudence for the Twenty-First Century Under the New York CPLR*, 12 ALB. L.J. SCI. & TECH. 191, 194 (2001).

Despite these dramatic changes since the passage of ECPA in 1986, Congress has failed to engage in a major revision of the law. Under this state of affairs, law enforcement cleverly employs new technologies to try to avoid triggering ECPA.[270] Often, these technologies are quite invasive, but the debate seems to turn on technicalities—whether the surveillance fits into ECPA's framework. This invites a technological rat race, in which law enforcement uses new technologies designed to fit within ECPA's less stringent provisions or to fall entirely outside of ECPA's scope.

Moreover, new surveillance technologies are often used before Congress has had a chance to study them, as was the case with Carnivore. In 2000, the *Wall Street Journal* reported that since 1999, the FBI had been using Carnivore, a device installed on ISP servers to intercept e-mail and instant messaging information.[271] The FBI contends that Carnivore is akin to a pen register, but critics charge that it actually has some features that resemble wiretaps.[272] Regardless of who is right on this issue, an important concern has been neglected—the FBI had been using this new device before it had been fully studied and debated.

In another example, the Key Logger System, as examined in *United States v. Scarfo*,[273] was used before being critically examined. The Key Logger System was a device the FBI developed that could be secretly installed into one's computer to log all of a person's keystrokes.[274] News reports disclosed that the FBI had also developed a second keystroke logging device called "Magic Lantern" that could be sent surreptitiously into a person's computer like a computer virus.[275] Even though Carnivore, the Key Logger System, and Magic Lantern were developed with electronic surveillance law in mind, this is not enough. Just because these devices may fit within the law does not mean that they do not pose new dangers. Even if such devices fit within the law technically, it is not clear that they correspond with the law's spirit. Lost amid the labyrinthian task of applying ECPA's complex provisions is the question of whether new technologies contravene the appropriate balance between effective law enforcement and privacy.

Currently, the focus is on following the dictates of a law developed before the rise of the Internet and e-mail rather than ensuring that the law responds to advancements in technology and provides effective law enforcement tools without stifling individual privacy. Although Congress has updated ECPA on numerous occasions, it has done so in relatively

---

270 *See supra* notes 157–161.

271 Neil King, Jr. & Ted Bridis, *FBI's Wiretaps to Scan E-Mail Spark Concern*, WALL ST. J., July 11, 2000, at A3.

272 *Id.*

273 United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

274 *Id.* at 574.

275 Bridis, *supra* note 8.

minor ways and has failed to address many difficult questions.

Moreover, the FBI has been developing and using new surveillance technologies without discussing them publicly. As one FBI spokesperson said: "It's completely inappropriate [to discuss new surveillance technologies]. Why would we? That would defeat the whole purpose of surveillance."[276] But as Raymond Ku aptly observes, the public should play a role in determining the scope of the executive branch's power.[277] Unfortunately, Ku notes, the use of surveillance technology is often "left entirely to the discretion of law enforcement."[278] In a self-governing democracy, it is hard to justify the secret deployment and use of surveillance technology on United States citizens without affording adequate public discussion about the costs and benefits of these new technologies. Electronic surveillance law does not adequately ensure for such discussion by the people directly or through their representatives in Congress.

3. Inadequate Judicial and Legislative Oversight

Under many parts of electronic surveillance law, there is insufficient legislative and judicial oversight. Congress loosely engages in oversight of law enforcement surveillance, only occasionally becoming directly involved. For example, when Congress learned about Carnivore, it held hearings to discuss the pros and cons of the device.[279] Another example is the Department of Defense's Total Information Awareness ("TIA") program, run by John Poindexter, which, in 2002, aimed to gather extensive information about American citizens for use in profiling for terrorists.[280] The media strongly criticized the program. William Safire wrote a vociferous editorial in the *New York Times* charging that Poindexter "is determined to break down the wall between commercial snooping and secret government intrusion. . . . [H]e has been given a $200 million budget to create computer dossiers on 300 million Americans."[281] In January 2003, the Senate added an amendment to a spending bill to deny funding for TIA until the Department submitted a report about the program for Congress to study.[282] Subsequently, the Senate prohibited funding for the program in another bill.[283] Only in cases that receive significant media

276 Sean Marciniak, *Web Privacy Services Complicate Feds' Job*, WALL ST. J., July 3, 2003, at B4.

277 Ku, *supra* note 27, at 1357.

278 *Id.* at 1358.

