UIC John Marshall Journal of Information Technology & Privacy Law

Volume 20
Issue 2 *Journal of Computer & Information Law - Winter 2002*

Article 4

Winter 2002

The "Magic Lantern" Revealed: A Report of the FBI's New "Key Logging" Trojan and Analysis of Its Possible Treatment in a Dynamic Legal Landscape, 20 J. Marshall J. Computer & Info. L. 287 (2002)

Neal Hartzog

THE "MAGIC LANTERN" REVEALED: A REPORT OF THE FBI'S NEW "KEY LOGGING" TROJAN AND ANALYSIS OF ITS POSSIBLE TREATMENT IN A DYNAMIC LEGAL LANDSCAPE

"You already have zero privacy anyway. Get over it."[1] Although this quip from Sun Microsystems CEO Scott McNealy seems extreme, it strongly illustrates the current tension between the power of technology and an individual's expectation of privacy.[2] This tension creates an incessant struggle, because for power of surveillance technology to increase, privacy must decrease, and vice versa. These struggles are best illustrated through the Federal Government's attempts to maintain national security through surveillance of communications and activities while attempting to sustain the legitimate expectations of privacy in the American people.[3] One of the most recent developments resulting from this quandary is the FBI's new enigmatic surveillance tool—a "keystroke logger" Trojan horse/computer worm they have dubbed "Magic Lantern."[4]

This surveillance tool was created to battle all crimes that utilize technology and information, especially crimes associated with terrorism to effectuate illegitimate ends.[5] Recent events have escalated the importance of "cyber intelligence" and have shifted the focus to domestic affairs in order to dispose of "sleeper cells," that is "small groups that live legally in the U.S. for years poised to [eventually] conduct terrorist attacks."[6] Historically, the FBI has been thwarted by certain counter-in-

1. Richard P. Cambell, *Addressing Myriad Issues of Privacy*, 23 Natl. L.J. C24 ¶ 1 (Aug. 6, 2001) (quoting Sun Microsystems CEO Scott McNealy, as he spoke to a group of reporters in 1999).

2. *Id.*

3. *Id.*

4. Dan Verton, CNN.com, *Feds Boost Online Surveillance Activity* ¶ 1 <http://www.cnn.com/2001/TECH/internet/12/11/online.surveillance.idg/index.html> (Dec. 11, 2001).

5. *Id.* at ¶ 2. *See generally* MSNBC Staff and Wire Reports, *FBI Confirms 'Magic Lantern' Exists* <http://www.msnbc.com/news/671981.asp> (Dec. 11, 2001).

6. Verton, *supra* n. 4, at ¶ 2.

telligence technologies, specifically encryption.[7] Magic Lantern would assist the FBI by recording the passwords used to encode/decode the encrypted messages, thereby permitting the Bureau to access the content of the otherwise indecipherable documents.[8] However, critics of the software raise serious concerns about the software's conflict with current laws, the Fourth Amendment,[9] and the public's reasonable expectation of privacy.[10]

Magic Lantern surfaced publicly in late November, 2001.[11] It is reported to have the capability to travel to a specific target via the Internet (e.g., e-mail) disguised as a Trojan horse/computer virus and install itself on the targeted personal computer and begin recording the keys typed on that computer.[12] The subject line of the Magic Lantern e-mail would encourage the user to open it – probably appearing as a note from family or friends.[13] Indeed, reports convey that "the recipient wouldn't even need to open the e-mail to install the file. So long as it lands in a mailbox, it can report."[14] However, due to the secretive nature of the software,[15] there is still a great degree of uncertainty regarding whether the program "would transmit keystrokes it records back to the FBI over the Internet or store the information to be seized later in a raid."[16] Some sources speculate that "Magic Lantern is a derivative of the Data Inter-

7. *See generally* Bob Port, *FBI's New Weapon a Lot Like a Virus*, N.Y. Daily News (Dec. 25, 2001) (available in 2001 WL 27307798). The FBI has stated that "encryption can pose potentially insurmountable challenges to law enforcement when used in conjunction with communication or plans for executing serious terrorist and criminal acts." Associated Press, *FBI Building 'Magic Lantern' To Monitor Computer Use*, Dow Jones International News ¶ 7 (Nov. 22, 2001) (available in WL 11/22/01 Dow Jones Int'l News 01:55:00) [hereinafter *FBI Building*].

8. *See generally* Port, *supra* n. 7. As a keystroke logger, Magic Lantern would be able to exploit "the weakness of any encryption system- when the message is being typed.". Matthew Fordahl, *Anonymous email Service Still Running After Sept. 11*, Associated Press Newswires ¶ 32 (Dec. 8, 2001) (available in WL, 12/8/01 APWIRES 15:46:00).

9. U.S. Const. amend. IV.

10. *See generally* Bob Sullivan, MSNBC.com, *FBI Software Cracks Encryption Wall* <http://www.msnbc.com/news/660096.asp?cpl=1> (Nov. 20, 2001).

11. *See generally id.*

12. MSNBC, *FBI Confirms*, *supra* n. 5, at ¶ 5. A Trojan horse is "a security-breaking program disguised as a benign program, such as a directory utility, game or email . . . . Viruses and worms infect host computers after being downloaded by the user. Both programs can reproduce and spread. A worm can spread automatically over the network from one computer to the next." John McElwaine, *Cyber Attacks*, 13 Feb. S.C. Lawyer 20, 22 (2002).

13. David Crocker, *Magic Lantern: Not the Name of an Opera* ¶ 2 <http://www.interfacenow.com/column.taf> (Dec. 21, 2001).

14. *Id.*

15. MSNBC, *FBI Confirms*, *supra* n. 5, at ¶ 2. FBI spokesman Paul Bresson stated that "we can't discuss [Magic Lantern] because it's under development." *Id.* at ¶ 3.

16. *FBI Building*, *supra* n. 7, at ¶ 10.

ception by Remote Transmission ("DIRT") program developed by Codexdatasystems."[17] If that speculation is correct, the reports imply that recorded keystrokes would be transmitted to the FBI and not stored for a later raid.[18] Other early reports support the "transmission" rumor.[19]

Although the existence of this software may seem implausible to many, according to some reports, "key loggers" have already been in use for a little over three years.[20] "Companies use keystroke loggers quite legally to keep an eye on their employees' behavior. Parents use them to monitor their children's activities online."[21] However, it is reported that the main purpose of Magic Lantern is to record passwords that the targets use to operate encryption software.[22] This encryption software scrambles incoming/outgoing messages with a complex code that the FBI previously has had great difficulties overcoming.[23] So although

> [e]ncryption keys are unbreakable by brute force. . .the keys themselves are only protected by the passphrase used to start the [encryption program]. If [the] agents can obtain that passphrase while typed into a computer by its owner, they can obtain the suspect's encryption key—similar to obtaining a key to a lock box which contains a piece of paper that includes the combination for a safe.[24]

Magic Lantern presents several difficult legal questions that are left unanswered due to new or non-existent statutes and case law directly pertaining to the unique situation that Magic Lantern creates.[25] The

---

17. Crocker, *supra* n. 13, at ¶ 2.

18. *Id.*

19. *See generally* Port, *supra* n. 7. "Magic Lantern is a program that records each keystroke made on a target computer and transmits that data to the bureau." *Id.* at ¶ 4; MSNBC, *FBI Confirms supra* n. 5, at ¶ 5. "Magic Lantern would allow the agency to gain that information without having to gain physical access to the computer." *Id.*

20. *See* Robert Lemos, CNET News.com, *FBI Snoop Tool Old Hat for Hackers* ¶ 1 <http://news.cnet.com/news/0-1003-200-7944351.html?tag=prntfr> (Nov. 21, 2000). "Several hacking tools, the two most popular being Back Orifice and SubSeven, allow full control over a remote PC infected by the program, including keystroke logging and even recording a conversation if a microphone is connected to the PC. Both programs have been incorporated into Trojan horses and are several years old." *Id.* at ¶ 11.

21. David Coursey, *Keep Yourself Top Secret! How to Defeat Spyware (Part 2)* ¶ 2 (Jan. 3, 2002) (available in 2002 WL 5880066).

22. *See* Sullivan, *supra* n. 10, at ¶ 10. Reportedly, Magic Lantern will watch "for a suspect to start a[n]. . .encryption program. . . It then logs the passphrase used to start the program, essentially giv[ing] agents access to keys needed to decrypt files." *Id.*

23. *See* Port, *supra* n. 7, at ¶¶ 13-15. "Encrypted email has bedeviled the FBI for years." *Id.* at ¶ 14. *See* Jovi Tanada Yam, *Lawyer.com Worst Tech Product of 2001?* (Dec. 27, 2001) (available in 2001 WL 31372969). "The FBI has always fretted openly about encryption technology's ability to help criminals and terrorists hide their work in the dark." *Id.* at ¶ 7.

24. Sullivan, *supra* n. 10, at ¶ 11.

25. *See generally* Lemos, *supra* n. 20.

first concern is statutory. It is unclear what laws, if any, will apply when Magic Lantern is put into use.[26] The recent terrorist attacks in the United States have brought the need for information as a matter of national security to the forefront. Congress recently passed legislation (i.e. *USA PATRIOT Act*)[27] that dramatically modifies current surveillance law, thus further complicating the untested waters of a new surveillance method with an undeveloped statutory scheme that would potentially regulate that method.[28] In addition, it is uncertain whether Magic Lantern can legally operate under the authority of a search warrant, requiring a relatively low burden of proof, or whether it will have to obtain a wiretap, with a high burden of proof, in order to conduct surveillance.[29]

The second concern is constitutional. If the FBI only obtained authorization to record a certain kind of information, and the keystroke logger recorded every keystroke entered by the target whether it regarded the information sought or not, then it is possible that the software could result in overly broad searches in violation of the Fourth Amendment.[30]

By considering the only recorded case dealing with a technology similar to Magic Lantern, Section I of this comment will develop the dynamic legal environment Magic Lantern is entering, as well as outline a sister software to Magic Lantern, also created by the FBI, that was known as "Carnivore."[31] Section II of this comment analyzes the constitutional questions Magic Lantern presents within the context of the Fourth Amendment.[32] It focuses the possible violations of search and seizure, invasion of privacy, and over-broad searches.[33] Section III explores the statutes that might apply to Magic Lantern and discusses the new niche that the software has carved, for it does not clearly fit into many of the laws that deal with electronic surveillance.[34] Specifically, Section III will examine such statutes as the *Electronic Communications Privacy Act* ("ECPA"),[35] the *Foreign Intelligence Surveillance Act*

26. *Id.* at ¶ 17.

