

HACKING THE FOURTH: HOW THE GAPS IN THE LAW AND FOURTH AMENDMENT JURISPRUDENCE LEAVE THE RIGHT TO PRIVACY AT RISK

INTRODUCTION

What happens when a computer hacker¹ illegally intrudes into an unsuspecting victim's computer, and then finds illegal material? What if the hacker turns the material over to the police? Can it be used in a criminal prosecution of the hacker's victim, or in a civil suit against him? The hacker himself has violated the law and may be prosecuted, but does his discovery of another crime and its disclosure to the government give him immunity for his own actions? If the prosecutor exercises discretion and chooses not to prosecute a hacker, does this constitute implied permission or even give the hacker an incentive for this conduct? Is a civil remedy available for the invasion of privacy which resulted in a term of imprisonment? These questions, and others like them, are becoming increasingly urgent, as evidence obtained by illegal hackers becomes more common.² When technology is used to discover evidence of identity theft, drug transactions or child pornography, courts are challenged in applying constitutional and

1. "Hacker" was a term originated by the team members at the Artificial Intelligence Lab at the Massachusetts Institute of Technology (MIT) as early as the 1950s. Original hackers believed that computer security was important and the commission of illegal acts, once developed by the hackers to commit technological intrusions, helped others to prepare and protect their computer systems and networks against the same security exploits once used by the hackers. Hackers in the 1960s and 1970s were "obsessed with not only achieving competency on the computer, but...gaining mastery over [it]." Hackers today believe that by writing new programs or taking over websites or other systems, they will be more recognized in the hacker community. See ROBERT MOORE, *SEARCH AND SEIZURE OF DIGITAL EVIDENCE* 19-20 (Marilyn McShane & Frank P. Williams III eds., L.F.B. Scholarly Publishing, LLC 2005).

2. See generally *United States v. Kline*, 112 F. App'x 562 (9th Cir. 2004); *O'Brien v. O'Brien*, 899 So. 2d 1133 (Fla. Dist. Ct. App. 2005); *United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003); *United States v. Jarrett*, 338 F.3d 339, 342 (4th Cir. 2003).

statutory safeguards intended to protect the individual to this changing environment.³

On May 10, 2000, Bradley Willman, a Canadian computer hacker, used a virus to invade a computer.⁴ During his intrusion and search of the computer's hard drive, Willman found child pornography.⁵ Through an Internet watchdog group, Willman subsequently contacted the Irvine Police Department (IPD) with the information he obtained by these questionable means.⁶ An IPD detective discovered that the computer belonged to Ronald C. Kline, a California Superior Court judge.⁷ A search warrant was issued and the evidence was seized.⁸ On September 25, 2002, Judge Kline was indicted on federal charges stemming from possession of child pornography.⁹ Because the materials recovered "were themselves the product[s] of a warrant-less search of [Kline's] home computer. . .by the criminal acts of a computer hacker,"¹⁰ who committed such crimes to provide law enforcement with information, the evidence was suppressed by the district court.¹¹ In October 2004, the Ninth Circuit reversed the suppression order and held that the hacker's pre-search contacts with law enforcement were "insufficient as a matter of law" to make him an agent of the state.¹² The court concluded that because the hacker was a private party, the protection of the Fourth Amendment did not apply and the evidence obtained by the hacker was admissible.¹³

A few months later, a Florida appellate court reached an apparently contrary result in a similar case. In *O'Brien v. O'Brien*,¹⁴ a wife used a hacking computer program to obtain evidence about her husband's online activities.¹⁵ The trial court refused to admit the

3. *Steiger*, 318 F.3d at 1039 (quoting *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002)).

4. *Kline*, 112 F. App'x at 563.

5. *Id.*

6. Christine Hanley, *Ex-judge Collapses at Sentencing*, L.A. TIMES, Feb. 21, 2007, at B3, available at <http://articles.latimes.com/2007/feb/21/local/me-kline21>.

7. Petition for Writ of Cert., *Kline v. United States*, 2005 WL 435912, at *5-*7 (9th Cir. 2004) (No. 04-1125).

8. *Id.* at *4, *7.

9. *Id.* at *3.

10. *Id.*

11. *Id.*

12. *Kline*, 112 F. App'x at 564.

13. *Id.*

14. 899 So. 2d 1133 (Fla. Dist. Ct. App. 2005).

