Harvard Journal of Law & Technology
Volume 15, Number 2 Spring 2002

THE CASE FOR MAGIC LANTERN: SEPTEMBER 11 HIGHLIGHTS THE NEED FOR INCREASED SURVEILLANCE

Christopher Woo & Miranda So

I. INTRODUCTION

The Federal Bureau of Investigation ("FBI") is reportedly developing a new surveillance technology, code-named Magic Lantern, that is capable of installing a keystroke logging program on a computer without requiring physical access to the computer.[1] This powerful surveillance tool can help the FBI obtain information to prevent terrorism. The attacks of September 11 showed how vulnerable the United States is to terrorism and led to calls for stronger government actions to safeguard national security.[2] The Bush Administration re-

1. *See* Carrie Kirby, *Network Associates Mired in Security Debate*, S.F. CHRON., Nov. 28, 2001, at B1; Robert Lemos, *FBI's Magic Revealed as Old Tricks*, ZDNET, Nov. 21, 2001, *at* http://zdnet.com.com/2100-1105-276145.html (last visited Mar. 10, 2002); Alex Salkever, *A Dark Side to the FBI's Magic Lantern*, BUS. WK. ONLINE, Nov. 27, 2001, *at* http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm (last visited Mar. 18, 2002); Bob Sullivan, *FBI Software Cracks Encryption Wall*, MSNBC, Nov. 20, 2001, *at* http://www.msnbc.com/news/660096.asp?cp1=1 (last visited Mar. 10, 2002); Robert Vamosi, Commentary, *Warning: The FBI Knows What You're Typing*, ZDNET, Dec. 4, 2001, *at* http://zdnet.com.com/2100-1107-504142.html (last visited on Feb. 10, 2002); *FBI Confirms Magic Lantern Exists*, MSNBC, Dec. 12, 2001, *at* http://www.msnbc.com/news/671981.asp?0si (last visited Mar. 10, 2002).

2. *See* Robin Toner & Janet Elder, *Public Is Wary but Supportive on Rights Curbs*, N.Y. TIMES, Dec. 12, 2001, at A1; Robert O'Harrow Jr. & Jonathan Krim, *National ID Card Gaining Support*, WASH. POST, Dec. 17, 2001, at A1.

sponded to such calls with a range of measures, including establishing military tribunals to try accused terrorists, allowing government officials to monitor conversations between some suspected terrorists and their attorneys, arresting more than 1000 suspects and detaining hundreds of them in jail, and questioning more than 5000 immigrants, mostly Muslims.[3] Surveillance will be an important tool in the government's arsenal of weapons against international terrorism.[4] Traditionally, Americans have been wary of the use of technology that may infringe upon civil liberties. However, in light of the attacks of September 11, many Americans are now ready to endorse more intrusive surveillance technologies that can aid in the fight against terrorism.[5]

Technology has always played a critical role in law enforcement surveillance. From wiretapping to thermal imaging, technological advancement has allowed the government to monitor an increasingly wide range of activities and has led to greater successes in intelligence gathering. The government has used wiretaps to monitor conversations for over a century.[6] The development of thermal imaging devices allows law enforcement agencies to detect heat emitted from residences and consequently to infer certain types of activities occurring inside such residences.[7] Recent advances in computer technology

---

3. *See* David Johnston & Don Van Natta Jr., *Ashcroft Weighs Easing F.B.I. Limits for Surveillance*, N.Y. TIMES, Dec. 1, 2001, § 1, at 1; Matthew Purdy, *Bush's New Rules to Fight Terror Transform the Legal Landscape*, N.Y. TIMES, Nov. 25, 2001, § 1A, at 1; Robin Toner, *Civil Liberty vs. Security: Finding a Wartime Balance*, N.Y. TIMES, Nov. 18, 2001 § 1A, at 1. These assertions of power by the executive branch may raise constitutional issues. *See* David E. Sanger, *There's a Small Matter of Checks and Balances*, N.Y. TIMES, Jan. 27, 2002, § 4, at 1.

4. In the wake of September 11, the government has been trying to increase surveillance efforts. *See* Simon Romero, *Bigger Brother in the Wireless World*, N.Y. TIMES, Sept. 24, 2001, at C10; John Schwartz, *Scouring the Internet in Search of the Tracks of Terrorists*, N.Y. TIMES, Sept. 17, 2001, at C2.

5. In the wake of September 11, Congress considered several bills that would increase the use of new surveillance technology for preventing crime and terrorism. *See* Lisa Guernsey, *Living Under an Electronic Eye*, N.Y. TIMES, Sept. 27, 2001, at G1.

6. *See* Mark G. Young, Note, *What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance*, 70 FORDHAM L. REV. 1017, 1024 (2001); *see also* Martin v. Sheriff, 5 Ohio Dec. 100 (Ohio Prob. 1894) (first American case discussing the tapping of telegraph wires); People v. McDonald, 165 N.Y.S. 41 (N.Y. App. Div. 1917) (first American case discussing evidence seized by the police from a telephone wiretap); Olmstead v. United States, 277 U.S. 438 (1928) (first Supreme Court case dealing with wiretapping).