27. *See infra* Part IIIC.1 for further discussion.

28. *See generally Stefanie* Olsen, CNET News.com, *Patriot Act Draws Privacy Concerns* <http://news.cnet.com/news/0-1005-200-7671240.html?tag=prntfr>) (Oct. 26, 2001); *see infra* Parts III.B., IIIC for further discussion.

29. *See generally U.S. v. Scarfo,* 180 F. Supp. 2d 572 (D.N.J. Dec. 26, 2001); *see* Crocker, *supra* n. 13, at ¶ 5.

30. *See* Sullivan, *supra* n. 10, at ¶¶ 14-16.

31. Crocker, *supra* n. 13, at ¶ 2.

32. U.S. Const. amend. IV.

33. *Id.*

34. 18 U.S.C.S. §§ 2510-2520, 2701-2709 (Lexis L. Publg. 2001); 50 U.S.C.S. §§ 1801 et. seq. (Lexis L. Publg. 2001); Pub. L. No. 107-56, 2001 H.R. 3162 (2001).

35. 18 U.S.C.S. §§ 2510-2520, 2701-2709.

("FISA"),[36] the *USA PATRIOT Act*,[37] and others that might substantially bear on the use of Magic Lantern. Section IV briefly confronts the practical dilemmas that Magic Lantern faces, such as its coexistence with anti-virus software programs and its foreign government quagmire.[38] Section V attempts to resolve the ambiguities surrounding Magic Lantern and suggests how Magic Lantern will be treated in the future.

I. *UNITED STATES v. SCARFO* AND THE FBI'S SPYWARE KNOWN AS "CARNIVORE." MAGIC LANTERN'S TWO CLOSEST RELATIVES.

Presently, there is no case that deals explicitly with key-logging software that operates in the exact fashion of Magic Lantern, specifically a technology that is planted via the Internet on a target's computer disguised as a Trojan/virus, and transmits data back to the FBI.[39] However, on December 26, 2001 the District Court for the District of New Jersey passed judgment in a case of first impression involving another form of key-logging technology used by the FBI.[40] In *United States v. Scarfo*, the district court denied a challenge to the introduction of evidence that was obtained with assistance from a key-logger system physically installed on the defendant's computer.[41] The opinion discusses many of the issues that will apply to the use of Magic Lantern, including a possible over-collection of data that would mandate a general warrant that is violative of the Fourth Amendment[42] and whether the Key Logger System ("KLS") intercepted wire communications.[43]

In *Scarfo*, the FBI, "acting pursuant to federal search warrants," entered Nicodemo S. Scarfo's business office "to search for evidence of an illegal gambling and loansharking operation."[44] They searched Scarfo's personal computer, but could not access certain encrypted files, which they suspected contained the evidence for which they were searching.[45]

---

36. 50 U.S.C.S. §§ 1801 et. seq.

37. *See generally Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Pub. L. No. 107-56, 2001 H.R. 3162 (2001) [hereinafter *USA PATRIOT Act*].

38. Crocker, *supra* n. 13, at ¶ 3.

39. *Id.* at ¶ 2.

40. *Scarfo*, 180 F. Supp. 2d at 574. "It appears that no district court in the country has addressed a similar issue." *Id.*

41. *Id.* "This case presents an interesting issue of first impression dealing with the ever-present tension between individual privacy and liberty rights and law enforcement's use of new and advanced technology to vigorously investigate criminal activity." *Id.*

42. *Id.* at 576; U.S. Const. amend. IV.

43. *Scarfo*, 180 F. Supp. 2d at 574-75.

44. *Id.* at 574.

45. *Id.*

After obtaining two search warrants,

> the F.B.I. returned to the location, . . . and installed what is known as a 'Key Logger System' ('KLS') on the computer and/or computer keyboard in order to decipher the passphrase to the encrypted file, thereby gaining entry to the file. The KLS records the keystrokes an individual enters on a personal computer's keyboard.[46]

The KLS then recorded the passphrases to the encrypted file as Scarfo typed them, consequently giving the FBI access to "what [was] alleged to be incriminating evidence."[47]

After Scarfo was indicted, "he filed [a] motion for discovery and to suppress the evidence recovered from his computer,"[48] alleging that the "KLS constituted an unlawful general warrant in violation of the Fourth Amendment" and that it "effectively intercepted a wire communication in violation of [ECPA] Title III, 18 U.S.C. § 2510."[49] The trial judge, after being exposed to all of the functions of the key-logger,[50] rejected Scarfo's claim that "the warrants were written and executed as general warrants. . .", primarily based on the theory that although the key-logger may record some information not prevalent to the criminal investigation, "no tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision."[51] The discussion on general warrants and the Fourth Amendment[52] in this case will be included and analyzed in detail in Section II of this comment.

Addressing Scarfo's statutory argument, the judge stated that "the principal mystery surrounding this case was whether the KLS inter-

---

46. *Id.*

47. *Id.*

48. *Id.*

49. *Id.* at 576. The defendant's also challenged the court's ruling concerning the government's discovery procedures and invocation of the *Classified Information Procedures Act*, 18 U.S.C. app. III §§ 1 *et seq.* (1980). *Id.* at 575.

50. *Id.* at 574. The government claimed shelter under the act after refusing to comply with a court order to submit a report "explaining fully how the KLS device functions and describing the KLS technology and how it works vis-à-vis the computer modem, Internet communications, email and all other uses of a computer." *Id.* at 575. The government then submitted a modified brief claiming that "disclosure of the KLS would jeopardize both ongoing and future domestic criminal investigations and national security interests." *Id.* After the court held an *in camera, ex parte* hearing where the FBI presented the court with "detailed and top-secret, classified information regarding the KLS, including how it operates in connection with a modem," the court found that "the government made a sufficient showing to warrant the issuance of an order protecting against the disclose of the classified information." *Id.* The issues of national security, evidence in criminal trials, and the application of the Classified Information Procedures Act will more than likely apply to Magic Lantern as well, due to the software's classified and developmental status. *See generally* MSNBC, *FBI Confirms, supra* n. 5.

51. *Scarfo*, 180 F. Supp. 2d at 578 (quoting *U.S. v. Conley*, 4 F.3d 1200, 1208 (3d Cir. 1993) (quoting *U.S. v. Christine*, 687 F.2d 749, 760 (3d Cir. 1982))).

52. U.S. Const. amend. IV.

cepted a wire communication in violation of the wiretap statute by recording keystrokes of e-mail or other communications made over a telephone or cable line while the modem operated."[53] The judge limited the inquiry as such because "[t]hese are the only conceivable wire communications which might emanate from Scarfo's computer and potentially fall under the wiretap statute."[54] The judge went on to rule that "upon a careful and through review of the classified information provided . . . the KLS technique. . . did not intercept any wire communications and therefore did not violate the wiretap statute."[55] Section III of this comment will further expound upon the ECPA[56], the role it played in *Scarfo*[57], and how it might apply to Magic Lantern. In explaining why the KLS didn't violate the ECPA,[58] the judge stated, "I am satisfied that the KLS did not operate during any period of time in which the computer's modem was activated."[59] The judge relied primarily on reports from the FBI that stated the software was configured to intentionally avoid "real time" interception of communication transmitted via the Internet.[60] The judge's ruling hinged on this decision, and "[a]ccordingly, the defendant's motion to suppress evidence for violation of Title III [was] denied."[61] Section III of this comment will further expound upon the ECPA, the role it played in *Scarfo*, and how it might apply to Magic Lantern.

Although the *Scarfo*[62] decision sets strong precedent for Magic Lantern, the case still leaves numerous stones unturned. The case gives good insight into how Magic Lantern will be treated by the courts if Magic Lantern, like the Key Logger System used in *Scarfo*, does not report any information that entered or exited through the modem.[63] However, as previously reported, it seems probable that Magic Lantern *will* transmit its information over the Internet; the remaining details of the software are either being developed or treated as classified.[64] Such fine threads are subject to close judicial scrutiny when put within the context of statutory interpretation. Section II and Section III will explore these issues further.

---

53. *Scarfo,* 180 F. Supp. 2d at 581.
54. *Id.*
55. *Id.*
56. 18 U.S.C.S. §§ 2510-2520, 2701-2709.
57. *Scarfo,* 180 F. Supp. 2d at 581.
58. 18 U.S.C.S. §§ 2510-2520, 2701-2709.
59. *Id. See infra* Section III and accompanying text.
60. *Scarfo,* 180 F. Supp. 2d at 581.
61. *Id.* at 582.
62. *See id.*
63. *Id.* at 581.
64. *See* MSNBC, *FBI Confirms,* supra n. 5, at ¶ 1.

Although *Scarfo*[65] was the first case to deal with Key Logging technology, Key Logging technology was not the first technology that the FBI has employed for electronic communication surveillance purposes.[66] "Last year, the FBI touched off a furor with its use of e-mail monitoring technology known as Carnivore."[67] The software, now known as DCS 1000,[68] is a system used "to implement court-ordered surveillance of electronic communication. It is used when other implementations. . . do not meet the needs of the investigators or the restrictions placed by the court."[69] Magic Lantern and Carnivore are similar in that they both record electronic information and report back to the FBI.[70] However, their differences may greatly affect their statutory treatment. In order to use Carnivore, the FBI must get permission according to the ECPA (Title III of the *Omnibus Crime Control and Safe Streets Act*)[71] or the FISA[72] to place a wiretap on the communications carrier, usually an Internet Service Provider or "ISP" such as AOL or CompuServe.[73] Because the use of Carnivore requires a wiretap order which is more difficult to obtain than a general search warrant, when Carnivore is put into action "[l]aw enforcement agents follow a rigorous, detailed procedure to obtain court orders and surveillance is performed under the supervision of the court issuing the order."[74] The Carnivore "clearance process" illustrates well how the wiretap/general search warrant distinction will prove critical in determining what kind of authority law enforcement officials will have to gain in order to implement Magic Lantern on a target's computer.[75]

Like Magic Lantern, Carnivore has also been the subject of much criticism and concern relating to its invasive nature and Constitutional

---

65. *Scarfo*, 180 F. Supp. 2d at 574.