15. *See id.*

evidence in their divorce proceedings.¹⁶ In *O'Brien*, the appellate court affirmed that the wife's conduct violated the Florida Wiretap Act,¹⁷ because the evidence obtained about communication between the husband and his online mistress was an interception of electronic communication.¹⁸ Although the Act does not include a suppression remedy for interceptions of electronic communication, the appellate court concluded that because the evidence was obtained illegally and the admissibility of evidence is within the sound discretion of the trial judge, the court did not abuse its discretion by suppressing the evidence.¹⁹

Conflicting evidentiary rulings about the admissibility of illegally-obtained electronic evidence in criminal and civil litigation are troubling. However, due to the fast-evolving technology of computers, the Internet, and due to underdeveloped law, further inconsistent results are likely to result.

In an attempt to provide better protection from new technological threats to privacy, Congress enacted the Federal Wiretap Act²⁰ and the Stored Communications Act.²¹ However, these laws are insufficient to confront the ever-growing invasions of personal computers by hackers.²² The Acts need to be amended to include stored information on personal electronic or mechanical devices, allow a discretionary suppression remedy based on the underlying facts of evidence obtained by a violation, and subject a violator to a forfeiture of the device used in the unauthorized invasion.

These proposed amendments will ensure a lawful right to privacy in a rapidly changing environment. First, they will discourage law enforcement from purposefully evading the "agent of the state" requirement by using intermediaries and turning a "blind eye" to hacker conduct. In addition, the amendments will prevent hackers from shifting attention away from their own unlawful activity to others by disclosing their findings to law enforcement, and deprive hackers of a "bargaining chip" that invites abuse of prosecutorial discretion. Overall, these amendments will protect society from the twin threats of law enforcement abuse and technological criminal activity. At the same

16. *Id.* at 1134, 1138.

17. *Id.* at 1138; FLA. STAT. ANN. § 934.03 (WEST 2009).

18. *O'Brien*, 899 So. 2d at 1138.

19. *Id.*

20. 18 U.S.C. § 2510-2520 (2006).

21. 18 U.S.C. § 2701 (2006).

22. *See generally* MOORE, *supra* note 1, at 143-46.

time, law enforcement can still utilize other means to “pierce” the privacy protection of individuals when appropriate, allowing the government to obtain proper, untainted probable cause and evidence which will lead to prosecution while preserving individuals’ privacy protection.

Part I will address the conflict between technological advancement and the right to privacy, and provide examples of current intrusive technology. Part II will examine the history of Fourth Amendment jurisprudence and statutory development in response to technological threats against search and seizure by private individuals and the government. It will further examine the agency requirement of the Fourth Amendment, and argue that it should be reinterpreted in cases involving computer hackers. Part III reviews the Federal Wiretap Act and the Stored Communication Act, and describes how the courts have had trouble interpreting and applying them in hacker cases. The Comment identifies a gap between the two Acts that must promptly be closed. The fast rise in technology and the confusion in applying current statutes call for congressional action in response to the threat of computer hackers and intruders.

I. PRIVACY, THE INTERNET, AND “ANTI-HACKING” LAWS

An invasion of privacy occurs when “there is an intentional intrusion into a private place, conversation or matter [of another] . . . where there is an actual, subjective expectation . . . of [privacy] in that place, conversation or matter, and [] that expectation of privacy is objectively reasonable.”²³ Where a government intrusion is involved, the expectation of privacy extends as far as an area one acted to keep private, as long as society is willing to accept the privacy as reasonable.²⁴

The Internet presents special threats to privacy. In order to understand how, a brief overview of computer intrusions is helpful. One type of intrusive device is known as “spyware.” Spyware is “software installed on a computer without the target user’s knowledge and meant to monitor the users conduct.”²⁵ The program can be

23. J. THOMAS MCCARTHY, *THE RIGHTS OF PUBLICITY AND PRIVACY* § 5.89 (2d ed. 2008); *see also* *Med. Lab. Mgmt. Consultant v. Am. Broad. Companies*, 306 F.3d 806, 812 (9th Cir. 2002).

24. *See generally* *Katz v. United States*, 389 U.S. 347, 511-12 (1967).