7. *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1498 (2000); Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 447–48 (1997); Young, *supra* note 6, at 1033; *see also* United States v. Deaner, Nos. 1:CR-92-0090-01, -02, 1992 WL 209966 (M.D. Pa., Jul. 27, 1992) (discussing whether a thermal imaging device violates the Fourth Amendment for the first time). The Supreme Court only recently addressed the issue of thermal imaging devices in *United States v. Kyllo*, 533 U.S. 27 (2001). The technology is particularly useful in detecting the heat emitting lamps used to grow marijuana.

have led to programs such as Carnivore, a surveillance system capable of collecting information sent from a suspect's computer through her Internet Service Provider to other computers on the Internet.[8] This information includes the content of e-mail messages, web pages viewed by the suspect, and files sent using File Transfer Protocol.[9] Although new technological devices greatly enhance the capability of law enforcement to collect intelligence data, if unchecked by rules, the government will be able to use these devices to intrude into virtually all aspects of our personal lives.

Courts have found it difficult to decide whether searches performed with new surveillance devices fall within the ambit of the Fourth Amendment. When it first examined the issue, the Supreme Court held that wiretapping without a warrant did not violate the Fourth Amendment because the installation of the wiretap did not require entry into the suspect's home or office.[10] Almost forty years later, realizing that such a reading would allow too great an intrusion into people's privacy, the Supreme Court reversed course. In *Katz v. United States*,[11] the Court held that wiretapping requires a warrant. The *Katz* Court found that "the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[12] In a concurrence, Justice Harlan expressed his view that the Fourth Amendment applies when there is a reasonable expectation of privacy, i.e., the person has a subjective expectation of privacy, and society recognizes the expectation as being reasonable.[13]

Harlan's concurrence in *Katz* has become the governing standard for defining when a Fourth Amendment search occurs and has been used by courts to determine whether a new technology comes within the scope of the Fourth Amendment.[14] For some time, courts applying the standard were reluctant to impose a warrant requirement on new technologies. In *Smith v. Maryland*,[15] the Court found that the use of a

---

8. *See* STEPHEN P. SMITH ET AL., IIT RESEARCH INSTITUTE, INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM: FINAL REPORT (2000), *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf (last visited Mar. 10, 2002); John Schwartz, *Wiretapping System Works on Internet, Review Finds*, N.Y. TIMES, Nov. 22, 2000, at A19. Carnivore has raised a wide range of privacy concerns. *See, e.g.*, John Schwartz, *Computer Security Experts Question Internet Wiretaps*, N.Y. TIMES, Dec. 5, 2000, at A16.

9. *See* SMITH ET AL., *supra* note 8, at ix.

10. *See* Olmstead v. United States, 277 U.S. 438, 464–66 (1928).

11. 389 U.S. 347 (1967).

12. *Id.* at 353.

13. *Id.* at 361 (Harlan, J., concurring).

14. *See, e.g.*, Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1366 (1992); Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1756 n.16 (1994).

15. 442 U.S. 735 (1979).

pen register is not a search because there is no legitimate expectation of privacy regarding numbers dialed on a telephone.[16] Likewise, the Supreme Court in *California v. Ciraolo*[17] and in *Florida v. Riley*[18] held that aerial surveillance of private homes and surrounding areas does not constitute a search because people cannot reasonably be expected to be protected from naked-eye aerial observations. In all of these cases, the Court allowed new technology to increasingly limit the areas where people have a reasonable expectation of privacy. However, over time, the pendulum swung back in the other direction. In *Kyllo v. United States*,[19] the Court held that the use of a thermal-imaging device requires a warrant because the device is not in general public use, and the surveillance reveals information about the interior of the house that ordinarily only a physical search would expose.[20]

In light of September 11, the balance may shift once again toward favoring the use of new technologies without Fourth Amendment protections. Allowing the use of advanced surveillance technologies such as Magic Lantern may restrict civil liberties, especially people's right of privacy.

The scope of activities that Magic Lantern can monitor goes well beyond that of traditional wiretapping devices. The FBI can install Magic Lantern without physical access to the target computer. For example, by taking advantage of vulnerabilities in e-mail software, Magic Lantern can enter a targeted system disguised as a message from a suspect's family member.[21] Alternatively, law enforcement can use known vulnerabilities in operating systems to hack into the target computer and insert the program. Once installed, Magic Lantern will capture keystrokes and send data logs back to the FBI while the suspect is connected to the Internet.[22] Anti-virus programs may be capable of detecting Magic Lantern and removing it from computers. However, the government has allegedly asked anti-virus companies not to interfere with Magic Lantern, and a few have reportedly agreed.[23]

---

16. "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released." United States v. New York Tel. Co., 434 U.S. 159, 161 n.1 (1977). The *Smith* Court found that even if there is a subjective expectation of privacy, the expectation is not reasonable as the person dialing the telephone gave the captured information to a third party — the telephone company. *Smith*, 442 U.S. at 742–44.

17. 476 U.S. 207, 213–14 (1986).

18. 488 U.S. 445, 450–52 (1989).

19. 533 U.S. 27 (2001).

20. *Id.* at 34–35.

21. *See* Sullivan, *supra* note 1. Depending on the vulnerability exploited, the suspect may not even need to open the e-mail message to activate Magic Lantern. *See* Salkever, *supra* note 1.