66. *See generally* William Matthews, Federal Computer Week, *FBI's Key Logger Under Scrutiny* <http://www.fcw.com/fcw/articles/2001/0813/news-fbi-08-13-01.asp> (Aug. 9, 2001).

67. *Id.* at ¶ 13.

68. Lemos, *supra* n. 20, at ¶ 15.

69. Thomas Gregory Motta, *Government and Electronic Privacy: Trends in Law Enforcement, Investigatory Tools and Protection of National Security*, 632 PLI/PAT 631, 642 (Jan. 2001).

70. Crocker, *supra* n. 13, at ¶ 2.

71. 18 U.S.C. §§ 2510-22 (2001).

72. 50 U.S.C. §§ 1801-29 (2001).

73. *See* Motta, *supra* n. 69, at 654. "The FBI is placing a black box inside the computer network of an ISP." *Id. See* Eric Manton M. Grier, Jr., Student Author, *The Software Formerly Known As "Carnivore": When Does Email Surveillance Encroach Upon a Reasonable Expectation of Privacy?*, 52 S.C. L. Rev. 875 (2001). "It is the FBI's latest email surveillance technology—a software program housed in a computer unit and attached to an Internet Service Provider, such as American Online." *Id.*

74. *See* Motta, *supra* n. 69, at 642.

75. *Scarfo*, 180 F. Supp. 2d at 578.

validity,[76] specifically in the environment of over broad searches.[77] So, although Magic Lantern and Carnivore are substantially different electronic surveillance devices that likely will be treated differently[78] under respectively applicable statutes, in some aspects their fates could be intertwined.

II. THE CONSTITUTIONAL IMPLICATIONS OF MAGIC LANTERN.

"There is no provision in the United States Constitution that specifically establishes or enumerates a general right to privacy. Notwithstanding, there are several provisions of the Bill of Rights or First Ten Amendments to the U.S. Constitution that imply. . .aspects of privacy protection in the context of the amendment."[79]

The specific component of the Constitution which most relates to Magic Lantern is the Fourth Amendment.[80] The Fourth Amendment grants to the people the right "to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, [and that those rights] shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[81] As a threshold question, whether Magic Lantern is going to implicate the Fourth Amendment will turn, then, on whether its consequent recording of keystrokes and transmission of data back to the FBI qualifies as a "search and seizure" under the meaning of the amendment.[82]

"In determining whether a particular form of government initiated electronic surveillance is a 'search' within the meaning of the Fourth Amendment, [the court's] lodestar is *Katz v. United States.*"[83] In *Katz,*[84] the FBI attached an electronic listening and recording device to a public telephone booth, recorded the contents of conversations and entered the dialogue into evidence against the speaker.[85] The FBI argued that there

76. *See e.g.* Sullivan, *supra* n. 10, at ¶ 14. *See generally* William Mathews, Federal Computer Week, *Senate OK's Easier Use of Carnivore* <http://www.fcw.com/fcw/articles/2001/0917/news-fbi-09-17-01.asp> (Sept. 17, 2001). "Critics have labeled Carnivore a sweeping invasion of privacy" *Id.* at ¶ 4.

77. *See generally id.*

78. *See* Sullivan, *supra* n. 10, at ¶¶ 7,8.

79. Eugene J. Yannon, *Privacy Law*, 34 Md. B.J. 24, 27 (Nov./Dec. 2001)

80. U.S. Const. amend. IV.

81. *Id.*

82. *See id.*

83. *Smith v. Md.*, 442 U.S. 735 (1979) (citing *Katz v. U.S.*, 389 U.S. 347 (1967)).

84. *Katz*, 389 U.S. at 347.

85. *Id.* at 348.

could be no violation of the Fourth Amendment "because '[t]here was no physical entrance into the area occupied by, [Katz].'"[86] The Court rejected this "physical" test used to determine whether a "search" had occurred, replacing it with a new test that rested on an individual's reasonable "expectation of privacy."[87] The Court outlined the test by presenting two requirements that must be met before a citizen may properly invoke the Fourth Amendment.[88] The first is "that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[89]

Using the "reasonable expectation of privacy"[90] test, the Court held, specifically that "a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies [a telephone booth], shuts the door behind him, and pays the toll. . . is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[91] Using this logic, the Court held that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[92]

The test developed in *Katz*[93] as applied to Magic Lantern poses an interesting question that courts must eventually answer: Does an individual have a reasonable expectation of privacy in the keystrokes that he enters into his computer? Keystrokes are used to compose e-mails, type "real-time" messages over an "instant messenger," and—at the heart of the matter—type passwords, which, by their nature necessitate secrecy. Considering this, there appears to be a strong presupposition that an individual has a reasonable expectation of privacy in the keystrokes made while using a computer.[94]

However, in *Smith v. Maryland*[95] the Supreme Court, using the test

86. *Id.* at 349.

87. *Id.* at 361 (Harlan, J., concurring). "[T]he Fourth Amendment protects people, not places." *Id.* at 351.

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

89. *Id.*

90. *Id.* at 351.

91. *Id.* at 352.

92. *Id.* at 353.

93. *See generally id.*

94. *Id.*

95. *See generally Smith,* 442 U.S. 735. In *Smith*, the police used a pen register to trace the calls of a man suspected of robbery. *Id.* They "did not get a warrant or court order before having the pen register installed." *Id.* at 737. The suspect was subsequently arrested and in a pretrial motion and in a pretrial motion "sought to suppress 'all fruits de-

developed in *Katz*,[96] held that the installation and use of a pen register ("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"[97]) did not violate an individual's "reasonable expectation of privacy."[98] Consequently, "the installation and use of a pen register. . .was not a "search" [for the purposes of the Fourth Amendment] and no warrant was required."[99] The Court in *Smith*[100] distinguished pen registers from the device used in *Katz* by pointing out that "pen registers do not acquire the *contents* of communications."[101] Providing support for the conclusion that pen registers do not violate a reasonable expectation of privacy, the Court doubted "that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[102] The Court went on to say that "although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."[103]

Although the Court concluded in *Smith*[104] that a pen register, which is a device similar to Magic Lantern, in that they both record the pushing of buttons and keystrokes, did not violate an individual's reasonable expectation of privacy, the Supreme Courts' decision only further serves to support Magic Lantern's presupposition supported by *Katz*[105]—that an individual has a reasonable expectation of privacy in the keystrokes made while using a computer.[106] *Smith*[107] noted the difference between surveillance devices that trace and ones that record content, holding that the use of content *recording* technologies is more likely to be seen as violating a "reasonable expectation of privacy."[108] The Court went so far as to assert that "the broad and unsuspected governmental incursions into

---

rived from the pen register' on the ground that the police had failed to secure a warrant prior to its instillation." *Id.* at 738.

96. *See generally Katz,* 389 U.S. 347.

97. *Id.* at 736 (quoting *U.S. v. N.Y. Tel. Co.*, 434 U.S. 159, 161 n. 1 (1977)).

98. *Smith*, 442 U.S. at 745-46.

99. *Id.*

100. *Id.* at 746.

101. *Id.* at 741.

102. *Id.* at 742.

103. *Id.* at 743.

104. *See generally id.*

105. *See generally Katz,* 389 U.S. 347.

106. *See generally Smith,* 442 U.S. 735.

107. *Id.* at 741.

108. *Id.*

conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."[109] Magic Lantern most likely will be classified as a "content" recorder: the keys are used to compose words (passwords) and sentences.[110] Although, due to the publicity of cookies, spyware, and the like, the public in general might expect that companies, individuals, and the government might be monitoring their internet connection, it seems unlikely that the public would expect or have knowledge that the keystrokes they used to compose their financial information, private digital diaries, and their passwords are being recorded by the government.[111] Assuming that, at the very least, Magic Lantern records passwords, and applying the rationale used by the Courts in *Smith*[112] and *Katz*,[113] it appears likely that, when Magic Lantern is put into use by the FBI, the recorded keystrokes will be seen as a "search" under the meaning of the Fourth Amendment,[114] and, consequently, the FBI must follow the appropriate statutory procedure in order to obtain authority for its use.

The issue, it seems, will be left to the courts. The only case on sufficiently on point to provide guidance is *United States v. Scarfo*.[115] However, the issue of whether the KLS is a "search and seizure" for purposes of the Fourth Amendment was not addressed in *Scarfo*[116] because the FBI obtained a search warrant to use the KLS on Scarfo's computer.[117] The issue in Scarfo's case then became whether the warrants authorizing the use of KLS were general warrants violative of the Fourth Amendment because "the government had the ability to capture and record only those keystrokes relevant to the 'passphrase' to the encrypted file, and because it received an unnecessary over-collection of data[.]"[118]

Once an activity is deemed to be a "search" within the meaning of the Fourth Amendment, law enforcement officers must then obtain a search warrant to proceed with the activity.[119] "Where a search warrant

109. *Id.* at 746.

110. Crocker, *supra* n. 13, at ¶ 2.

111. *See generally In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 507 (S.D.N.Y. 2001). "Cookies are computer programs commonly used by Web sites to store useful information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner." *Id.* at 502, 503. Websites typically "store this information on the users hard drive" until the websites administrators "access the cookies and [upload] the data." *Id.* at 503.

112. *Smith*, 442 U.S. 735.

113. *Katz*, 389 U.S. 347.

114. U.S. Const. amend. IV.

115. *See generally Scarfo*, 180 F. Supp. 2d 572.

116. *Id.*

117. *Id.* at 574. "[T]he F.B.I. returned to the location and , pursuant to two search warrants, installed what is known as a "Key Logger System" ("KLS") on the computer" *Id.*

118. *Id.* at 576.