279 *See* SOLOVE & ROTENBERG, *supra* note 100, at 365.

280 William Safire, *You Are a Suspect*, N.Y. TIMES, Nov. 14, 2002, at A35.

281 *Id.*

282 *See* Cheryl Bolen, *Senate Withholds Data-Mining Funds Until DOD Addresses Privacy, Rights Issues*, Privacy L. Watch (BNA) (Jan. 27, 2003).

283 *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE

attention will Congress become involved. Indeed, although Congress curtailed TIA, similar data-mining endeavors continue to take place because they have received less publicity.[284]

Oversight is also lacking in the reporting system for electronic surveillance. The Wiretap Act requires the government to submit reports about wiretapping activity to the Administrative Office of the United States Courts, which are then transmitted to Congress.[285] No such reports are required under the Stored Communications Act. Moreover, as Charles Kennedy and Peter Swire point out, there is little congressional supervision over state wiretaps.[286] The majority of approved wiretap applications are at the state rather than the federal level, and only half of the states report statistics about their wiretap orders.[287] As a result, Congress often does not learn about new surveillance technologies until after they are deployed.

Many surveillance technologies remain unstudied and without judicial supervision. The FBI is largely under the supervision of the executive branch; but unlike federal agencies, the FBI does not have enabling legislation that establishes its jurisdiction and powers. Therefore, oversight often is turned over to the judicial branch. Unfortunately, electronic surveillance law has very lax standards that often do not give the judiciary sufficient involvement or ability to circumscribe the use of surveillance.

Moreover, electronic surveillance law does not provide for enough oversight of the FBI by the judicial and legislative branches. Unlike other government agencies, such as the Food and Drug Administration and the Securities and Exchange Commission, the FBI does not have enabling legislation that defines its powers and jurisdiction. Instead, many of the FBI's surveillance practices are governed by guidelines established by the Attorney General. In 1976, in response to the growing awareness about the FBI's checkered history of abuses, Attorney General Edward Levi crafted guidelines for the FBI to safeguard against surveillance that could affect First Amendment activities.[288] The Levi Guidelines provided specific limits on the types of investigative activities in which the FBI could engage.[289] FBI agents could use undercover agents, engage in surveillance of political activities, and undertake other invasive investigative techniques

INFORMATION AGE (forthcoming 2004).

284 *See id.*

285 18 U.S.C. § 2519 (2000).

286 Charles H. Kennedy & Peter P. Swire, *State Wiretaps and Electronic Surveillance After September 11*, 54 HASTINGS L.J. 971, 972 (2003).

287 *See id.* at 972–73.

288 *See* Banks & Bowman, *supra* note 79, at 68–69. The Guidelines were called UNITED STATES ATTORNEY GENERAL DOMESTIC SECURITY INVESTIGATION GUIDELINES (1976). *FBI Oversight Hearings Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 95th Cong. 521–60 (1976) [hereinafter *Levi Guidelines*].

289 *See* Banks & Bowman, *supra* note 79, at 68–69.

only if pursuant to "investigation" authorized under the guidelines.[290] Investigations could be initiated when FBI agents had "specific and articulable facts" creating a reason to believe that a person was involved in violent activities in order to conduct an investigation.[291]

Under subsequent presidential administrations, these guidelines have been made less restrictive.[292] In 1983, Attorney General William French Smith revised the Levi Guidelines.[293] The Smith Guidelines lowered the threshold standard for initiating an investigation to "when the facts or circumstances reasonably indicate that two or more persons are engaged in an enterprise for the purpose of furthering political or social goals wholly or in part through activities that involve force or violence and a violation of the criminal laws of the United States."[294] Thus, the threshold changed from the standard of "specific and articulable facts" to the looser standard of "reasonable indication." The Smith Guidelines stated that the "reasonable indication" standard is "substantially lower than probable cause," and that it "does not require specific facts or circumstances indicating a past, current, or impending violation. There must be an objective, factual basis for initiating the investigation; a mere hunch is insufficient."[295] In 1989, Attorney General Dick Thornburgh revised the guidelines again, although the changes were minor.[296]

In 2002, Attorney General John Ashcroft made profound changes to the guidelines. Under both the Levi and Smith Guidelines, the FBI was restricted from monitoring public events and gathering information about people's First Amendment activities unless it was related to an investigation. As discussed above, the Smith Guidelines lowered the standard to initiate an investigation, but there was still a threshold before the FBI could begin to engage in these activities. Ashcroft's revised guidelines allow the FBI to gather information and mine the Internet for data without any requirement that it relate to criminal activity.[297]

---

290 *Levi Guidelines*, *supra* note 288, at 22.