25. *See* Sharon D. Nelson & John W. Simek, *The Growing Phenomenon of Computer Spying*, *ELECTRONIC EVIDENCE*, Sept. 2007, http://www.senseient.com/pdf/Electronic_Evidence_for_Family_Law_Practitioners.pdf.

installed either by someone with access to the target computer or remotely, for example, by sending a picture to someone with the program embedded in the picture.²⁶ As soon as the unsuspecting victim opens the picture file, the program is installed on the computer without the user's knowledge.²⁷ Spyware programs are very common and can be purchased for \$30-\$100.²⁸ Despite the negative publicity spyware has received in recent years, it has some useful "non-law-enforcement" purposes. For example, with spyware parents can track and monitor their children's online activity, employers can track their employees' activities, and schools can monitor students' use of the Internet.

Another tool used to access a computer without the owner's or user's knowledge is a computer virus, such as a "Trojan" virus.²⁹ While not as common as spyware, the Trojan virus is one of the most dangerous viruses known today, with over 1000 strands in circulation.³⁰ In the past, viruses were used by gifted programmers as a means of self expression, and mainly functioned to make a computer act abnormally.³¹ Today, the primary objective in the use of such a virus is to allow a remote user access to the victim's machine to do anything that the victim could do.³² The intruder's usual objective is to remotely browse the hard drive for valuable information.³³ If such information is found, the intruder can copy it onto his or her own hard drive, completely unnoticed by the victim, even if the victim is using the computer at the time.³⁴

The Trojan virus infects the computer in the same way the spyware is set up on a system. It can be attached in a picture, downloaded as an attachment to an email or by executing a file from an unknown source.³⁵ The difference between spyware and the Trojan virus is that while spyware allows the intruder to see what the victim is doing, the Trojan virus furnishes access to the hard drive, allowing the intruder to make changes, add and delete files, and copy any file to the intruder's own

26. *Id.*

27. *Id.*

28. *Id.*

29. See generally *Steiger*, 318 F.3d at 1044, 1047, 1050; *Kline*, 112 F. App'x at 564.

30. Daniel Petri, *What Is a Trojan Horse and What Threat Does It Pose?*, Jan. 8, 2009, PETRI IT KNOWLEDGEBASE, http://www.petri.co.il/what's_a_trojan_horse.htm.

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

hard drive.³⁶ The Trojan virus is clearly much more threatening to a person's privacy. Virtually all states have enacted statutes which penalize technological intruders.³⁷ The California legislature, for example, declared that "the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems and computer data."³⁸ Based on these observations, the legislature enacted a statute that prohibits "knowingly access[ing] and without permission tak[ing], cop[y]ing, or mak[ing] use of any data from a computer . . . ,"³⁹ punishable by a "fine not exceeding ten thousand dollars . . . or by imprisonment in state prison for 16 months, or two or three years, or by both that fine and imprisonment."⁴⁰ Further, simply "knowingly introduc[ing] any computer contaminant into any computer"⁴¹ is, as a first offense, a "misdemeanor punishable by fine not exceeding five thousand dollars . . . or imprisonment in a county jail not exceeding one year, or by both."⁴²

O'Brien v. O'Brien,⁴³ the Florida divorce case discussed above, involved spyware-obtained evidence in the civil litigation context.⁴⁴ A

36. See Petri, *supra* note 30.

37. See ALA. CODE 1975 § 13A-8-102 (West 2003); ALASKA STAT. ANN. § 11.46.484 (West 1996); ARIZ. REV. STAT. § 44-7302(A) (West 2005); ARK. CODE ANN. § 5-41-203 (West 2001); CAL. PENAL CODE § 502 (West 2001); COLO. REV. STAT. ANN. § 18-5.5-102 (West 2007); CONN. GEN. STAT. ANN. § 53a-251 (West 1984); DEL. CODE ANN. tit.11, § 932 (West 1995); FLA. STAT. ANN. § 815.06 (West 2001), § 934.03 (West 2002); GA. CODE ANN. § 16-9-93 (West 1991); HAW. REV. STAT. ANN. § 708-893 (West 2006); IDAHO CODE ANN. § 18-2202 (West 1984); 720 ILL. COMP. STAT. ANN. 5/16D-3 (West 2008); IND. CODE ANN. 35-43-2-3 (West 2001); IOWA CODE ANN. § 714.1 (West 2005); KAN. STAT. ANN. 21-3755 (West 1984); KY. REV. STAT. ANN. § 434.850 (West 2002); LA. REV. STAT. ANN. § 14:73.7 (West 2001); ME. REV. STAT. ANN. tit. 17-A § 433 (West 1989); MD. CODE ANN., CRIM. LAW § 7-302 (West 2008); MASS. GEN. LAW ANN. ch. 266, § 120F (West 1994); MICH. COMP. LAWS ANN. 752.795 (West 1997); MINN. STAT. ANN. § 609.891 (West 2006); MO. ANN. STAT. § 569.095 (West 2002); NEB. REV. ST. ANN. § 28-1343.01 (West 2008); N.H. REV. STAT. ANN. § 638:17 (West 2003); N.J. Stat. Ann. § 20-23-20-36 (West 2003); N. M. STAT. ANN., § 30-45-5 (West 2006); N.Y. PENAL LAW § 156.05 (McKinney's 2006); N.C. GEN. STAT. ANN. § 14-454 (West 2000); N.D. CENT. CODE, 12.1-06.1-08 (West 2008); OHIO REV. CODE ANN. § 2913.04 (West 2004); R.I. GEN. LAWS § 11-52-3 (West 2007); S.C. CODE ANN. § 16-16-20 (West 2002); TENN. CODE ANN. § 24.052(west effective 2009); VA. CODE ANN. § 4102 (West 1999); WIS. STAT. ANN. 943.70 (West 2002); W. VA. CODE ANN. § 61-3C-5 (West 1989); WYO. STAT. ANN. § 6-3-504 (West 2008).