22. *See* sources cited *supra* note 1.

23. *See* Kirby, *supra* note 1, at B1.

The types of information that a keystroke logging program is capable of gathering distinguish it from other types of surveillance. Keystroke loggers may provide the best way for law enforcement to crack strong encryption used by criminals and terrorists to hide information. Although there are strong encryption systems that cannot be defeated in a person's lifetime, many have a weak point in that a user must enter a passphrase to access his data.[24] Cracking a passphrase can take significantly less time than attacking the encryption scheme itself — as little as six months for a passphrase consisting of three randomly chosen words.[25] A keystroke logger allows for immediate access to encrypted information because it "watches" the user type his passphrase and relays the passphrase to the party that installed the logger.

The ability of keystroke logging software to assist law enforcement in decrypting information is only one function of the software. By logging keystrokes, much more information can be gathered. Indeed, for many computer users, keystrokes are the primary means by which information is entered into a computer. Every e-mail message composed, even if it is not sent, can be reconstructed by a keystroke logger. Diary entries, drafts of documents that are never released, and other information that the user never intended to make public can also be collected by a keystroke logger.

Magic Lantern and other similarly intrusive programs that law enforcement may use in the future present a challenge to the balance of national security and civil liberties. On one hand, the failure of the government to adequately address the risks of terrorism and prevent the attacks of September 11 underscores the need for greater intelligence gathering. On the other hand, in evaluating the reasonableness of new surveillance technology, courts should be aware that the risk of erosion of civil liberties is greatest during national emergencies.[26] Part II of this Note presents the competing concerns of national security and civil liberties in determining the legality of a new surveillance device. Part III argues that, in response to heightened national security concerns, Congress should authorize the use of Magic Lantern but constrain its use in order to minimize its potential intrusion on civil liberties.

---

24. *See generally* The Passphrase FAQ (version 1.04, last revised Jan. 13, 1997, Randall T. Williams ed.), *at* http://www.stack.nl/~galactus/remailers/passphrase-faq.html.

25. *See id.* § 2.7.

26. *See generally* PHILIP B. HEYMANN, TERRORISM AND AMERICA: A COMMONSENSE STRATEGY FOR A DEMOCRATIC SOCIETY (paperback ed. 2000) (discussing the need to respect civil liberties while combating terrorism).

II. BALANCING OF NATIONAL SECURITY AND CIVIL LIBERTIES

A. National Security

Surveillance for the purpose of national security requires courts to balance two conflicting interests: the government's duty to protect the nation, and the danger that unreasonable surveillance poses to individual privacy and free expression.[27] In 1978, Congress enacted the Foreign Intelligence Surveillance Act ("FISA"),[28] which places some limits on the government's powers to search for foreign intelligence. This regime for gathering foreign intelligence is separate from the regime for wiretaps for normal surveillance, popularly known as "Title III."[29] FISA establishes a special court, the Foreign Intelligence Surveillance Court ("FISC").[30] In general, the government needs to obtain a warrant from the FISC before wiretapping for foreign intelligence purposes.[31] Each application for a FISA order requires the At-

27. United States v. United States District Court, 407 U.S. 297, 314–15 (1972).

28. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1811 (1994 & Supp. V 1999) [hereinafter FISA]. All cites to FISA refer to the statute as it existed before the passage of the USA PATRIOT Act.

29. Omnibus Crime Control and Safe Streets Act of 1968, Title III, 18 U.S.C. §§ 2510–2520 (1994 & Supp. V 1999).

30. FISA § 103, 50 U.S.C. § 1803.

31. *Id.* There are exceptions to the warrant requirement. First,

> The President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that —
> (A) the electronic surveillance is solely directed at —
> (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or
> (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title;
> (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and
> (C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

torney General or Deputy Attorney General's approval and must contain information specified in 50 U.S.C. § 1804. The FISC shall issue the order if the judge finds that:

> (1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;
> (2) the application has been made by a Federal officer and approved by the Attorney General;
> (3) on the basis of the facts submitted by the applicant there is probable cause to believe that —
>
> > (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and
> > (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
>
> (4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and
> 5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.[32]

The passage of FISA has provided the intelligence community with a process for obtaining wiretaps that is less strict than the process used for Title III wiretaps; the FISC has rarely, if ever, denied applications for wiretaps under FISA.[33]

Id. § 1802. There is also an exception for emergency situations. *Id.* § 1805. Another exception exists for fifteen days following a Congressional declaration of war. *Id.* § 1811.

32. *Id.* § 1805.

33. *See* HEYMANN, *supra* note 26, at 138 (discussing ease of obtaining FISA warrant as compared to obtaining warrant in standard criminal case); William Carlsen, *Secretive U.S. Court May Add to Power; Bush Wants to Use Terrorism Panel in*

September 11 reinforces national security as a paramount concern of the administration. For the first time, foreign terrorists were able to launch a large scale and audacious attack on American soil. The magnitude of lives lost and the destruction of the World Trade Center, a symbol of America's success,[34] have put a tremendous amount of pressure on the Bush Administration to eradicate the Al Qaeda network. Al Qaeda has allegedly been involved in numerous other attacks: the bombing of U.S. embassies in East Africa, the attacks on U.S. troops in Somalia during Operation Restore Hope, and the bombing of the USS Cole off the coast of Yemen.[35] The threat that terrorists may start to use other unconventional weapons — radiological, chemical, biological, and nuclear weapons[36] — also makes Americans more receptive to the use of surveillance devices that would maximize the success of foreign intelligence gathering, even if such devices come at the price of infringement on civil liberties.