291 *Id.*

292 *See* Banks & Bowman, *supra* note 79, at 69–70; David M. Park, Note, *Re-Examining the Attorney General's Guidelines for FBI Investigations of Domestic Groups*, 39 ARIZ. L. REV. 769, 772–73 (1997); Mitchell S. Rubin, Note, *The FBI and Dissidents: A First Amendment Analysis of Attorney General Smith's 1983 FBI Guidelines on Domestic Security Investigations*, 27 ARIZ. L. REV. 453, 454–55 (1985). For more background about the guidelines, see generally John T. Elliff, *The Attorney General's Guidelines for FBI Investigations*, 69 CORNELL L. REV. 785 (1984).

293 *See* THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND DOMESTIC SECURITY/TERRORISM INVESTIGATIONS (1983).

294 *Id*. § III.B.1.a.

295 *Id.* § II.C.1.

296 *See* THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND DOMESTIC SECURITY/TERRORISM INVESTIGATIONS § II.C.1 (1989), http://www.usdoj.gov/ag/readingroom/generalcrimea.htm (last visited June 5, 2004).

297 *See* THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING

Accordingly, the FBI can collect any "publicly available information" and can "carry out general topical research, including conducting online searches and accessing online sites and forums."[298] These new guidelines apply not just to terrorism, but to federal crimes in general.[299]

Despite the significance of these changes, it is unclear what, if anything, electronic surveillance law has to say about them. These changes took place through executive fiat rather than through legislative discussion or debate. They were not subjected to any checks by the judicial or legislative branches.

By and large the responsibility for keeping government surveillance under control has been delegated to the judiciary. Unfortunately, in many instances, electronic surveillance law provides very weak standards for the judiciary to authorize the surveillance. As discussed above, many provisions in the Stored Communications Act and Pen Register Act fall dramatically short of requiring probable cause, individualized suspicion, or minimization procedures. At times, the judicial role appears to be little more than a rubber stamp.[300] With such a limited role, problems with government surveillance applications can go undetected. The FISA court in its only published opinion of May 17, 2002, noted that the government had admitted it erred in about seventy-five FISA applications, which included making false statements about the nature of the investigation and the sharing of the information.[301] Had the government not admitted the errors, it is unlikely that they would ever have been discovered.

In sum, electronic surveillance law has not established an adequate system of checks and balances on executive power. Congress updates the law from time to time, and occasionally becomes involved, but often, the law is left to drift. Congress needs to play a greater role in monitoring the executive branch, and electronic surveillance law must afford the judiciary with more meaningful oversight.

ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS § VI (2002), http://www.usdoj.gov/olp/generalcrimes2.pdf (last visited June 5, 2004). For more information about data mining and the Ashcroft Guidelines, see Solove, *supra* note 50, at 1096–97.

298 THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS , *supra* note 297, § VI.B.1.

299 SCHULHOFER, *supra* note 101, at 58.

300 As Paul Schwartz notes, electronic surveillance orders are rarely denied. Between 1968 and 1996, judges rejected only twenty-eight applications for surveillance orders out of 20,000. *See* Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 HASTINGS L.J. 751, 793–94 (2003).

301 *See In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 620 (Foreign Intell. Surv. Ct. 2002).

III. Reconstruction

Many of the problems with electronic surveillance law stem from its rigid, Byzantine structure, which makes a myriad of distinctions that quickly become antiquated as technology evolves. The result is that the law ends up with lapses in protection. The degree of protection against certain forms of surveillance often does not turn on how problematic or invasive it is, but on the technicalities of how the surveillance fits into the law's structure. In this Part, I suggest two solutions. First, I propose a broad rule that warrants should be required for most instances of electronic surveillance. Second, I contend that Congress should enact a legislative charter to regulate the FBI. Both solutions I recommend are designed to maintain a better system of checks and balances by giving the judicial and legislative branches a greater role in monitoring and constraining the surveillance activities of the executive branch. As the Church Committee noted, "The overwhelming number of excesses continuing over a prolonged period of time were due in large measure to the fact that the system of checks and balances—created in our Constitution to limit abuse of Governmental power—was seldom applied to the intelligence community."[302] Presidents, Attorneys General, and other high-ranking executive officials have historically provided "broad mandates" and "vague" guidance to intelligence agencies that led to "excessive or improper intelligence activity."[303] Electronic surveillance law thus must be reconstructed to increase legislative and judicial oversight.