38. CAL. PENAL CODE § 502 (West 2001).

39. CAL. PENAL CODE § 502 (c)(2) (West 2001).

40. CAL. PENAL CODE § 502 (d)(1) (West 2001).

41. CAL. PENAL CODE § 502(c)(8) (West 2001).

42. CAL. PENAL CODE § 502(d)(4) (West 2001).

43. 899 So. 2d at 1134.

44. See *id.*

wife installed the program to monitor her husband's conduct and discovered that he had been communicating with another woman.⁴⁵ The evidence the wife obtained using the program ultimately was excluded.⁴⁶ The wife's search was held to be an invasion of privacy and regarded by the court as an unreasonable search. Even though the spyware technology was in use by the general public, the husband had a subjective expectation of privacy in his online communications, which society is willing to recognize as objectively reasonable.⁴⁷ In excluding evidence resulting from this invasion of privacy, the court relied solely on the Florida Wiretap Act.⁴⁸

II. THE FOURTH AMENDMENT AND INTERNET-ASSISTED "SEARCHES"

Hacker or otherwise illegally-obtained electronic evidence is evaluated differently in the criminal context. Here, the Fourth Amendment governs admissibility. The Fourth Amendment to the United States Constitution provides that

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be search, and the persons or things to be seized.⁴⁹

Originally, the Fourth Amendment applied to civil trespass actions.⁵⁰ The evidentiary consequences of an illegal search on a criminal prosecution were not clearly established until 1914.⁵¹ In *Weeks v. United States*,⁵² the Supreme Court held for the first time that the exclusionary rule is a necessary effect of the rights guaranteed in the Fourth Amendment.⁵³ Still, the Fourth Amendment was "written in a

45. *See id.*

46. *Id.*

47. *See id.* at 1135 (discussing the purpose of the Florida Act which was the reason the evidence was excluded).

48. *Id.* at 1137-38.

49. U.S. CONST. amend. IV.

50. Sam Kamin, *The Private is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83, 91 (2004).

51. *See, e.g.,* *Mapp v. Ohio*, 367 U.S. 643, 648 (1961) ("[I]n the *Weeks* case, this Court 'for the first time' held that 'in federal prosecution the Fourth amendment barred the use of evidence secured through an illegal search and seizure.'") (quoting *Wolf v. Colorado*, 338 U.S. 25, 28 (1949)).

52. 232 U.S. 383, 398 (1914).

53. *See generally* *Weeks v. United States*, 232 U.S. 383, 398 (1914).

very different context and address[ed] very different concerns,”⁵⁴ which repeatedly challenged the courts in its interpretation. Two separate aspects of the Fourth Amendment are relevant in the context of hacker-obtained evidence. The first is the scope of Fourth Amendment protection, and the effect of technology on the changing understanding of privacy. The second is the “agent of the state” requirement.

A. *Technology and Privacy*

In the non-Internet “real world,” the Fourth Amendment applies whenever an individual maintains an expectation of privacy which society is willing to find reasonable.⁵⁵ The Constitution therefore requires a valid search warrant.⁵⁶ But if someone places trash on the street, the right to privacy and the concomitant need for a search warrant disappear.⁵⁷ Similarly, if a person shares information or property with another and no special privilege applies,⁵⁸ the government can go to that third party and obtain the information or property without a warrant.⁵⁹ Should the same “disclosure” principles apply to computer searches as well?