119. *See generally Johnson v. U.S.*, 68 S. Ct. 367 (1948).

is obtained, the Fourth Amendment requires a certain modicum of particularity in the language of the warrant with respect to the area and items to be searched and/or seized."[120] The court in *Scarfo* stated that "[t]he particularity requirement exists so that law enforcement officers are constrained from undertaking a boundless and exploratory rummaging through one's property."[121]

The ruling in *Scarfo* that the KLS did not violate the Fourth Amendment[122] could prove important to the legal treatment of Magic Lantern concerning general warrants because it appears that for the purposes of the Fourth Amendment, the two technologies perform analogous, and nearly identical functions.[123] Both technologies run the risk of performing "over broad" searches.[124] In *Scarfo,* the court focused on the specificity of the search warrant, stating "it is clear that the Court Orders suffer from no constitutional infirmity with respect to particularity."[125] The court further stated that "[o]n its face, the Order is very comprehensive and lists the items, including the evidence in the encrypted files, to be seized with more than sufficient specificity."[126] This statement would indicate that if the FBI obtained a detailed search warrant or wiretap order to use Magic Lantern with a comprehensive list of items to be searched that it would, at least in the view of some courts, withstand a Fourth Amendment general warrant challenge.[127]

The court goes on to pronounce that the fact that the KLS recorded keystrokes other "than the searched for passphrase" does "not. . .convert the limited search for the passphrase into a general exploratory search."[128] In expounding on the rationale justifying the KLS non-specified interception (and consequently building support for the constitutional use of Magic Lantern), the *Scarfo* court reasoned that "[d]uring many lawful police searches, police officers may not know the exact nature of the incriminating evidence sought until they stumble upon it."[129] The court then analogized that "[j]ust like searches for incriminating

120. *Scarfo*, 180 F. Supp. 2d at 576 (*citing Tores v. McLaughlin*, 163 F.3d 169, 173 (3d Cir. 1988)).

121. *Id.* (*citing U.S. v. Johnson*, 690 F.2d 60, 64 (3d Cir. 1982) (*citing Coolidge v. N.H.*, 403 U.S. 443, 467 (1971))).

122. *Scarfo*, 180 F. Supp. 2d at 578.

123. *See* Sullivan, *supra* n. 10, at ¶ 9.

124. *Id.* at ¶ 14.

125. *Scarfo*, 180 F. Supp. 2d at 577.

126. *Id.* (citing *Andersen v. Md.*, 427 U.S. 463, 480-81 (1976)). In *Andersen*, the "defendant's general warrant claim was rejected where [the] search warrant contained, among other things, a lengthy list of specified and particular items to be seized." *Id.* (citing *Andersen v. Md.*, 427 U.S. 463, 480-81 (1976)).

127. *See generally id.*

128. *Id.* at 578.

129. *Id.*

documents in a closet or filing cabinet, it is true that during a search for a passphrase "some innocuous [items] will be at least cursorily perused in order to determine whether they are among those [items] to be seized."[130] Consequently, the court reasoned, "law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence which is properly specified in the warrant."[131] The court then cited to the Supreme Court decision of *Anderson v. Maryland*[132] quoting "the complexity of an illegal scheme may not be used as a shield to avoid detection when the [government] has demonstrated probable cause to believe that a crime has been committed and probable cause to believe that evidence of this crime is in the suspect's possession."[133] The court then concluded that the warrants authorizing the KLS were not written and executed as general warrants.[134]

The ruling in *Scarfo*[135] outlines the legal theory that the FBI must adhere to if the use of Magic Lantern is going avoid falling into the category of "general warrant."[136] If the FBI obtains a warrant to use Magic Lantern and the warrant names, with sufficient specificity, the items to be searched, then following the holding in *Scarfo*, such a warrant would avoid violation of the Fourth Amendment as a general warrant.[137] Therefore, if Magic Lantern intercepts communications that were not specifically listed in the warrant, the courts should allow a certain amount of flexibility in order for the FBI to determine whether the communications are among the items sought.[138] However, as with the use of any surveillance tool capable of abuse, if law enforcement officials fail to stay within the letter of the law regarding the use of Magic Lantern and begin to abuse their authority, the court's flexibility in acquiescing to an over-collection of information could quickly expire, making a constitutional use of Magic Lantern both difficult and fruitless.[139]

---

130. *Id.* (*citing U.S. v. Conley*, 4 F.3d 1200, 1208 (3d Cir. 1993)). "[N]o tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision." (*quoting U.S. v. Christine*, 687 F.2d 749 (3d Cir. 1982) *Id.*

131. *Scarfo*, 180 F. Supp. 2d at 578.

132. *Anderson*, 427 U.S. at 482.

133. *Id.* (*citing Anderson* 427 U.S. at 482).

134. *Scarfo*, 180 F. Supp. 2d at 578.

135. *See generally id.*

136. *Id.* at 576.

137. *Id.*

138. *Id.*

139. *See generally id.* The court in *Scarfo* ultimately passed judgment on the specifications of the warrant, the technology of the KLS, and the ability of the KLS to remain within existing law. *See generally id.* This would seem to indicate that the constitutionality of Magic Lantern is dependant on the specifications of the warrant, technology, and how it is put to use. *See generally id.*

III. MAGIC LANTERN AND STATUTORY LAW

The body of statutory law governing surveillance, privacy, and the Federal government's involvement with interception of electronic communications is massive, cryptic, dynamic and, due to the recent passage of the *USA PATRIOT Act*,[140] untested.[141] It is unclear which laws, if any, will apply to Magic Lantern once it has been put into use. Arguably, the determination of which statutes will be deemed applicable to Magic Lantern will rest on the determination of whether Magic Lantern will be found legally to "intercept wire communications."[142] If Magic Lantern is deemed to "intercept wire communications," thus classifying it as a "wiretap," then it will fall under the umbrella of such acts as the ECPA,[143] the FISA of 1978 ,[144] and possibly the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* ("USA PATRIOT Act").[145] The purpose of this section is to analyze the language and interpretation of the statutes that could possible be relevant to Magic Lantern and to analyze the likelihood of the statute's applicability.

A. THE *ELECTRONIC COMMUNICATIONS PRIVACY ACT* ("ECPA")[146]

In 1986, the ECPA "was enacted to amend Title III of the *Omnibus Crime Control and Safe Streets Act of 1968* [also known as the *"Federal Wiretap Act"*], which authorized court-ordered government wiretapping."[147] "Court orders described by and issued under the *Federal Wiretap Act* [that was modified by the ECPA] are known as Title III warrants."[148] The ECPA protects against unauthorized access, interception, or disclosure of private communications by the government as well as by individuals and third parties."[149] The ECPA is divided into two parts, "Title I of the ECPA restricts the interception of oral, wire, and electronic communications while in transit, and Title II pertains to the

140. *U.S.A. PATRIOT Act*, Pub. L. No., 107-56, 2001 HR 3162.

141. The *U.S.A. PATRIOT Act* was passed October 26, 2001, and at the time of composition of this comment, no cases had challenged it. *See generally id.*

142. *See generally* 18 U.S.C. § 2510 (2001).

143. *Electronic Communications Privacy Act of 1986*, Pub. L. No. 99-508, 100 Stat. 1851, 1859-1868 (codified as 18 U.S.C. §§ 2510-2522, 2701-2711 (2001)).

144. *Foreign Intelligence Surveillance Act of 1978*, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-11863 (1994 & Supp. V 1999)).

145. *U.S.A. PATRIOT Act*, Pub. L. No., 107-56, 2001 HR 3162.

146. 18 U.S.C.S. §§ 2510-2522, 2701-2711.

147. *U.S. v. Reyes*, 922 F.Supp. 818, 836 (S.D.N.Y. 1996).

148. *Id.* at 836 n.18.

149. Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 S.D. L. Rev. 1153, 1197 (1997).

acquisition and disclosure of stored communications."[150] Title I outlaws the interception of electronic communications and "Title II, also known as the *Stored Communications Act*, bars unauthorized "access" to stored electronic communications."[151] Due to the language of the statute and the novelty of Magic Lantern, it is unclear if either Title I or Title II would apply to the FBI's most recent surveillance device.

The importance of whether the ECPA (also referred to as "Title III")[152] will govern Magic Lantern when it is put to use lies in the heightened difficulty of obtaining authorization for surveillance under the ECPA, opposed to the procedure for obtaining a search warrant.[153] "A surveillance order, the authorization that Congress created for law enforcement to legally conduct a wiretap, bears many similarities to a search warrant, which it is essentially modeled after."[154] However, the surveillance order is much more difficult to obtain than a general search warrant, which only requires probable cause.[155] In order to obtain a sur-

150. *Id.* Title I is located in 18 U.S.C. §§ 2510-2521 of the *Electronic Communications Privacy Act* of 1986. Title II is located in 18 U.S.C. §§ 2701-2710 of the *Electronic Communications Privacy Act* of 1986.

151. *Recent Case, Federal Statutes—Electronic Communications Privacy Act of 1986-Ninth Circuit Holds that the Wiretap Act Protects Electronic Communications in Storage to the Same Extent as Those In Transit.—Konop v. Hawaiian Airlines 236 F.3d 1035 (9th Cir. 2001)*, 114 Harv. L. Rev. 2563, 2563 (2001) [hereinafter *Recent Case*].

152. The ECPA modified Title III of the *Omnibus Crime Control and Safe Streets Act of 1968* (18 U.S.C. §§ 2510-2522). Consequently, the two Acts are referred to in the collective as "Title III."

153. Melissa J. Annis, U.SA. Attorneys' Bulletin, *Electronic Surveillance: Does it Bug You?* (Sept. 1997).

154. Mark G. Young, Student Author, *What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance*, 70 Fordham L. Rev. 1017, 1058 (2001).