A. A Warrant Rule for Electronic Surveillance

We need a surveillance law that is flexible enough to respond to emerging technologies. A better approach would be more sweeping.[304] I contend that for most uses of electronic surveillance, warrants supported by probable cause should be required.[305] This should be the general rule, with specific exceptions authorizing access under less strict standards enumerated in the statute. This approach has the virtue of simplicity. Additionally, all violations should be enforced by an exclusionary rule. Warrants under the law could have a duration of thirty days, as often electronic surveillance must take place over a longer time period than a regular search or seizure.

---

302 2 *Church Comm. Report*, *supra* note 85, at 14.

303 *Id.*

304 I will not discuss the rules to govern surveillance by private parties. These rules may need to be different, as the dangers and harms resulting from private party surveillance are not identical to those of government surveillance.

305 My approach attempts to shift the defaults in a somewhat similar way to how Raymond Ku suggests that Fourth Amendment analysis be altered. He argues that Congress should authorize the government's use of technology by statute for it to be considered reasonable under the Fourth Amendment. Ku, *supra* note 27, at 1374–75.

Critics of warrants might point out that they are cumbersome because probable cause is a higher standard than the existing standards under much of federal surveillance law. Warrants, however, serve several important functions. First, they are an effective way of checking the power of law enforcement entities and of circumscribing the government's investigation power.[306] As discussed in Part II, the central problems of surveillance are that it will chill individual freedom and political activity, and that it can lead to excessive exercises of executive power. James Madison captured the heart of the problem when he wrote:

> But what is government itself but the greatest of all reflections on human nature? If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controuls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: You must first enable the government to controul the governed; and in the next place, oblige it to controul itself.[307]

In other words, Madison's concern can be captured with the famous question: *Who will watch the watchers?* Madison's solution was to separate the power of the government into different branches so they could check each other.[308]

Warrants force law enforcement officials to justify their exercises of power.[309] As Justice Douglas explained for the Court:

> We are not dealing with formalities. The presence of a search warrant serves a high function. Absent some grave emergency, the Fourth Amendment has interposed a magistrate between the citizen and the police. This was done not to shield criminals nor to make the home a safe haven for illegal activities. It was done so that an objective mind might weigh the need to invade that privacy in order to enforce the law.[310]

Second, warrants protect against sweeping dragnet investigations. The Fourth Amendment's requirement that the government demonstrate that there be individualized suspicion protects against the risk that innocent people will be searched. It also prevents the government from engaging in "fishing expeditions."[311] This is why a warrant must describe with

---

306 Solove, *supra* note 50, at 1127.

307 THE FEDERALIST NO. 51, at 349 (James Madison) (Jacob E. Cooke ed., 1961).

308 *Id.*

309 Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 17 (1991).

310 McDonald v. United States, 335 U.S. 451, 455 (1948).

311 Fisher, *supra* note 72, at 115 ("The spirit and letter of the fourth amendment counselled against the belief that Congress intended to authorize a 'fishing expedition' into

"particular[ity] . . . the place to be searched, and the persons or things to be seized."[312]

Third, warrants prevent hindsight bias because they require the courts to balance privacy and law enforcement needs prior to the search.[313] This prevents the results of the search from tainting the court's decision.

Some might claim that warrants are ineffective because judges frequently grant warrant applications. Christopher Slobogin argues, however, that warrants raise the "standard of care" of law enforcement officials, forcing them to "document their requests for authorization."[314] Warrants thus force law enforcement officials to be certain that a search is really necessary. The high rate of granting warrants may be a reflection of warrants doing their job efficiently by having law enforcement officials avoid making overreaching requests to search in the first place.

What makes warrants such an effective compromise is that they do not constitute an absolute bar to the activities of law enforcement. Warrants merely ensure that law enforcement officials focus on particular individuals and that they are given adequate independent oversight.

Of course, there will need to be exceptions from this general rule. Specific electronic devices that do not pose difficulties (such as regular cameras) should be exempted from this requirement. Another exception could apply if a communication is made directly to a government agent. Certain voluntary disclosures of communications to the government could also be exempted. Thus, if a person receives an e-mail from Osama Bin Laden by mistake, she can forward it on to the government. Other exceptions will also need to be made.