The recent proliferation of technology crime is partly due to the lack of trained law enforcement in the technology field and ignorance of the threat on the part of law enforcement.⁶⁰ The Fourth Amendment, already a complex and much-litigated provision of the Constitution,⁶¹ becomes even more complex when technological evidence is at issue.⁶² Changing technology has caused much confusion in the interpretation of the Fourth Amendment.⁶³ A further problem with applying Fourth Amendment doctrines to technological issues is the time-consuming process of litigation itself.⁶⁴ By the time a case works its way through

54. Kamin, *supra* note 50, at 92.

55. See *California v. Greenwood*, 486 U.S. 35 (1988); *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986); *Katz v. United States*, 389 U.S. 347 (1967).

56. See U.S. CONST. amend. IV.

57. See *California v. Greenwood*, 486 U.S. 35, 40-41 (1988).

58. For example, attorney client privilege, physician-patient privilege, etc.

59. See *Hoffa v. United States*, 385 U.S. 293, 302-03 (1966).

60. MOORE, *supra* note 1, at 10.

61. *Id.* at 11.

62. *Id.*

63. See Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 YALE J. L. & TECH. 120 (2007).

64. See MOORE, *supra* note 1, at 12.

the appeal process, “the technology could evolve to the point where judicial holding is irrelevant.”⁶⁵

An early example of the challenges the Supreme Court faces in understanding the Fourth Amendment’s protections in light of changing technology arose in the 1928 case of *Olmstead v. United States*.⁶⁶ In that case, the Court held that the Government’s eavesdropping on Olmstead’s telephone calls did not constitute a “search or seizure” for Fourth Amendment purposes, because the Government never entered Olmstead’s house or office.⁶⁷ At that time, the Court interpreted the Fourth Amendment to apply only to a search of material things – the person, a house, his papers or his effects.⁶⁸ Thus, because an individual’s conversation is intangible, they were not protected by the Fourth Amendment.

However, beginning in the 1960’s, the Supreme Court has consistently protected individuals’ privacy from government-sponsored technology-enhanced intrusion.⁶⁹ In 1961, in *Silverman v. United States*,⁷⁰ the Supreme Court held that the Fourth Amendment was violated when the police attached an electronic device to a heating duct in for the purpose of listening to conversations taking place inside the house.⁷¹ In 1967, Justice Stewart, writing for the majority in *Katz v. United States*,⁷² held that the FBI violated the Fourth Amendment when agents used an electronic device to listen and record a person’s conversations in a phone booth. In *Katz*, the Court clarified that “the Fourth Amendment protects people not places. [But] what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”⁷³ It follows that whatever area a person acts to keep private, if society is willing to recognize the reasonableness of that expectation of privacy,⁷⁴ is protected from government search by the Fourth Amendment.⁷⁵

65. *Id.*

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

67. *Id.* at 464-66.

68. *Id.* at 464.

69. *See* *Silverman v. United States*, 365 U.S. 505 (1961); *Katz v. United States*, 389 U.S. 347 (1967).

70. 365 U.S. 505 (1961).

71. *Silverman*, 365 U.S. at 509-11.

72. 389 U.S. 347 (1967).

73. *Katz*, 389 U.S. at 351.

74. *Id.* at 361.

75. *Id.* at 351.

A series of cases following *Katz* further clarified the contours of the doctrine.⁷⁶ In *Dow Chemical Company v. United States*,⁷⁷ decided in 1986, the Court held that the government did not violate the Fourth Amendment by using aircraft to photograph the defendant's property visible from the air.⁷⁸ The Court reasoned that because the defendant chemical company knowingly exposed that part of the property to the public, it had no expectation of privacy in that part of the property.⁷⁹

In the landmark case for analyzing searches using technology, *Kyllo v. United States*,⁸⁰ decided in 2001, the Supreme Court articulated a test to determine whether the use of a particular technology is a "search" for Fourth Amendment purposes. If the technology in question allows the government to obtain information that it could not otherwise obtain without a physical intrusion, the intrusion into a constitutionally protected area, such as a home, constitutes a search.⁸¹ In addition, the technology in question cannot be in "general public use."⁸²

In *Kyllo*, the government used thermal imaging technology to gather information by way of heat signatures from the inside of a home where agents suspected marijuana was being cultivated.⁸³ The Supreme Court held that the thermal imaging technology revealed private details that would have been undiscoverable without technology and hence, the use of the technology constituted a search for Fourth Amendment purposes.⁸⁴ By contrast, under the rule of *Kyllo*, a dog sniffing test is not a search.⁸⁵ The critical difference is that the technology in *Kyllo* was "capable of detecting lawful activity . . . [and] [t]he legitimate expectation that information about perfectly lawful activity will remain private is categorically distinguishable from . . . a dog sniff . . . that

76. See *Kyllo v. United States*, 533 U.S. 27 (2001); *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986).

77. 476 U.S. 227 (1986).