At times of heightened passion, the public's desire for protection against national security risks is potentially dangerous because such public sentiment may sway the government into using techniques that are overly intrusive.[37] It is imperative that we not forget the lessons of

---

Criminal Probes, S.F. CHRON., Oct. 6, 2001, at A3 (as of October 2001, the Foreign Intelligence Surveillance Court has only denied one request for a warrant).

34. *See, e.g.*, Tara Bahrampour, *Shadows Across the City*, N.Y. TIMES, Sept. 23, 2001, § 14, at 6.

35. *See* TONY C. L. BLAIR, RESPONSIBILITY FOR THE TERRORIST ATROCITIES IN THE UNITED STATES, 11 SEPTEMBER 2001 AN UPDATED ACCOUNT (2001) (10 Downing Street's report implicating Osama Bin Laden), *available at* http://www.pm.gov.uk/filestore/Culpability_document1.pdf (last visited Mar. 17, 2002); Judith Miller, *Planning for Terror but Failing to Act*, N.Y. TIMES, Dec. 30, 2001, § 1A, at 1; Walter Pincus, *Al Qaeda Leader Talked of Plot Against U.S. Embassy; Interrogation Led to Closing of Facility in Yemen*, WASH. POST, Jan. 23, 2002, at A9.

36. There are rumors that Bin Laden was attempting to obtain biological, chemical, and nuclear weapons before disruption of his operations in Afghanistan. *See* Jimmy Burns, *London Plot 'Verifies Bin Laden Threat'*, FIN. TIMES, Dec. 17, 2001, at 8. In 1995, Aum Shinrikyo tried to launch sarin gas attacks in Japan. *See* William J. Perry, *Preparing for the Next Attack*, FOREIGN AFF., Nov./Dec. 2001, at 31; Judith Miller, *Some in Japan Fear Authors of Subway Attack Are Regaining Ground*, N.Y. TIMES, Oct. 11, 1998, § 1, at 12. Closer to home, there was an anthrax mailing scare in 2001 that claimed several victims. *See* Lawrence K. Altman & Gina Kolata, *Anthrax Missteps Offer Guide to Fight Next Bioterror Battle*, N.Y. TIMES, Jan. 6, 2002, § 1, at 1; Eric Lipton & Kirk Johnson, *Tracking Bioterror's Tangled Course*, N.Y. TIMES, Dec. 26, 2001, § 1A, at 1; Steve Twomey & Justin Blum, *How the Experts Missed Anthrax: Brentwood Cases Defied Assumptions About Risks*, WASH. POST, Nov. 19, 2001, at A1.

37. In times of crisis, people often are prepared to allow for greater surveillance. *See* Guernsey, *supra* note 5, at G1. In 1948, Justice Jackson expressed his concerns about the danger of using "war power" to justify government action. He wrote: "It usually is invoked in haste and excitement when calm legislative consideration of constitutional limitation is difficult. It is executed in a time of patriotic fervor that makes moderation unpopular. And, worst of all, it is interpreted by the Judges under

history when abuses were perpetrated in the name of national security. In January 1920, in response to the threat supposedly posed by the Communist revolution in Russia, Attorney General Palmer authorized mass dragnet raids, arresting more than 6000 citizens and aliens attending meetings of the Communist Party and the Communist Labor Party, ostensibly to deport alien radicals.[38] In World War II, the Roosevelt Administration excluded Japanese-Americans from certain areas of the West Coast, and the Supreme Court upheld the practice.[39] During the Cold War, the FBI investigated Adlai E. Stevenson, Henry Cabot Lodge, Eleanor Roosevelt, John F. Kennedy, Ernest Hemingway, and Martin Luther King Jr., among others.[40] Prior abuses remind us that while national security may justify more extensive surveillance efforts, the administration and courts should be careful to appropriately contain the response to September 11.

B. Civil Liberties

1. Right to Privacy

The right to privacy is the primary civil liberties concern when analyzing surveillance devices. Since *Griswold v. Connecticut*,[41] the Supreme Court has recognized that the Constitution affords some protection for the right to privacy.[42] While the government has a legitimate right and duty to interfere with illegal activities, the probability that its monitoring efforts may affect those who engage in perfectly legitimate activities requires courts to put limitations on intrusive surveillance systems. People engaged in legitimate activities have valid reasons for not wanting the government to monitor them. E-mail messages to friends, for example, may contain embarrassing details that the author does not want anyone other than the intended recipients to

---

the influence of the same passions and pressures." Woods v. Cloyd W. Miller Co., 333 U.S. 138, 146 (1948) (Jackson, J., concurring).

38. *See* Peter H. Irons, *"Fighting Fair": Zechariah Chafee, Jr., The Department of Justice, and the "Trial at the Harvard Club"*, 94 HARV. L. REV. 1205, 1209 (1981); Athan Theoharis, Opinion, *Civil Liberties; The Cost of Fighting Terrorism*, L.A. TIMES, Apr. 30, 1995, at M1.