The key difference in this approach is that it refocuses the debate. The discussion will be over the specific instances where warrants are too cumbersome, rather than over technicalities. As technology continues to develop, the burden should be on law enforcement officials to convince Congress that a new device does not threaten individual privacy and that they should be authorized to use it with less than a warrant. The problem with the current law is that the FBI can try out new technologies in secret. Unless these technologies are reported to the public, which sometimes sparks an outcry, then there will be little pressure on Congress to investigate them and determine whether to enact protections. If the burden is placed on law enforcement to lobby Congress to use new technology, this would allow necessary debate and discussion about the costs and benefits of these technologies to occur.

What makes this simple approach preferable is that it is more

private papers on the possibility that they may disclose a crime.").

312 U.S. CONST. amend. IV.

313 Solove, *supra* note 50, at 1127.

314 Slobogin, *supra* note 309, at 17.

adaptable to changing technology than the highly technical provisions of much of current wiretap law. It allows law enforcement to engage in surveillance while keeping it circumscribed and accountable.

One might object that warrants are not feasible to achieve the purposes of electronic surveillance, especially in cases of national security. The *Keith* Court noted that "domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.'"[315] In particular, national security surveillance is often not aimed at finding out about who perpetrated past crimes; it is often prospective, designed to glean information about future threats. *Keith* suggested that the traditional Fourth Amendment warrant and probable cause requirements might not be compatible with the aims of such surveillance and that "[d]ifferent standards" may be constitutional if they are "reasonable."[316] This language in *Keith* suggests one of two alternatives to my proposal for warrants. First, one could generally support my approach but carve out an exception for cases involving national security, where less stringent requirements than warrants and probable cause would be required. Second, one could contend more broadly that warrants should not be required for electronic surveillance and that a standard of "reasonableness" should suffice.

Regarding an exception for national security, such a rule could threaten to practically eviscerate most protection against electronic surveillance. "National security" has often been abused as a justification not only for surveillance, but also for maintaining the secrecy of government records as well as violating the civil liberties of citizens. The Japanese Internment, as well as many of the abuses chronicled by the Church Committee, were justified in the name of national security.[317] As the court noted in *United States v. Ehrlichman*,[318] the Watergate burglary was an example of the misuse of "national security" powers: "The danger of leaving delicate decisions of propriety and probable cause to those actually assigned to ferret out 'national security' information is patent, and is indeed illustrated by the intrusion undertaken in this case . . . ."[319] The government has often raised national security concerns to conceal embarrassing and scandalous documents from the public—documents which often turned out to be harmless, such as the Pentagon Papers.[320]

---

315 United States v. United States District Court, 407 U.S. 297, 322 (1972).

316 *Id.* at 322–23.

317 DIFFIE & LANDAU, *supra* note 78, at 121.

318 United States v. Ehrlichman, 546 F.2d 910 (D.C. Cir. 1976).

319 *Id.* at 926.

320 *See* New York Times Co. v. United States, 403 U.S. 713 (1971); A CULTURE OF SECRECY: THE GOVERNMENT VERSUS THE PEOPLE'S RIGHT TO KNOW (Athan G. Theoharis ed., 1998). Attorney General John Mitchell wrote to the *New York Times*, stating that the Pentagon Papers "'will cause irreparable injury to the defense interests of the United

Beyond abusive invocations of national security, the line between national security and regular criminal activities is very blurry, especially in an age of terrorism. What precisely is "national security"? Is a mass murderer on the loose a national security issue? Some have even argued that drug trafficking is a national security issue.[321] Justice Brennan aptly observed that "the concept of military necessity is seductively broad, and has a dangerous plasticity."[322] Because of these problems, a national security exception to the warrant requirement should not be made.

An even broader approach is to apply a "reasonableness" standard in lieu of the warrant requirement. Akhil Amar argues that the Fourth Amendment has long been misinterpreted to require the use of warrants supported by probable cause for searches and seizures.[323] Reasonableness, Amar contends, is what the Fourth Amendment requires.[324] Setting aside the question of whether this is the correct interpretation of the Fourth Amendment, should electronic surveillance law adopt a reasonableness standard as a policy matter?[325] I submit that the answer should be an emphatic "no." The standard of "reasonableness" is a rather toothless one. For administrative, school, and employment searches, the Court has held that the Fourth Amendment merely requires that a search be "reasonable."[326] In a vast majority of applications of this standard—from searching employee offices and files, searching a student's purse at school, testing student athletes for drugs, and testing all students engaged in extracurricular activities for drugs—the Court has concluded that the search was reasonable.[327] Since the reasonableness standard has proven to be

States.'" STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 1017 (3d ed. 2002) (quoting Attorney General John Mitchell). The Pentagon Papers revealed that the government had misled the public about the origin of United States involvement in Vietnam. *See id.* at 1013.