78. See *Dow Chem. Co.*, 476 U.S. at 239.

79. *Id.*

80. 533 U.S. 27 (2001).

81. *Kyllo*, 533 U.S. at 34.

82. *Id.*

83. *Id.* at 29-30 (2001).

84. *Id.* at 40.

85. See, e.g., *Illinois v. Caballes*, 543 U.S. 405, 409-10 (2005) (differentiating dog sniff to find contraband and technology that can be used to intrude on perfectly lawful activities); *United States v. Broadway*, 580 F.Supp. 2d 1179, 1191 (D. Colo. 2008) (same); *State v. Wiegand*, 645 N.W.2d 125 (Minn. 2002) (holding that dog sniff around exterior of a car in a public place does not constitute a search, however reversed on other grounds).

reveals no information other than the location of [an illegal substance].”⁸⁶

Kyllo could be used to argue for a distinction between the spyware used in *O’Brien*, which can be purchased from ordinary retail stores, and the Trojan virus “technology” that was used by the hackers in the criminal cases mentioned below.⁸⁷ Although the Trojan virus is in circulation, it is not widely available to the general public thus making it more like the technology in *Kyllo*. A home computer user has a subjective expectation of privacy because the computer is in his home and the most personal information is stored on home computers today.⁸⁸ “In the home, [Supreme Court] cases show, all details are intimate details, because the entire area is held safe from prying government eyes.”⁸⁹ It is also evident that society is willing to recognize such expectation of privacy as evident in the anti-hacking statutes across the country.⁹⁰ Therefore, the intrusive conduct is likely to qualify as a search under the standard set forth in *Kyllo*, and thus if the government participates in such a search, the evidence obtained would be inadmissible.

Most recently, the Circuit Courts have ruled on evidence obtained using Internet technology. In *United States v. Simon*,⁹¹ decided in 2000, Simon was convicted of receiving and possessing child pornography through the use of the Internet.⁹² The material was discovered when Simon’s employer was conducting a routine audit of the network, as per the employer policy.⁹³ In his suppression motion, Simon argued that the warrantless search of his office and computer violated his Fourth Amendment rights.⁹⁴ The Court applied the rule of *Katz* and held that “[t]o establish a violation . . . under the Fourth Amendment, [one] must prove that he had a legitimate expectation of privacy in the place searched or the item seized.”⁹⁵ In addition, proving the legitimate

86. See *Caballes*, 543 U.S. at 409-10 (quoting *Kyllo v. United States*, 533 U.S. 27, 38 (2001)).

87. See *Jarret*, 338 F.3d at 342; *Steiger*, 318 F.3d at 1050.

88. For example, bank account information, diaries, family pictures, resumes, bill records, etc.

89. *Kyllo*, 533 U.S. at 37 (2001).

90. See *Jarrett*, 338 F.3d at 342.

91. 206 F.3d 392 (4th Cir. 2000).

92. *United States v. Simon*, 206 F.3d 392, 399 (4th Cir. 2000).

93. *Id.* at 396-97.

94. *Id.* at 398 (claiming a Fourth Amendment violation since his employer was the Federal Bureau Information Services, a division of the Central Intelligence Agency, and the persons which executed the search were government employees).

95. *Id.*

expectation of privacy requires one to “prove that [the] subjective expectation of privacy is one that society is prepared to accept as objectively reasonable.”⁹⁶ Simon lacked a legitimate expectation of privacy in his work computer because of his employer’s Internet policy.⁹⁷ On that basis, without ever discussing the agent of the state requirement, the court held that the remote searches of Simon’s computer did not violate his Fourth Amendment rights.⁹⁸ There is a major difference between a subjective expectation of privacy at an office, where one under employment is aware of system audits, and an expectation of privacy in one’s home.