39. *See* Korematsu v. United States, 323 U.S. 214, 217–19 (1944). There was little public objection when FDR ordered the internment of Japanese-Americans. In fact, many prominent Americans supported the move. *See* Boris I. Bittker, *Eugene V. Rostow*, 94 YALE L.J. 1315, 1319–20 (1985); Toner, *supra* note 3, at 1.

40. *See* Neal Gabler, *A Political Verdict; Pratt; A Remainder of the Old FBI*, L.A. TIMES, June 8, 1997, at M1; Johnston & Van Natta Jr., *supra* note 3, at 1; Theoharis, *supra* note 38, at M1.

41. 381 U.S. 479 (1965).

42. *Id.* at 484–85.

read.[43] As people increasingly rely on computers to accomplish daily tasks, programs such as Magic Lantern may greatly intrude into people's private lives.

As technology advances, the expectation of privacy changes. People in modernized societies may have a lower expectation of privacy as they realize that their actions leave electronic trails that businesses and governments can trace. However, the availability of programs such as Anonymizer[44] suggests that people would like to remain anonymous when on the Internet and are not yet willing to accept a greater loss of privacy.[45] A reasonable expectation of privacy seems even more appropriate in the context of files kept on a computer but not sent to anyone else, particularly those files that are encrypted. As computers have become an integral and personal part of people's lives, computer users may begin to expect that the information on their machines is private. Alternatively, as people become more aware about the ability of unauthorized users to exploit security holes and access computers connected to the Internet, their expectation of privacy may decrease. Thus, it is unclear whether or not courts should decide that people have a reasonable expectation of privacy in the contents of their computers.[46]

2. Freedom of Speech

Electronic surveillance may hinder free speech, a Constitutional protection the Founders explicitly granted to the American people in the Bill of Rights. Historically, the First Amendment protects all kinds of speech, even speech that conventional wisdom considers misguided. In *Brandenburg v. Ohio*,[47] the Court ruled that the government cannot prevent people from advocating violence, short of direct in-

43. Some cases address the expectation of privacy in e-mail messages. *See* United States v. Charbonneau, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997); United States v. Maxwell, 45 M.J. 406, 418–19 (C.A.A.F. 1996).

44. *See* Anonymizer.com *at* http://www.anonymizer.com (last visited Mar. 8, 2002) (advertising product that "[p]revent[s] tracking by Web sites, hackers and others; [s]hields your IP address; [and r]emoves privacy threats from the pages you view").

45. Many people support increased surveillance online in return for better security. However, consumers are still interested in protecting their privacy from government and business. *See* John Schwartz, *Seeking Privacy Online, Even as Security Tightens*, N.Y. TIMES, Nov. 11, 2001, § 3, at 10; *see also* Guernsey, *supra* note 5, at G1.

46. This is a decision that could have a tremendous economic impact on the nation. Restricting the right to privacy may result in real economic loss, such as a decrease in worker efficiency, if people become more reluctant to use personal computers. *See* Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 473–74 (1999).

47. 395 U.S. 444 (1969).

citement.[48] Freedom of speech guarantees that the government will not outlaw the advocacy of unpopular causes, allowing for democratic debate.

The U.S. government has a track record of clamping down on free speech during periods of crisis, and the audacity of the September 11 attacks brings to the foreground the concern that free speech values may once again be compromised. For example, during the First World War, the Supreme Court upheld a ten-year sentence for an anti-war speech, stating that the speech hindered recruiting for war efforts and therefore violated the Espionage Act.[49] In 1798, during a quasi-war with France, Congress passed the Alien and Sedition Acts, prohibiting people from criticizing the government.[50] As much as Americans want to fight terrorism, most would not want to sacrifice their Constitutional right of free speech. Lawmakers should therefore be careful to distinguish between acts that support terrorism and mere speech expressing opposition to some of the government's activities in its "war against terrorism." Advocating support for the goals of a terrorist organization, such as the unification of Northern Ireland with Ireland, should not be criminalized. President Bush's recent speech, stating that "anyone who espouses a philosophy that's terrorist and bent, I assure you we will bring that person to justice,"[51] threatens to blur the line between speech, which is protected, and incitement to violence, which is not. In the present climate, citizens may be afraid to openly oppose government action. If they feel the government might be secretly monitoring their computers, they may be overly cautious about what they write in e-mails or even documents that are drafted but never sent to a recipient.

3. Racial Profiling

Targeted surveillance may lead to another civil liberties concern — racial discrimination. The Equal Protection Clause of the Fourteenth Amendment requires the government to give all similarly situated people the equal protection of the law and prohibits discriminatory treatment based on race and other suspect categories. Plaintiffs who wish to prove an equal protection violation, however,

48. *Id.* at 447.

49. *See* Debs v. United States, 249 U.S. 211, 214–16 (1919); *see also* Espionage Act, ch. 30, tit. 1, § 3, 40 Stat. 217, 219 (1917) (codified as amended at 18 U.S.C. § 2388 (1994)).