321 DIFFIE & LANDAU, *supra* note 78, at 78 (discussing the trend of classifying the drug war as a national security issue).

322 Brown v. Glines, 444 U.S. 348, 369 (1980) (Brennan, J., dissenting).

323 AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE 31 (1997).

324 *Id.* I have critiqued Amar's views more extensively elsewhere. *See* Solove, *supra* note 50, at 1124–28.

325 In an interesting proposal regarding the FISA, Nola Breglio recommends that FISA orders be issued not by the secret FISC, but by regular Article III courts. *See* Breglio, *supra* note 236. Additionally, Breglio contends that the standard for foreign intelligence surveillance should be one of "reasonableness," which should be determined post hoc, after the surveillance has taken place. *See id.* at 211–14. In addition to the problems with the reasonableness standard discussed below, a post hoc review will suffer from extreme hindsight bias.

326 According to the doctrine, warrantless searches and seizures without probable cause do not violate the Fourth Amendment if "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (citations omitted).

327 *See, e.g.*, Bd. of Educ. v. Earls, 536 U.S. 822, 838 (2002) (drug testing of all students engaged in extracurricular activities was "reasonable"); Vernonia Sch. Dist. v. Acton, 515 U.S. 646, 665 (1995) (drug testing of student athletes was "reasonable");

quite weak in practice, it will not afford sufficient protection against the use of electronic surveillance.

The warrant and probable cause requirements are not incompatible with surveillance designed to detect prospective threats. Probable cause exists "where the facts and circumstances within [law enforcement officials'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed."[328] Such a requirement would prohibit surveillance based upon mere conjecture, naked suspicion, race or nationality, religious affiliation, or political speech. It would not, however, require that the government investigate only previously completed crimes. The planning of future crimes, especially terrorism, is itself a crime, most likely conspiracy or attempt. Therefore, the government could obtain a warrant to engage in electronic surveillance if it had "reasonably trustworthy information" that a future crime was being discussed between conspirators or being planned. The warrant rule would prevent dragnet surveillance designed to listen in broadly on people's conversations—most likely people from disfavored groups—in the hope of hearing some suspicious chatter.

The approach I recommend does not apply to the FISA. The FISA, as it was originally conceived before being altered by the USA PATRIOT Act, aimed to allow for foreign intelligence gathering, which is different from criminal investigations. Foreign intelligence gathering enables the government to pursue counterintelligence activities—to monitor foreign agents working in the United States, to investigate spies, and so on.[329] These purposes are quite different from ordinary criminal cases, as the primary goal of FISA surveillance is to gather data, not to deal with crimes. This is why the FISA required that the primary purpose for the surveillance be intelligence gathering. The USA PATRIOT Act loosened this requirement, which is a troubling development since much surveillance in today's world of terrorism has a dual purpose—it involves both intelligence gathering and investigating criminal activity. The USA PATRIOT Act also weakened the wall that existed to prevent intelligence gathering from being used as a pretext to gather criminal evidence outside of the stricter ECPA regime. In the old version of FISA, the wall would allow evidence gleaned from a bona fide intelligence operation that revealed evidence of criminal activity to be used in a criminal prosecution. But a wall was erected to prevent the pretextual use of FISA for criminal investigation purposes. I

O'Connor v. Ortega, 480 U.S. 709 (1987) (search of employee's office and files may be "reasonable"); New Jersey v. T.L.O., 469 U.S. 325, 346–47 (1985) (search of student's purse at school was "reasonable").

328 Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (citations omitted).