155. Annis, *supra* n. 153, at 34.

> Congress has outlined very strenuous requirements for the lawful application, interception, and use of electronic surveillance, given the nature of the intrusion in wire, oral, and electronic interceptions. For example, applications to intercept communications under Title III must be authorized by the Attorney General, Associate Attorney General, Deputy Attorney General, Assistant Attorney General, or a Deputy Assistant Attorney General in the Criminal Division of the Department of Justice [[18 U.S.C.] 2516(1)]. Without the proper authorizations, the evidence will be suppressed. Search warrants require some specificity, but Title II requires that an application to intercept communications include: (1) the identity of the investigative or law enforcement officer submitting the application [§ 2518(1)(a)]; (2) a full and complete statement of the facts relied upon to conclude there is probable cause [§ 2518(1)(d)]: (3) details as to the alleged offenses [§ 2518(1)(b)]; (4) details as to the nature and location of the facilities from which or where the communications are to be intercepted [§ 2518(1)(b)]; (5) a particular description of the type of communications to be intercepted [§ 2518(1)(b)]; (6) the identity of the persons (if known) committing the offense(s) and the persons whose communications are to be intercepted ("named interceptees") [§ 2518(1)(b)]; (7) a full and complete statement of whether other investigative procedures have been tried and failed or why they appear unlikely to succeed or are too dangerous to employ [§ 2518(1)(c)]; (8) a statement of the period of time for which the interception is to

veillance order, the application to intercept communications must include an extremely detailed and tailored list of all targets and communications to be intercepted.[156] In addition, the application must come from the U.S. Attorney General's office, must be approved by a Federal judge or magistrate, and all other investigative techniques must have been proven unsuccessful, potentially unsuccessful, or too dangerous.[157] This difficult process illustrates the gravity of the ECPA's applicability to the use of Magic Lantern.

The question of the ECPA's applicability to Magic Lantern will more than likely hinge on the construction and application of particular definitions within § 2510.[158] The terms "wire communication," "intercept," "electronic communication," "electronic storage" and "aural transfer" are of particular and specific importance.[159] Section 2511 of the ECPA criminalizes the interception of any "wire, oral, or electronic communication."[160] Section 2510 defines "wire communication" as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception. . .affecting interstate or foreign commerce."[161] The definition of "aural transfer" is "a transfer containing the human voice at any point between and including the point of origin and the point of reception."[162] Consequently, Magic Lantern would not be classified as a "wire communication" for the purposes of the ECPA, as it does not record the human voice, but instead, only records keystrokes.[163] Because of the nature of Magic Lantern, under the statute, it would not be classified as "Oral Communication" because recording keystrokes would not likely be classified as "oral."[164]

The remaining form of "communication" in the statute is "electronic communication," and is likely the form of communication most applicable to Magic Lantern. "Electronic Communication" is defined as "any

---

be conducted. . .(9) a statement of prior applications to intercept the same person, place, or facility, including the action taken by the court for each application [§ 2518(1)(e)]

Id.

156. 18 U.S.C. § 2518(1)(a-f); *see Recent Case, supra* n. 151.

157. 18 U.S.C. § 2518(3)(c); *see Recent Case, supra* n. 151.

158. *See generally* 18 U.S.C. § 2510.

159. *See id.*

160. *Id.* § 2511(1)(a).

161. *Id.* § 2510(1).

162. *Id.* § 2510(18).

163. Crocker, *supra* n. 13, at ¶ 2.

164. *Id.* § 2510(2). "'[O]ral' communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." *Id.; see U.S. v Carroll,* 332 F Supp. 1299 (D.D.C. 1971).

transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce[.]"[165] Without knowing the exact specifics of how and when Magic Lantern records the keystrokes, it is difficult to tell whether it will fall within the definition, but presumptively it could record keystrokes used in composing communications such as e-mail, instant messaging, electronic bulletin board posting, and online transactions, that are transmitted via the Internet, thus brining it within the scope of Title III.[166] However, if Magic Lantern is configured so as not to record information traveling over the Internet, but only to record keystrokes made "offline" (such as the KLS in *Scarfo*),[167] then it would seem that law enforcement agencies and personnel would not need the authority granted under Title I of the ECPA (dealing primarily with wiretaps) in order to operate Magic Lantern.[168]

For example, the court in *Scarfo* stated that "the F.B.I. did not install and operate any component which would search for and record data entering or exiting the computer from the transmission pathway through the modem attached to the computer[,]" because the "F.B.I. configured the KLS to avoid intercepting electronic communications typed on the keyboard and simultaneously transmitted in real time via the communication ports."[169] This means that the KLS did not record keystrokes while the modem operated.[170] Consequently, the court ruled that "the KLS did not intercept any wire communications" and therefore did not violate Title III, 18 U.S.C. § 2510 ("ECPA," "wiretap act," or "Title III").[171] However, the law is still very unclear in this area, and with only one district court ruling on the subject matter, many other courts could come to contrary holdings.

The distinction in *Scarfo*[172] between online and offline communications could be moot, however, contingent on the courts interpretation of "intercept" as defined in 18 U.S.C. § 2510(4): "'intercept' means the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical, or other device[.]"[173]

The case law surrounding the interpretation of the word "intercep-

165. 18 U.S.C. § 2510(12).
166. *Id.* §§ 2510-2522.
167. *See generally Scarfo,* 180 F. Supp. 2d 572.
168. 18 U.S.C. §§ 2510-2520.
169. *Scarfo,* 180 F. Supp. 2d at 581.
170. *Id.* at 582.
171. *Id.*
172. *See generally id.*
173. 18 U.S.C. § 2510(4).

tion" is unclear, conflicting, and contradictory at best.[174] However, there are some concurrences.[175] Although its function is less potent than Magic Lantern's, the installation and use of a pen register has been held not to be an "interception" under the definition of Title III, due principally to the fact that pen registers do not record content.[176] As previously stated, Magic Lantern would probably be found to record "content," unless otherwise configured and specified (i.e., the KLS in *Scarfo*[177]). This is due mainly to the fact that, if Magic Lantern recorded every keystroke, then it would collect all letters turning into sentences, turning into paragraphs, typed in word processing documents, e-mails, instant messaging, etc.[178]

A conflict of authority exists concerning whether an "interception" must be made while the communication is *in transit*, or if an interception can occur upon the seizure of communications that have previously been in transit but currently are stored, or communications that are waiting to be sent.[179] The answer to this quagmire differs among the various courts.[180]

In *Steve Jackson Games, Inc. v. United States Secret Service,*[181] the Fifth Circuit considered "whether the seizure of a computer on which is stored private Email that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, constitutes an "intercept" proscribed by 18 U.S.C. § 2511(1)(a)[Title III]."[182] The court held that "Congress' use of the word 'transfer' in the definition of 'electronic communications', and its omission in that definition of the phrase 'any electronic storage of information'. . .reflects that Congress did not intend for

174. *See generally N.Y. Tel.* 434 U.S. 159; *Korman v. U.S.,* 486 F.2d 926 (7th Cir. 1973); *U.S. v. Ill. Bell Tel. Co.* 531 F.2d 809 (7th Cir. 1976); *U.S. v. Kai,* 612 F.2d 443 (9th Cir. 1979).

175. *Id.*

176. *Id.*

177. *See generally Scarfo,* 180 F. Supp. 2d 572.

178. George Anastasia, *Scarfo Case Could Test Cyber-spying Tactic,* Inquirer ¶ 5 (Jan. 6, 2002) (available at <http://philly.com/inquirer/2000/12/04/front_page/jmoBo4.htm?template+aprint.html>).

179. *See generally Konop v. Hawaiian Airlines, Inc.,* 236 F.3d 1035 (9th Cir. 2001), *opinion withdrawn by Konop v. Hawaiian Airlines, Inc.,* 262 F.3d 972 (9th Cir. 2001) (holding that electronic communications in transit and in storage should be treated equally for the purposes of defining "interception" according to the ECPA).

180. *Id.*

181. 36 F.3d 457 (5th Cir. 1994).

182. *Id.* at 460. In *Steve Jackson,* plaintiff "operated from one of its computers an electronic bulletin board system. . ." *Id.* The United States Secret Service, in an attempt to recover information, seized Jackson's computers that contained information that the Secret Service was seeking. *Id.* Jackson then sued claiming the Secret Service violated, among others, the *Federal Wiretap Act* (18 U.S.C. §§ 2510 et seq.) and the *Stored Communications Act* (18 U.S.C. § 2701 et seq.). *Id.*

'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'"[183] The court held that Title II of the ECPA, instead of Title I, should govern electronic communications intercepted in electronic storage.[184] Some courts have followed the rationale in *Steve Jackson,*[185] while other courts have come to contrary decisions.[186]

The definition of "intercept" could prove to be crucial to the treatment of Magic Lantern, particularly if the recording of keystrokes does not qualify as accessing "stored communications" "without authorization a facility through which an electronic communication service is provided; or (2) [if the recording of keystrokes] intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage."[187] This outcome seems probable, taking into account that the statute was created to provide "both criminal sanctions and a civil right of action against persons who gain unauthorized access to communications facilities and thereby access electronic communications stored incident to their transmission."[188] The language of the statute also indicates that Title II of the ECPA will not govern Magic Lantern because Magic Lantern is installed on a personal computer, not "a facility through which an electronic communication service is provided" such as an ISP.[189]

In the case *In re DoubleClick Inc. Privacy Litigation,*[190] the district court found that software known as "cookies", which is implanted on a target's hard drive and collect information "such as usernames, passwords, and preferences," a technology not unsimilar to Magic Lantern, is not governed under Title II based on the "temporary" language used in

183. *Id.* at 461-62.

184. *Id.* at 462-63.

185. *See generally U.S. v. Reyes,* 922 F.Supp. 818 (S.D.N.Y. 1996) (holding that retrieval of numbers from the memory of a pager is not an "interception" within the meaning of the ECPA). The court in *Reyes* stated that "intercepting an electronic communication essentially means acquiring the *transfer* of data. . .the definitions [provided in 18 U.S.C. 2510] thus imply a requirement that the acquisition of the data be simultaneous with the original transmission of the data." *Id.* at 836. The court went on to state "[c]onsequently, in retrieving numbers from the pagers memories, the agents in this case access stored electronic communications. The accessing of stored electronic communications is governed by Title II of the ECPA, 18 U.S.C. § 2701 *et seq.*" *Id.* at 837.

186. *See generally Konop,* 236 F.3d 1035 (9th Cir. 2001) (*opinion withdrawn by Konop,* 262 F.3d 972).

187. 18 U.S.C. § 2701.

188. *DoubleClick,* 154 F. Supp. 2d at 507.

189. 18 U.S.C. § 2701.