50. *See* Alien and Sedition Acts, ch. 73, 1 Stat. 596, 596–97 (1798) (expired 1801); *see also* William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1 (2000); Larry D. Kramer, *Putting the Politics Back into the Political Safeguards of Federalism*, 100 COLUM. L. REV. 215, 272 (2000).

51. David E. Sanger, *Bush, on Offense, Says He'll Fight to Keep Tax Cuts*, N.Y. TIMES, Jan. 6, 2002, at 1 (internal quotation marks omitted).

who wish to prove an equal protection violation, however, face a high barrier — they must show both disproportionate impact and racially discriminatory intent or purpose.[52]

Plaintiffs could also challenge racially motivated searches under the Fourth Amendment, stating that race alone is not a basis for reasonable suspicion.[53] However, so long as the law enforcement agent is able to establish probable cause, the fact that a search may be racially motivated is probably not relevant to a Fourth Amendment claim. In *Whren v. United States*, the Supreme Court ruled that "the constitutional basis for objecting to intentionally discriminatory application of laws is the Equal Protection Clause, not the Fourth Amendment. Subjective intentions play no role in ordinary, probable-cause Fourth Amendment analysis."[54] A recent Ninth Circuit decision distinguishes between ethnicity as *a* factor in a search and ethnicity as the *only* factor in a search. In *United States v. Montero-Camargo*,[55] the court ruled that "persons of a particular racial or ethnic group may not be stopped and questioned because of such appearance, unless there are other individualized or particularized factors which, together with the racial or ethnic appearance identified, rise to the level of reasonable suspicion or probable cause."[56]

After the September 11 attacks, a Gallup poll showed that fifty-eight percent of Americans favored requiring Arabs, including Arab-Americans, to go through more intensive security checks at airports.[57] The results highlight the concern that Americans may favor surveillance policies that focus on Arabs and Arab-Americans solely because of their ethnicity. Although all nineteen hijackers on the September 11 airplanes were Arabs, a policy that singles out people based solely on ethnicity presents critical equal protection issues. Law enforcement may argue that being Arab is a suspect characteristic, but being Arab alone cannot justify government investigation. The danger of creating second-class citizens through discrimination is great. Racial discrimination against Arab-Americans may radicalize members of the community. Courts have a duty to protect all people, regardless of sex,

---

52. *See* Washington v. Davis, 426 U.S. 229, 239 (1976); *see also* United States v. Armstrong, 517 U.S. 456, 465 (1996); Chavez v. Ill. State Police, 251 F.3d 612, 635–36 (7th Cir. 2001); United States v. Avery, 137 F.3d 343, 355–56 (6th Cir. 1997).

53. *See* Anthony C. Thompson, *Stopping the Usual Suspects: Race and the Fourth Amendment*, 75 N.Y.U. L. REV. 1517 (1999) (arguing that the Fourth Amendment, rather than the Equal Protection Clause, should be used to protest racially motivated searches).

54. 517 U.S. 806, 813 (1996).

55. 208 F.3d 1122 (9th Cir. 2000).

56. *Id.* at 1134 n.22.

57. Mark Singer, *America's Largest Arab Community in the Aftermath of September 11th*, NEW YORKER, Oct. 15, 2001, at 62.

age, and ethnicity when they evaluate the reasonableness of a surveillance.

III. SHOULD MAGIC LANTERN BE ALLOWED?

Magic Lantern is a valuable program that would enhance the government's ability to collect intelligence information. It is, however, an extremely powerful technology that, if unfettered, could allow law enforcement to monitor every keystroke typed on a computer once the FBI has successfully installed the logging program. In times when terrorists are capitalizing on the technological revolution in their planning and operations, Magic Lantern may be necessary to combat devious and sophisticated terrorists trying to outpace law enforcement. To combat the terrorists' use of modern technology, the FBI should be allowed to use Magic Lantern to keep track of all keystrokes. Terrorists can hide messages in pictures and other seemingly innocuous files that they can then send to each other through the Internet.[58] Keystroke logs give the FBI access to the secret messages without the need to decode the picture.

Recently, the court in *United States v. Scarfo*[59] found that a key-logging device installed with a search warrant did not violate the Fourth Amendment.[60] The court stated: "we must be ever vigilant against the evisceration of Constitutional rights at the hands of modern technology. Yet, at the same time, it is likewise true that modern-day criminals have also embraced technological advances and used them to further their felonious purposes."[61]

If there is the slightest possibility that Magic Lantern would uncover terrorist acts and avert thousands of deaths, the government is justified in using it as a tool in foreign intelligence surveillance. Yet, how do we know whether new technology may increase the probability of detection of future terrorist incidents? The key question in all surveillance is deciding whom to monitor. To prevent the government from overly intruding on people's right of privacy and to make the amount of intelligence collected manageable for the agency, the FBI needs to target suspects and not use Magic Lantern indiscriminately. Law enforcement should target people it has probable cause to believe are engaged in terrorist activities. However, terrorist groups recruit new people and new terrorist organizations form all the time; there is always the problem of fresh faces appearing. Of the nineteen hijackers on the September 11 planes, only two were on the FBI's terrorist

58. *See* Gina Kolata, *Veiled Messages of Terror May Lurk in Cyberspace*, N.Y. TIMES, Oct. 30, 2001, at F1.

59. 180 F. Supp. 2d 572 (D.N.J. 2001).