329 **Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. ___, manuscript 33 (2004).**

recommend that FISA be returned to its pre–USA PATRIOT Act state. The old FISA, and the procedures developed in light of it at the DOJ, provide a compromise solution that would allow for the surveillance of foreign agents, yet prevent the FISA from being abused for criminal investigations.[330]

B. A Legislative Charter for the FBI

Another important component of a regulatory regime for government surveillance is a legislative charter for the FBI. The FBI wields a tremendous amount of power and it should be placed under greater control by Congress. Today, the FBI has about 11,000 agents and 16,000 support staff; it has 56 field offices, 400 satellite offices, and 40 foreign liaison posts.[331] Despite its vast size, extensive and expanding responsibilities, and profound technological capabilities, the FBI lacks a legislative charter.[332]

A charter defining the FBI's scope and powers as well as requiring more regular congressional oversight would go a long way to ensuring against the terrible abuses of the FBI's past. A detailed proposal for such a charter is beyond the scope of this Article. The bulk of such a charter, however, could be composed by codifying existing internal FBI Guidelines into law. The Church Committee recommended a legislative charter to govern intelligence gathering activities, but many of the Committee's proposals were put into operation through executive orders and guidelines.[333] Executive orders and Attorney General Guidelines are the "primary source of authority for national security surveillance."[334]

Unfortunately, executive orders and guidelines can all be changed by executive fiat, as demonstrated by Ashcroft's substantial revision to the guidelines in 2002.[335] Moreover, the Attorney General Guidelines are not judicially enforceable.[336] The problem with the current system is that it

---

330 Under the old FISA approach, the foreign intelligence exception to a warrant applies until the primary purpose of the surveillance ceases to be for foreign intelligence. United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980); *see also* DYCUS ET AL., *supra* note 320, at 655.

331 FBI, GENERAL FREQUENTLY ASKED QUESTIONS, http://www.fbi.gov/aboutus/faqs/faqsone.html (last visited Dec. 4, 2003).

332 *See* DYCUS ET AL., *supra* note 320, at 698. The closest thing to a statutory authorization for the FBI is 28 U.S.C. § 533 (2000), which gives the Attorney General the authority to appoint officials to detect and prosecute crimes and to conduct investigations of the Department of Justice and Department of State. DYCUS ET AL., *supra* note 320, at 698.

333 *See* DYCUS ET AL., *supra* note 320, at 464; Banks & Bowman, *supra* note 79, at 34–35. President Ford responded to the Committee by issuing Executive Order No. 11,905. DYCUS ET AL., *supra* note 320, at 464. Ford's order was superseded with President Carter's Executive Order No. 12,036. *Id.* President Reagan replaced Carter's order with Executive Order No. 12,333. *Id.*

334 Banks & Bowman, *supra* note 79, at 74.

335 *See supra* notes 297–299 and accompanying text.

336 DYCUS ET AL, *supra* note 320, at 712. There is one exception. In *Alliance to End*

relies extensively on self-regulation by the executive branch. Much of this regulation has been effective, but it can too readily be changed in times of crisis without debate or discussion. Codifying the internal executive regulations of the FBI would also allow for public input into the process. The FBI is a very powerful arm of the executive branch, and if we believe in separation of powers, then it is imperative that the legislative branch, not the executive alone, become involved in the regulation of the FBI. The guidelines should be judicially enforceable to ensure that they are strictly followed.

I recommend that the original FBI guidelines, under Attorney General Levi, should be used as the foundation for a legislative charter for the FBI. The Levi Guidelines were crafted to prevent the abuses chronicled by the Church Committee, and they provide strong limits on the use of surveillance directed at free speech and political activities.[337] The threshold standards of the Levi Guidelines are more meaningful than the watered-down versions employed in subsequent revisions. The Levi threshold standards are not insurmountable—they are a practical compromise between privacy and effective law enforcement that safeguards against abuses.

Additionally, the charter should require Congress to undertake an extensive assessment of intelligence activities at five- to ten-year intervals. This assessment would be similar in scope to the Church Committee Report. The Church Committee performed a profoundly valuable service, exposing and memorializing surveillance abuses that occurred over a period of about forty years. This kind of thorough accounting of the often clandestine activities of governmental intelligence agencies should not be an isolated undertaking.

Conclusion

Currently, Congress is considering whether certain changes to surveillance law made by the USA PATRIOT Act should sunset in 2005. Congress should take this opportunity to reconsider electronic surveillance law more generally. Merely rolling back the USA PATRIOT Act changes will not address the most serious failings of electronic surveillance law. Tweaks and patches will not be sufficient—a more radical reconstruction is sorely needed.

Repression v. City of Chicago, 742 F.2d 1007, 1010 (7th Cir. 1984), the FBI agreed as part of a settlement that the Guidelines would be judicially enforceable for the plaintiffs.

337 *See* Banks & Bowman, *supra* note 79, at 68–69.