190. 154 F. Supp. 2d 497 (2001).

defining "electronic storage"[191] under the ECPA.[192] The court in *DoubleClick* held that the section defining "electronic storage" "is specifically targeted at communications temporarily stored by electronic communications services incident to their transmission."[193] This means that, according to the court's holding, the statute is directed towards ISP's that store their client's communications temporarily as they are routed through the system.[194] The decision only provides further support for the contention that Title II of the ECPA will not govern Magic Lantern.[195]

Therefore, analysis of the applicability of the *Electronic Communications Privacy Act*[196] to the use of Magic Lantern is as follows: Magic Lantern's use must first be deemed an "interception" of "electronic communication."[197] It is likely that Magic Lantern will meet the "acquisition" requirement because it records data, as well as, and for the same reason, the requirement that the interception be done "through the use of any electronic, mechanical, or other device."[198] However, it seems that the determination of whether keystrokes will be deemed "electronic communication" will depend on the specifications and configuration of Magic Lantern, specifications which are largely heretofore unrevealed, as well as judicial interpretation of the statute's definition.[199] Assuming, *arguendo*, that keystrokes *are* deemed electronic communication, the use of Magic Lantern would then require clearance through the rigorous authorization process outlined in Title I of the ECPA,[200] and analysis of any challenges to Magic Lantern's use would have to be on a case-by-case basis since the amount of information collected could possibly vary.[201] However, if Magic Lantern's use is *not* found to be one of "interception" under Title I of the ECPA,[202] it is additionally unlikely that Title II of the ECPA will govern its use.[203] The language of the statute does not apply to individual users, whereas the use of Magic Lantern does exactly

191. 18 U.S.C. § 2510(17) (defining "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication").

192. *DoubleClick*, 154 F. Supp. 2d at 511-12.

193. *Id.*

194. *Id.*

195. *Id.* at 512.

196. 18 U.S.C. §§ 2510-2522, 2701-2709.

197. *Id.* §§ 2510(4)-(12).

198. *Id.*

199. *See supra* nn. 120-125 and accompanying text.

200. 18 U.S.C. §§ 2510-2522.

201. *See supra* nn. 113-117 and accompanying text.

202. 18 U.S.C. §§ 2510-2522.

203. *See supra* nn. 140-145 and accompanying text.

that.[204] Ultimately, unless Congress acts to extend the reach of the ECPA, Magic Lantern's use will probably not be governed under the ECPA at all, due to the strong implication in the language of the statute that it was drafted primarily for technologies more akin to "Carnivore," a technology capable of intercepting communications similar to those intercepted by a traditional wiretap.[205]

B. *FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978*[206]

In light of recent acts of foreign and domestic terrorism, perhaps the most significant piece of legislation that could potentially authorize and govern much of the use of Magic Lantern is the FISA.[207] FISA, enacted in 1978 in response to "public concern about executive wiretaps," created and outlined "standards for obtaining a court order authorizing foreign intelligence electronic surveillance."[208] Specifically, FISA "authorizes the issuance of secret wiretap orders" for foreign intelligence information "upon a judicial finding of probable cause to believe that the subject of the order is a foreign power or an agent of a foreign power."[209] No court order is required for authorization under FISA if no United States person is likely to be overheard in the surveillance, "only certification by the Attorney General. If a United States person is involved, however, FISA requires an order issued by a special foreign intelligence surveillance court. A judge [on the] court must approve the electronic surveillance if . . . the requirements of the statute have been satisfied."[210]

---

204. 18 U.S.C. § 270. Sullivan, *supra* n. 10, at ¶ 14; Lemos, *supra* n. 20, at ¶ 16. "'If Magic Lantern is as described, then it is a rifle-shot attack on a suspect'. . .compared with Carnivore's shotgun blast." *Id.*

205. *See* 18 U.S.C. § 2510. The statute continually makes use of the word "transmitted" and "transmission", indicating a wiretap/Carnivore technology that intercepts communications in "transit" over the internet or a wire, not keystrokes made on an individuals keyboard. *Id.* § 2510(12) (17).

206. 50 U.S.C.A. §§1801-1863 (1994 & Supp. V 1999).

207. *Id.*

208. Brian H. Redmond, *Validity, Construction, and Application of Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.A. §§ 1801 et. seq.) Authorizing Electronic Surveillance of Foreign Powers and Their Agents*, 86 A.L.R. Fed. 782, 788 (1988).

209. Marc Roth, *Subpoenas, Search Warrants and Surveillance Orders-Coming to an ISP Near You?* 18 No. 7 E-Commerce 1; *see* 50 U.S.C.A. §§ 1801, 1802 (1994 & Supp. V 1999).

210. Motta, *supra* n. 69, at 664. FISA created a Foreign Intelligence Surveillance Court on which seven United States District Court judges, selected by the Chief Justice of the United States, sit.

> The order must specify the identity or provide a description of the target of the electronic surveillance, the nature and location of each facility or place at which electronic surveillance will be effected and whether physical entry will be used to effect the surveillance, the period of time during which the electronic surveillance is approved and when more than one surveillance devise is used under the order, the authorized coverage of each device and the minimization procedures to be ap-

In order for FISA to be deemed applicable, Magic Lantern must first meet the statute's definition of "electronic surveillance."[211] Although FISA provides several circumstances that would qualify as "electronic surveillance," the definition that will more than likely apply to Magic Lantern is 50 U.S.C. § 1801(f)(4). This definition provides that electronic surveillance is the:

> installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for enforcement purposes.[212]

Magic Lantern is a surveillance device used to record keystrokes, thus falling under the first part of FISA's definition.[213] Additionally, unless otherwise notified of the Trojan/virus that was secretly installed into the hard drive, it seems manifest that one would have a reasonable expectation of privacy in the keystrokes entered into his or her computer.[214] Moreover, as demonstrated in *Scarfo*,[215] keystroke logging is the kind of activity for which "a warrant would be required for law enforcement purposes."[216] Consequently, it seems likely that the use of Magic Lantern will meet both the traditional and legal definition of "electronic surveillance."

The use of Magic Lantern will also have to meet the minimization requirements and procedures laid out in 50 U.S.C. § 1801(f).[217] The statute mandates specific procedures that must be followed in order to minimize any disruption and damage the surveillance may cause.[218] For

---

> plied. The order also must direct that the minimization procedures be followed and may direct third parties to furnish law enforcement authorities with necessary information, facilities, or technical assistance necessary to accomplish the electronic surveillance in a manner that will protect its secrecy and interfere minimally with the services of the subject of that order.

Id. at 664-65.

211. 50 U.S.C. § 1801(f)(4).

212. *Id.*

213. *See generally* Sullivan, *supra* n. 10.

214. *See supra* Part II and accompanying text (discussing an individual's reasonable expectation of privacy).

215. *Scarfo*, 180 F. Supp. 2d at 578-80.

216. 50 U.S.C. § 1801(f)(4); *see Scarfo*, F. Supp. 2d at 574. The FBI obtained two search warrants to install the KLS on Scarfo's computer. *Id.*

217. *Id.*

218. 50 U.S.C. § 1801(h).

> "Minimization procedures", with respect to electronic surveillance, means-
> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information; (2) procedures that require that nonpublicly

example, given that Magic Lantern is a computer program whose source code is capable of being edited if necessary to perform, or quit performing, certain functions, it would appear that the use of Magic Lantern could be altered as needed to comply with the minimization procedures.[219]

FISA's significance and importance to Magic Lantern lie in the ease of which authorization is obtained for electronic surveillance under the statute.[220] "Because the governmental interest in gathering intelligence information is different from that of a criminal investigation,"[221] the prerequisites required for authorization of electronic surveillance under FISA contain a much lower burden of proof and thus are much easier to obtain than that required for the issuance of a warrant or wiretap in a criminal investigation.[222] FISA authorization requires

> that the FISA Judge find probable cause to believe that the target is a foreign power or an agent of a foreign power, and that the place at which the electronic surveillance is to be directed is being used or is about to be used by a foreign power or an agent of a foreign power; and it requires him to find that the application meets the requirements of the Act.[223]

The relaxed burden of proof required to obtain authorization for sur-

---

available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than twenty-four hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

Id.

219. *Id.*

220. *Id.* §§ 1801-1805.

221. Redmond, *supra* n. 208, § 3[b].

222. *Id.* (*citing U.S. v. Dugan*, 743 F.2d 59 (N.Y. 1984)). *Duggan* held that "given the differences between ordinary criminal investigations and foreign counterintelligence investigations, the adoption in [FISA] of prerequisites to surveillance that are less stringent than those precedent to the issuance of a warrant for a criminal investigation is reasonable." *Id.*

223. *Dugan*, 743 F.2d at 73. The court in *Duggan* stated "We conclude that these requirements provide an appropriate balance between the individual's interest in privacy and the government's need to obtain foreign intelligence information, and that FISA does not violate the probable cause requirement of the Fourth Amendment." *Id.* at 74.

veillance under FISA[224] takes on even more importance for Magic Lantern when viewed in light of the recent passage of the *USA PATRIOT Act*[225], a statute that significantly broadened the surveillance power of the national government by modifying numerous existing statutes including FISA.[226] Specifically pertaining to the use of Magic Lantern under FISA, the *USA PATRIOT Act* relaxed the authorization requirement by stating that the purpose of obtaining "foreign intelligence information" need not be the entire reason for the surveillance, but only a "significant purpose."[227] This amendment of the threshold requirement seems to indicate that Congress is now more willing to accept, and perhaps encourage, the use of governmental surveillance for anti-terrorism and intelligence warfare purposes.[228] This acquiescence to governmental electronic surveillance combined with FISA's likely application to Magic Lantern would seemingly give the FBI a great amount of leeway in choosing its targets, obtaining authorization for the use of Magic Lantern, and recording keystrokes that could potentially reveal more information than was specified in the authorization order.[229]

C. Additional Statutes Possibly Affecting the Use of Magic Lantern: *USA PATRIOT Act*, the *Privacy Protection Act*, and the *Computer Fraud and Abuse Act*.

Although the web of interweaving laws that could conceivably apply to the use of Magic Lantern is vast and of varying consequence, a brief analysis of the *USA PATRIOT Act*,[230] the *Privacy Protection Act* ("PPA"),[231] and the *Computer Fraud and Abuse Act* ("CFAA")[232] helps demonstrate the applicability of statutory law on Magic Lantern.