60. *Id.* at 578.

61. *Id.* at 583.

watch list.[62] We must remember that intelligence gathering will never give us information on every terrorist plot; there are limits to the efficacy of any new technology.

Congress should pass a new statute, separate from FISA and Title III, to govern Magic Lantern and other keystroke logging programs for foreign intelligence gathering purposes.[63] The greater potential for intrusion that these technologies present means Congress needs to place more restrictions on their use. By passing a new statute, Congress can allow for their use while imposing restrictions of a greater degree than the law currently does on existing technologies, thus minimizing intrusion into Americans' civil liberties.

The government should be required to obtain a warrant from a court before using Magic Lantern to conduct surveillance. In their desire to gather intelligence, law enforcement officials may be too eager to monitor potential suspects and may, in the process, give inadequate consideration to civil liberty concerns. By requiring review by the judiciary, an independent institution, Congress can force law enforcement officials to articulate their reasons for probable cause. Race or ethnicity and vocal support for terrorism are reasonable factors to consider in a probable cause determination, but courts should require more proof that the subject of the requested warrant is actually involved in terrorism. In addition, courts should require the FBI to prove that Magic Lantern is the least intrusive of all practical measures the FBI could use to gather information in a timely and effective manner. Since the information gathering is for foreign intelligence purposes, law enforcement should obtain the warrant from the FISC, which has experience processing applications for warrants for foreign intelligence surveillance.

Courts should only permit exceptions to the warrant requirement in exigent circumstances. To ensure that this exception is limited, courts should define exigency narrowly.[64] One such narrow standard would limit exigency to only those circumstances where (a) there is probable cause to believe that a suspect is engaging in terrorist activities and (b) failure to install Magic Lantern immediately means law enforcement officials could not obtain the necessary intelligence to stop an impending terrorist attack. The exception is available only as long as the exigent situation continues to exist. After law enforcement has installed Magic Lantern on the suspect's computer, officers

---

62. *See* David Johnston & James Risen, *Officials Find No Clear Signs of Terrorism in Crash, but No Firm Answers, Either*, N.Y. TIMES, Nov. 13, 2001, at D9.

63. Formulating rules for using Magic Lantern for domestic crime-fighting purposes would involve balancing protection of civil liberties with crime prevention rather than national security and therefore may reach a different result.

64. Courts have tended to define exigency too broadly. *See, e.g.*, United States v. Rohrig, 98 F.3d 1506, 1519–25 (6th Cir. 1996) (finding that a neighbor's complaint of loud noise was an exigent circumstance).

should obtain a warrant from the appropriate court as soon as possible, and in no circumstance should the period between installing Magic Lantern and seeking a warrant last for more than one week.

Placing an upper limit on the time of surveillance will help limit Magic Lantern's potential intrusion on civil liberties. FISA generally limits warrants to ninety days.[65] The USA PATRIOT Act extends the period to 120 days.[66] Because Magic Lantern is potentially much more intrusive than a phone wiretap or similar surveillance techniques, warrants for Magic Lantern should carry a stricter time limitation. Law enforcement officials are free to ask the FISC for an extension, but the FISC needs to make another probable cause determination. If law enforcement officials can prove that the surveillance by Magic Lantern has revealed information that links the suspect to terrorism, a subsequent extension should last for a longer period of time than that of the initial warrant, obviating the need for law enforcement to constantly go to the court for extensions.

In the ideal situation, the FISC would require law enforcement officials to tailor Magic Lantern to intercept only those documents and messages that contain certain words or phrases, thus limiting the program's intrusion into civil liberties. However, in reality, having a minimization requirement is impractical. First, terrorists may communicate with each other in foreign languages, and it is infeasible to require law enforcement officials to create a comprehensive list of foreign and English words and phrases terrorists would use in their correspondence that is neither underinclusive nor overinclusive. Second, courts have tended to allow law enforcement broad discretion over the amount of surveillance even when there is a minimization requirement.[67] It therefore appears that minimization would serve no useful function but would increase the administrative costs of law enforcement. Since minimization is probably not feasible, to ensure that law

---

65. FISA § 105, 50 U.S.C. § 1805 (1994). In certain circumstances, the warrant can last for up to one year. *Id.* § 1802.

66. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, § 207, 115 Stat. 282 (2001) (amending 50 U.S.C. § 1805 (1994)) [hereinafter USA PATRIOT Act].

67. *See, e.g.*, United States v. Scott, 436 U.S. 128 (1978) (finding no violation of Title III's minimization requirement although sixty percent of the calls intercepted did not relate to the investigation, reasoning (1) most of those calls were short, (2) in a conspiracy case, it is often hard to determine the relevance of the calls before they were completed, and (3) a large number of the calls were ambiguous in nature); United States v. Rahman, 861 F. Supp. 247, 252–53 (S.D.N.Y. 1994) (finding the allegation that all calls were recorded, even if proven, was not a violation of FISA's minimization requirement, reasoning (1) many of the conversations were in Arabic, (2) coded or cryptic language was used, (3) there was not much time to detect patterns of innocent conversation, (4) conversations that sound innocent may be significant, and (5) greater flexibility in acquiring and storing information is necessary in gathering foreign intelligence).

enforcement does not use information irrelevant to the investigation, they should be obliged to discard any material revealed by the investigation that is irrelevant for intelligence purposes.