B. “Agent of the State” Requirement

Nothing in the Fourth Amendment explicitly states that the right to freedom from unreasonable searches and seizures is implicated only if such searches are conducted by governmental agencies. The Fourth Amendment, on its face, neither “restrict[s] its operation exclusively to governmental intrusions, nor requires exclusion in criminal trials of any evidence obtained in violation thereof.”⁹⁹ The limitation to government intrusion and the exclusionary rule are derived from the vast judicial interpretation of the Fourth Amendment.¹⁰⁰ However, it has long been the dogma in the law that “[t]he Fourth Amendment gives protection . . . [which] applies to governmental action . . . [that] was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon [anything] other than governmental agencies.”¹⁰¹ Private searches implicate Fourth Amendment protection only if the private individual is acting as an agent of the government at the time of the search.¹⁰²

The leading case on private searches is *Burdeau v. McDowell*.¹⁰³ McDowell’s employer discharged him for alleged unlawful and fraudulent conduct in the course of the business.¹⁰⁴ An officer of his employer (with permission from the president of the company), along with a detective, took possession of McDowell’s office, where two safes

96. *Id.*

97. *Id.* at 398.

98. *Simon*, 206 F.3d at 398-99 (4th Cir. 2000).

99. See Paul G. Reiter, Annotation, *Admissibility, in Criminal Cases, of Evidence Obtained by Search by Private Individual*, 36 A.L.R. 3d 553, 557 (1971).

100. *Id.*

101. *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921).

102. *United States v. Reed*, 15 F.3d 928, 930-31 (9th Cir. 1994).

103. 256 U.S. 465 (1921).

104. *Id.* at 474.

were present; a large one belonging to the company and a small one belonging to McDowell.¹⁰⁵ While the detective was in charge of the room, the two safes were blown open and all papers and possessions were taken out.¹⁰⁶ The company thereafter turned over a letter belonging to McDowell to the Department of Justice.¹⁰⁷

McDowell requested the return of his property (functionally a motion to suppress), which was granted by the District Court for the Western District of Pennsylvania.¹⁰⁸ The court ordered the evidence to be turned over to the clerk, sealed, and unless an appeal was made, returned to McDowell.¹⁰⁹ The District Court explained that the “order was made . . . not because of any unlawful act on the part of . . . the United States or any of its departments but solely upon the ground that the government should not use stolen property for any purpose after demand for its return.”¹¹⁰ The Supreme Court reversed, holding that the Fourth Amendment was “an intended restraint upon the activities of sovereign authority, and was not intended to be limitation upon other than governmental agencies.”¹¹¹

Although the decision has been challenged, it has consistently been followed and even broadened.¹¹² In *Coolidge v. New Hampshire*,¹¹³ decided in 1971, the Supreme Court established that searches by private persons are subject to the Fourth Amendment only if the private person is acting as an instrument or agent of the government.¹¹⁴ An individual is an agent of the state if “the government knew of and acquiesced in the intrusive conduct, and . . . the party performing the search intended

105. *Id.*

106. *Id.*

107. *Id.* at 475.

108. *Id.* at 472.

109. *Burdeau*, 256 U.S. at 471 (1921).

110. *Id.* at 472.

111. *Id.* at 475.

112. *See, e.g.,* *Elkins v. United States*, 364 U.S. 206, 223-24 (1960) (overturning *Week v. United States* 232 U.S. 383 (1914) by refusing to admit evidence offered as a result of an illegal search and seizure by state officials and broadening the rule from *Burdeau* to apply to any governmental agency not only the federal government); *United States v. Goldberg*, 330 F.2d 30, 35 (1964) (noting that the government had no part or knowledge in the conduct and holding the evidence admissible by directly relying on *Burdeau*); *People v. Horman*, 22 N.Y.2d 378, 381 (1968) (upholding a conviction for possession of a pistol where the defendant was apprehended by two department store employees, the court held that it was long settled that prohibitions against unlawful searches and seizures do not require exclusion of evidence because a private individual has gathered it by unlawful means).

113. 403 U.S. 443 (1971).

114. *See id.* at 487-90.

to assist law enforcement efforts.”¹¹⁵ Generally, the question of whether a private citizen has conducted a search as an agent of the state has arisen where the private individual was either authorized to be at the location of the search,¹¹⁶ or the search resulted from the individual’s duties under an employment contract.¹¹⁷ A hacker, by definition, is not “authorized” to be at the location of the search (inside the computer’s hard drive), nor is he covered by an employment contract that requires him to disclose illegal content in the place he is searching (as in *Simon*). Does this mean a hacker is never an agent of the state?