1. *The USA PATRIOT Act*

As previously discussed, the *USA PATRIOT Act*, passed mainly in response to the recent terrorist attacks,[233] significantly modifies current government surveillance law.[234] In addition to loosening the restrictions required to obtain authorization for surveillance under FISA, the Act

224. 50 U.S.C. §§ 1801-1863.
225. *U.S.A.PATRIOT Act*, Pub. L. No., 107-56, 2001 HR 3162, §§ 206-208, 218.
226. *Id.*
227. *Id.* § 218.
228. *Id.*
229. *Id.*
230. *Id.*
231. 42 U.S.C.A. § 2000aa (2001).
232. 18 U.S.C.A. § 1030.
233. Bret A. Fausett, Webtechniques, *Becoming a Patriot* 10 <http://www.webtechnique.com> (Feb. 2002).
234. *See supra* nn. 169, 170 and accompanying text.

makes terrorism an action for which a wiretap may be authorized under Title III (ECPA, *Wiretap Act*).[235] The Act also specifically authorizes the use of the FBI's "other" electronic surveillance tool Carnivore,[236] authorizes additional sharing between information law-enforcement and national security agencies of surveillance intelligence,[237] expands governmental surveillance duration limits,[238] authorizes "sneak and peek" warrants,[239] and leaves most of these provisions intact even after the "sunset" clause in the Act terminates many other provisions.[240] Although the passage of the *USA PATRIOT Act* mainly affects the use of Magic Lantern indirectly, as previously discussed, the Act represents a liberal trend in Congress and serves to both allow and encourage the development and use of governmental surveillance technologies.[241] Thus, every challenge to governmental surveillance, and, more specifically, challenges to the use of Magic Lantern made while these statutes remain in effect will occur against the backdrop of a government providing leniency to surveillance technologies.

2. *The Privacy Protection Act*

The PPA[242] could prove to complicate the use of Magic Lantern, contingent on how the courts interpret the language of the statute as it applies to "keystroke logging" as opposed to a more traditional "seizure" under the Fourth Amendment.[243] "The [PPA] ensures publishers' First Amendment rights of freedom of the press by establishing that government seizure of publishers' 'work product materials' is a criminal offense unless there is a probable cause to believe that the person possessing such materials is committing the offense to which the materials relate."[244] Specifically, the Act prohibits any government officer, while investigating or prosecuting a criminal offense, to "search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book broadcast,

235. *See* Young, *supra* n. 154, at 1058 (*citing U.S.A. PATRIOT Act*, Pub. L. No. 107-56, 115 Stat. 272, § 201 (amending 18 U.S.C. 2516(1)).

236. *See id.* (*citing* U.S.A. PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, § 214, 216 (amending 50 U.S.C. §§ 1842, 1843; 18 U.S.C. §§ 3121,3123,3127)).

237. *See id.* (*citing U.S.A. PARTIOT Act*, Pub. L. No. 107-56, 115 Stat. 272, § 203(b)-(d) (amending 18 U.S.C. § 2510, 2517)).

238. *See id.* (*citing U.S.A. PATRIOT Act*, Pub. L. No. 107-56, 115 Stat. 272, § 207 (amending 50 U.S.C. §§ 1805, 1824)).

239. *See id.* (*citing U.S.A. PATRIOT Act*, Pub. L. No. 107-56, 115 Stat. 272, § 213 (amending 18 U.S.C. § 3103a)).

240. *See id.* (*citing U.S.A. PATRIOT Act*, Pub. L. No. 107-56, 115 Stat. 272, § 224).

241. *See supra* nn. 237-241 and accompanying text.

242. 42 U.S.C.A. § 2000aa.

243. U.S. Const. amend. IV.

244. Gindin, *supra* n. 149, at 1203.

or other similar form of public communication[.]"[245] Although it is axiomatic that the communications composed electronically and, consequently typed on a keyboard, can be "published" to the public via the Internet (Web pages, bulletin boards, etc.),[246] it is unclear whether keystrokes will fall into the definition of "work product materials" or "documentary materials," both of which refer to actual materials or in the case of electronic communication, "magnetically or electronically" stored materials.[247] Since Magic Lantern presumably only records actions such as keystrokes and does not collect actual materials stored electronically or magnetically, then the PPA will apply to the use of Magic Lantern only if the courts find that Magic Lantern "constructively" seizes information that would later (when the work that the keystrokes made up were saved on a hard drive or communicated via the Internet) qualify as "work product materials" or "documentary materials."[248] If this rationale is carried out in the courts, then the use of Magic Lantern will have to fit into one of the exceptions provided for in the PPA,[249] or alternatively only intercept passwords and like keystrokes that by their very nature are generally not published to the public. Of course, these challenges must be handled on a case-by-case basis, and given the political support for governmental surveillance,[250] Magic Lantern will probably fall outside the range of the PPA.[251]

---

245. 42 U.S.C.A. § 2000aa(a).

246. Gindin, *supra* n. 149, at 1204. "[A]nyone posting messages on the Internet or online services can be considered a 'publisher.'" *Id.*

247. 42 U.S.C.A. § 2000aa-7(a) (b) reads:

> 'Documentary materials,' as used in this chapter, means materials upon which information is recorded, and includes, but is not limited to, written or printed materials, photographs, motion picture films, negatives, video tapes, audio tapes, and other mechanically, magnetically or electronically recorded cards, tapes, or discs, but does not include contraband or the fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or which is or has been used as, the means of committing a criminal offense. (b) 'Work product materials,' as used in this chapter, means materials, other than contraband or the fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or which is or has been used, as the means of committing a criminal offense, and— (1) in anticipation of communicating such materials to the public, are prepared, produced, authored, or created, whether by the person in possession of the materials or by any other person; (2) are possessed for the purposes of communicating such materials to the public; and (3) include mental impressions, conclusions, opinions, or theories of the person who prepared, produced, authored, or created such material.

Id.

248. *Id.*

249. *See id.*

250. *See supra* part III.C.1 (concerning the recent passage of the *USA PATRIOT Act*).

251. *See* 42 U.S.C. § 2000aa.

3. *The Computer Fraud and Abuse Act*

The *Computer Fraud and Abuse Act* ("CFAA")[252] is "primarily intended to prevent unauthorized access to computer networks to protect the privacy of communications associated with those networks."[253] Although the statute lies on the fringe affecting the use of Magic Lantern, it will be of particular importance if the Magic Lantern technology is intercepted and used by a hacker seeking to conform the FBI's snoop software for his or her own benefit by accessing a computer prohibited by the statute.[254]

4. *The Usual Suspects?*

In addition to the aforementioned statutes, Magic Lantern will also be subject to the same "informational privacy" based statues by which many other surveillance technologies are governed, specifically the *Privacy Act*[255] and the *Freedom of Information Act* ("FOIA").[256] If Magic Lantern records more than mere passwords, these acts will probably require disclosure of particular information kept by the FBI and obtained through the technology's use.[257] Magic Lantern does not deviate far from other surveillance technologies concerning its application to these two statutes.[258]

However, not all statutes that affect governmental surveillance will be deemed applicable to Magic Lantern because the technology clearly does not fall under the language of these statutes. For example, the *Communications Assistance for Law Enforcement Act* ("CALEA"),[259] as it applies only to ISPs by imposing upon them an obligation to "ensure their networks are sufficiently accessible to law enforcement. Note that CALEA has no effect on law enforcement's ability to obtain a court order, such as a search warrant. . .it simply defines the scope of obligation to telecommunications carriers to make technical changes to their networks to accommodate surveillance."[260] So although the statute proves

252. 18 U.S.C. § 1030.

253. Edward Fenno, *Federal Internet Privacy Law,* 12-Feb S.C. Law. 36, 41 (2001) (*citing* 18 U.S.C. § 1030 (2001)).

254. 18 U.S.C. § 1030.

255. 5 U.S.C.A. § 552a (2001).

256. *Id.*

257. Gindin, *supra* n. 149, at 1203. "The Privacy Act of 1974 is the primary statute governing the federal government's acquisition and use of federal agency records containing personal information. The act prohibits disclosure of a record without the written consent of the subject of the record except under certain circumstances." *Id.* at 1204.

258. *See* 5 U.S.C. § 552a.

259. 47 U.S.C.A. §§ 1001-10 (2001).

260. Donna N Lampert, *Internet Privacy: An Overview of Domestic and International Issue and Policy Responses,* 597 PLI/PAT 357, 365 (2000).

beneficial for surveillance technologies, such as "Carnivore," that require the assistance of an ISP for "wiretapping," CALEA demonstrates well the numerous laws that Magic Lantern will bypass due to the fact that the surveillance needs no direct assistance from a communications carrier.[261]

IV. THE PRACTICAL APPLICATION AND DILEMMAS OF MAGIC LANTERN, AND THE RAMIFICATIONS OF ITS USE.

Although it appears that the use of Magic Lantern, with the proper authorization, will be within the proper boundaries of the law, the practical application of the technology will probably be much more difficult.[262] The technology faces serious conflict with anti-virus software programs and foreign governments.[263] However, many critics argue that the software is a better alternative than the previous software snoop, "Carnivore," and the proposed "national key escrow" to combat criminals that encrypt their communication.[264]

A. THE ANTI-VIRUS DILEMMA

After Magic Lantern jumps the legal hurdles and barriers to the authorization of its use and once the FBI sends it, the Trojan must remain hidden on the target's computer in order to be effective.[265] Consequently, the use of Magic Lantern will be greatly hindered if not made altogether futile, unless anti-virus software developers acquiesce to the use of the trojan and design their software programs to "look over" the infecting file, or perhaps, alternatively, abstain from designing the software to "find" the file.[266]

Mixed reports abound concerning whether the anti-virus software developers are going to cooperate with the government.[267] "Major anti-virus vendors [have said] that they would not voluntarily cooperate with the FBI and said their products would continue to be updated to detect and prevent viruses, regardless of their origin, unless there was a legal order otherwise."[268] The software vendors state that "looking over" the virus would "anger U.S. customers and alienate non-U.S. customers and governments."[269] Contrary to some reports,[270] and at the release of this article, the general sentiment of the anti-virus industry appears to be

261. 47 U.S.C.A. §§ 1001-10.
262. *See supra* nn. 237-242, and accompanying text.
263. Crocker, *supra* n. 13, at ¶ 4.
264. *See generally* Lemos, *supra* n. 20; Sullivan, *supra* n. 10, at ¶¶ 1, 12.
265. *See generally* Sullivan, *supra* n. 10.
266. *Id.*
267. *Id.*
268. MSNBC, *FBI Confirms, supra* n. 5, at ¶ 8.
269. *Id.* at ¶ 9.