Furthermore, there should be restraints on using information found through the FBI's use of Magic Lantern in criminal trials. Both Congress and the courts have been more willing to allow surveillance for foreign intelligence than for domestic crimes.[68] In 1978, Congress enacted FISA and created a procedure for obtaining a warrant for surveillance for foreign intelligence reasons. The statute allows the government to introduce evidence found through the use of a FISA warrant in criminal trials only if the government's primary purpose for conducting the surveillance is to gather foreign intelligence.[69] However, the primary purpose test is unworkable in practice because it is rarely clear what the primary purpose of an investigation is. Often, several interests are at work. In addition, a law enforcement officer may easily claim that a surveillance's primary purpose is national security; it is difficult for courts to evaluate ex post the actual intention of the officer.

A better rule in both the Magic Lantern and FISA wiretap contexts is a bright line rule that allows prosecutors to use information obtained from either method only in those criminal proceedings related to espionage or terrorism. That way, law enforcement officials will have little incentive to ask for a warrant on intelligence grounds while really trying to obtain evidence for a conventional criminal trial. Without the fear that law enforcement officials will use an intelligence gathering warrant to obtain evidence for a criminal conviction, Congress can allow law enforcement officials to freely share the intelligence received from the surveillance with other agencies to prevent terrorist attacks. Sharing information among agencies is a useful way of preventing terrorism. For example, if the Federal Aviation Administration had access to the Central Intelligence Agency's terrorist watch list, it may have been able to prevent two of the hijackers from boarding the planes on September 11.[70]

In addition to greater restrictions on the use of surveillance information in criminal cases, appropriate forms of punishment are necessary to provide adequate incentives to deter law enforcement from

---

68. Before 1978, some lower courts had suggested that a warrant was not required for foreign intelligence surveillance. *See* United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973); United States v. Butenko, 494 F.2d 593, 605–06 (3d Cir. 1974). *But see* Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 156–57 (D.D.C. 1976).

69. The USA PATRIOT Act changed this standard. The new law requires only that foreign intelligence be a "significant purpose" of the wiretap. USA PATRIOT Act § 218, 115 Stat. 291 (amending 50 U.S.C. §§ 1804, 1823 (1994)).

70. *See* Dana Dillon & Paolo Pasicolan, *Beware the Jihad in Southeast Asia*, WALL ST. J., Jan. 17, 2002, at A14.

abusing the technology. Criminal sanctions in the form of fines, for example, may make officers think twice before installing Magic Lantern onto a person's computer. The magnitude of optimal fines for unwarranted surveillance should be high enough to counter the low probability of catching violations. Where monetary sanctions do not provide adequate deterrence, the statute should provide for the imprisonment of violators who show an intentional pattern of willful violations.

Such punishment will work to deter law enforcement agents only if courts would grant broad discovery powers to disclose the government's surveillance activity. In *Master v. FBI*,[71] the plaintiff filed suit to try to get access to alleged records that detailed illegal wiretapping. However, the court granted summary judgment to the FBI and found that "the plaintiffs contentions, while they may relate to whether the [FBI] is improperly withholding documents, fail to provide any support for the proposition that the [FBI] did not conduct a search reasonably calculated to uncover all relevant documents."[72] Similarly, in *ACLU v. Barr*,[73] the court held that the government did not have to deny allegations that the plaintiffs were the subjects of ongoing foreign intelligence surveillance under FISA.[74] While revealing surveillance may compromise national security, such rulings make it hard for suspects to determine if they are past or current targets of surveillance. In fact, courts could assist the suspect and, at the same time, maintain national security by ordering the government to reveal the existence or non-existence of surveillance in an in camera proceeding. The judge could then decide whether the surveillance was reasonable.

Finally, the statute authorizing keylogging programs such as Magic Lantern should have a sunset provision. Limiting the validity of the statute to five years, the length of time of the sunset provisions in the USA PATRIOT Act,[75] would force Congress to re-evaluate the balance struck between national security and civil liberties after Americans have had time to deal with the grief and shock associated with September 11. It would also force Congress to examine alternatives to Magic Lantern that achieve a better trade-off between effectiveness and minimal intrusion. Finally, it would permit Congress to look back over the five-year period and use actual data to gauge both the effectiveness of Magic Lantern and the threat posed by catastrophic terrorism.

71. 926 F. Supp. 193 (D.D.C. 1996).
72. *Id.* at 197.
73. 952 F.2d 457 (D.C. Cir. 1991).
74. *Id.* at 469.
75. USA PATRIOT Act § 224, 115 Stat. 295.

IV. CONCLUSION

September 11 highlighted the government's weakness in gathering foreign intelligence to adequately protect the nation. The advance of technology requires law enforcement agencies to develop and implement more powerful surveillance devices to keep up with sophisticated terrorists and criminals. We should carefully balance the national security benefits such technology brings against the civil liberties problems it causes. The line is a difficult one to draw, as demonstrated by the case of Magic Lantern. Perhaps the best we can do with new technologies such as Magic Lantern is to allow their use and, at the same time, ensure that limitations are imposed to minimize their intrusion into people's civil liberties.