that vendors are "in the business of providing a virus-free environment for [their] users and [they are] not going to do anything to compromise that security."[271]

The conflict becomes more complicated considering that "for antivirus vendors to know which Trojan horse to 'overlook', the FBI would need to provide a sample of the code. For security reasons, it is unlikely that this would happen."[272] The technology could be adapted without authorization and used illegally by hackers.[273] In addition, "[i]f anti-virus vendors were to leave a hole for an FBI-created Trojan horse program, malicious hackers would try to exploit the hole too. . .[i]f you leave the weakness for the FBI, you leave it for everybody."[274] Additionally, there is a question regarding "how. . .vendors [will] know which code is written by the FBI and which originates from virus authors with a chip on their shoulder[.]"[275]

An additional problem could be the precedent set if the anti-virus companies "ignore" Magic Lantern. Although the FBI is the only governmental agency to announce publicly its need for such cooperation from the anti-virus vendors, how will the vendors respond when other agencies (such as the CIA and NSA) request their cooperation? Many critics of the technology argue that "[t]he government would have to convince all anti-virus vendors to cooperate or the plan wouldn't work, since those not cooperating would have a market advantage and since they all share information."[276] The anti-virus vendors face "an impossible dilemma: if they do not comply with the FBI, they appear unpatriotic; if they do comply, they risk a catastrophic loss of business."[277]

B. The Foreign Government Dilemma

The use of Magic Lantern and its conflict with foreign governments could also cause conflict with those governments. "It is likely that the governments of other nations would want protection against anything like Magic Lantern" via the anti-virus vendors.[278] What if other law enforcement agencies from other countries developed technologies similar

270. *See generally* Robert Vamosi, MSNBC.com, *We Know What You're Typing* <http://www.msnbc.com/news/669010.asp> (Dec. 7, 2001).

271. Elinor Mills Abreu, *USA: Antivirus firms say they won't create FBI Loophole* Reuters English News Service ¶ 6 (Dec. 10, 2001) (available in WL 12/10/01 Reuters Eng. News Serv. 20:24:00).

272. *BugWatch: Magic Lantern- Not Magic and Not Very Bright* VNU Newswire ¶ 6 (Dec. 17, 2001) (available in 2001 WL 7311550) [hereinafter *Bug Watch*].

273. *Id.*

274. Abreu, *supra* n. 271, at ¶¶ 8, 9.

275. *BugWatch*, *supra* n. 272, at ¶ 7.

276. Abreu, *supra* n. 271, at ¶ 11.

277. Crocker, *supra* n. 13, at ¶ 4.

278. *See generally BugWatch*, *supra* n. 272.

to Magic Lantern? How would the United States government and anti-virus vendors react to a request to accommodate them?

Another diplomatic problem related to Magic Lantern and the anti-virus dilemma relates to the impression presented if the anti-virus vendors, with sales world wide, accommodate a spy tool of the United States government.[279] For example, "[i]f (the Chinese) thought that the company was a tool of the CIA [or in this case the FBI], China would stop using [the anti-virus products that comply with U.S. governmental requests] in critical environments."[280]

C. The Proponents Answer

Although Magic Lantern has drawn strong criticism,[281] those in favor of the technology feel that, in this era of informational warfare, Magic Lantern is a much more suitable technology for both security concerns and civil rights than previous surveillance technologies.[282] U.S. Rep. Richard Armey has been cited supporting the technology. "The way we look at it, this may be better than other available tools. . . Where the Carnivore system. . . has access to an entire data stream and could potentially spy on any traffic on that network, the so-called 'Magic Lantern' technology would only be installed on a single PC."[283] A spokesman for Armey stated that "if Magic Lantern is as described, then it is a rifle-shot attack on a suspect, compared with Carnivore's shotgun blast."[284]

Magic Lantern advocates also argue that the technology is a much more pragmatic and suitable alternative to the proposed "national key escrow."[285] The National Key Escrow system is one that would entrust all of the keys to unlock any encryption in a third party escrow, with the U.S. government owning the "master key," and consequently having "backdoor access to all encryption products made in the United States."[286] The logic behind this argument is that both the government and private citizens are better off giving the government authority to use Magic Lantern only on individuals for which they can obtain the proper authorization, as opposed to giving the government the "master key" that would allow them to decrypt every cipher message sent within the United States.[287]

---

279. *See generally* Abreu, *supra* n. 271.

280. *Id.* at ¶ 14.

281. *See generally BugWatch*, *supra* n. 272.

282. *See generally* Lemos, *supra* n. 20.

283. *Id.*

284. *Id.*

285. Sullivan, *supra* n. 10, at ¶ 12.

286. Brian Fonseca, CNN.com, *Fears Rekindle Key Escrow Debates* ¶ 3 <http://www.cnn.com/2001/TECH/internet/10/23/escrow.debate.idg/index.html> (Oct. 23, 2001).

287. Sullivan, *supra* n. 10, at ¶¶ 13, 14.

V. CONCLUSION

Magic Lantern, the FBI's electronic keystroke logger that is implanted via the Internet, is being introduced as a legally undeveloped surveillance technology into an uncertain and dynamic legal landscape. Although the technology has drawn criticism from many who claim the technology is a violation of privacy rights, the recent terrorist attacks have shifted government attitudes concerning electronic surveillance and altered the landscape in which any challenge to surveillance technology will be evaluated.[288] Purportedly used primarily to collect passwords needed to break encrypted messages which have historically been a problem for the FBI, the technology is reported to arrive via e-mail in the form of a Trojan horse or worm that installs itself secretly on the target's computer, records some or all keystrokes made, and supposedly transmits the information back to the FBI.[289]

In order to determine what authorization, if any, will be required for the use of Magic Lantern, both Constitutional and statutory determinations must be made. Using the "reasonable expectation of privacy" test developed in *Katz*,[290] it is likely that the use of Magic Lantern, and the consequent recording of keystrokes entered into a Personal Computer, will be considered a search and seizure under the Fourth Amendment[291], as it is axiomatic that many of the keystrokes which are recorded would be made, initially, with an expectation of privacy.[292] This determination would, at the very least, require a search warrant in order to utilize Magic Lantern on a specific target.[293] Additionally, use of the key logging technology would have to pass Constitutional standards prohibiting the use of a general warrant.[294] Considering the fact that the software can be modified to conform to constitutional standards, and that search warrants my be written with specificity, it is likely that Magic Lantern can be utilized without violating the general warrant prohibition in the Constitution.[295]

An additional burden will be placed on the use of Magic Lantern if such use is found to fall within the regulation of the *Electronic Communications Privacy Act*,[296] or the *Foreign Intelligence Surveillance Act*.[297]

---

288. William Matthew, Federal Computer Week, *Security Trumps Privacy in New Order* ¶ 4 <http://www.fcw.compcw/articles/2001/0924/pol-security-09-24-01.asp> (Sept. 24, 2001).

289. Crocker, *supra* n. 13, at ¶ 2.

290. *Katz*, 389 U.S. 347.

291. U.S. Const. amend. IV.

292. *See generally Katz*, 389 U.S. 347.

293. *Scarfo*, 180 F. Supp. 2d at 576.

294. *Id.* at 577.

295. *Id.*

296. 18 U.S.C. § 2510-2522, 2701-2709.

If the ECPA is deemed applicable to Magic Lantern's use, then authorization for a wiretap must be obtained before the technology is deployed on a target.[298] The burden for obtaining authorization under FISA is significantly less, however, requiring that "a significant purpose" of the investigation must be for foreign intelligence purposes.[299]

Whether Magic Lantern will be governed by the ECPA[300] will depend on whether courts interpret keystrokes as "electronic communications" and Magic Lantern's recording of those keystrokes as an "interception" under the definition of the statute.[301] It might be possible for some courts to reach the conclusion that the ECPA's definitions were meant to include the use of Magic Lantern because it "constructively intercepts" electronic communications by recording data that could later make up the content of an e-mail or other communication traveling through an ISP.[302] It is more likely, however, that Magic Lantern will be deemed not to fall within the reach of the ECPA, as the language of the statute is geared toward surveillance technologies similar to the FBI's "Carnivore" and is much more difficult to apply to the recording of keystrokes.[303]

If the FBI seeks to deploy Magic Lantern for purposes of Foreign Intelligence, then such use will most likely require authorization under FISA.[304] However, the burden is very low and requires only a showing probable cause the target is a foreign power or agent of a foreign power.[305] It is likely, therefore, that FISA will be a significant source for the authorization of Magic Lantern's use, as many recent security and surveillance concerns focus on international information.[306] Magic Lantern will also have to comply with the *Privacy Act*[307] and *Freedom of Information Act*, as do the other surveillance technologies.

The legal future of Magic Lantern rests in the hands of Congress and the courts. In this age of information warfare, such technologies can prove to be invaluable in thwarting those that use technology to cause unthinkable disasters and tragedy. But the coexisting values of security and privacy require balance, and as one increases, the other, by nature, decreases. The question then turns on which value is more necessary.

---

297. 50 U.S.C. § 1801(f)(4)

298. *Reyes*, 922 F. Supp. at 836.

299. Roth, *supra* n. 209, §§ Pre-Patriot Act, Wiretap and Electronic Surveilance Statutes.

300. *Scarfo*, 180 F. Supp. 2d at 581.

301. *See generally* 18 U.S.C. § 2510.

302. *See id.*

303. *See id.*

304. *Dugan*, 743 F.2d at 73.

305. 50 U.S.C.A. §§ 1801-1863 (1994 & Supp. V 1999).

306. *Redmond, supra* n. 209, at 788.

307. 42 U.S.C.A. § 2000aa-7(a)(b).

Magic Lantern has the potential to be a functional security safeguard, and with that comes the potential for great abuse. In order to maintain the balance between privacy and security, enough safeguards must be put into place to ensure Constitutional and statutory compliance while maintaining the utility, or "Magic," of Magic Lantern.

Neal Hartzog †

† J.D. candidate, Cumberland School of Law, December 2002; B.A., Samford University, 2000. The author would like to thank those who contributed advice in the drafting of this article, his parents for their inspiration and his wife, Jennifer, for her love and support.