Consider the following situation. In *United States v. Steiger*,¹¹⁸ an anonymous person hacked Steiger’s computer, found child pornography, and contacted the Montgomery, Alabama police by electronic mail (email).¹¹⁹ Officer Murphy asked to talk to the hacker, who replied that he was from Turkey, could not afford a phone call and spoke very little English, but would provide all the information by email.¹²⁰ Murphy then replied that he was welcome to send the information that he had.¹²¹ The hacker sent an email with eight pictures, Steiger’s internet service account, possible home address, and other details.¹²² In subsequent unsolicited email messages, the hacker provided Steiger’s checking account numbers and the specific folders where the pictures were stored on Steiger’s computer.¹²³ Murphy contacted Agent Faulkner of the FBI, who obtained a warrant to search Steiger’s computer.¹²⁴ The affidavit used to obtain the warrant stated

115. *United States v. Miller*, 688 F.2d 652, 658 (9th Cir. 1982).

116. *See United States v. Roberts*, 644 F.2d 683, 687-88 (8th Cir. 1980) (upholding, in part, a second search by a Lessor of a storage facility who found bags containing a large amount of marijuana); *Roberts* was later reversed by *Horton v. California*, 496 U.S. 128 (1990) for the first search resulting in the suppression of separate large amount of marijuana; *see also People v. Wilkinson*, 163 Cal. App. 4th 1554, 1574 (Ct. App. 2008) (denying a motion to suppress evidence turned over by the defendant’s roommate’s boyfriend).

117. *See, e.g., People v. Hively*, 480 P.2d 559 (Colo. 1970) (stating that it was the duty of an airline employee to notify police when the employee discovered the presence of contraband and rejecting an argument that an unlawful search and seizure occurred when employee originally opened the bag); *People v. Adler*, 50 N.Y. 2d 730, 736 (1980) (holding that where an airline employee searched a package and found a large amount of pills, subsequent governmental warrantless search was not protected).

118. 318 F.3d 1039 (11th Cir. 2003).

119. *See id.* at 1041-42.

120. *Id.* at 1042.

121. *Id.* at 1043.

122. *Id.*

123. *Id.*

124. *Steiger*, 318 F. 3d at 1042-43.

that an anonymous source found a child molester on the Internet and described the pictures obtained.¹²⁵ It did not mention that the source obtained the evidence by illegal hacking.¹²⁶ The subsequent search of Steiger's computer revealed child pornography.¹²⁷

Steiger moved to suppress the evidence.¹²⁸ The federal district court denied the motion on the basis that the hacker was not an agent of the government, and the provisions of the Wiretap Act addressing suppression did not include electronic communications.¹²⁹ The Eleventh Circuit affirmed, holding that the hacker was a private party, thus the Fourth Amendment was not implicated.¹³⁰ Furthermore, the circuit court held that the hacker's conduct, although tortious, did not violate the Wiretap Act because his intrusion did not fall under the Act's classification of "interception," which, relying on analyses from Fifth and Ninth circuit cases, requires that "contemporaneous interception-i.e., an acquisition during 'flight'- is required to implicate the Wiretap Act with respect to electronic communications."¹³¹

Shortly after Steiger was indicted, FBI Agent Duffy, who was stationed in Turkey, attempted to meet with the hacker, thanked him for his assistance, informed the hacker he would not be prosecuted for his assistance, and stated that "if [he] want[ed] to bring other information forward [the agent was] available."¹³² Five months later, Duffy contacted the hacker, informed him about the trial, thanked him again, and reassured him that he would not be prosecuted if he chose to participate in the trial.¹³³

Seven months after being involved in *Steiger*, the same hacker was involved in *United States v. Jarrett*,¹³⁴ where the hacker used the same means to gain access to Jarrett's computer as he had in *Steiger*.¹³⁵ The hacker contacted Murphy, from the Alabama police, once again, asking for the contact at the FBI.¹³⁶ Murphy, after contacting the FBI, informed the unknown hacker that the FBI preferred that he "send the

125. *Id.* at 1043.

126. *Id.*

127. *Id.*

128. *Id.* at 1044.

129. *See id.* at 1044-46.

130. *Steiger*, 318 F.3d at 1046.

131. *Id.* at 1046-51.

132. *Jarrett*, 338 F.3d at 342.

133. *Id.*

134. 338 F.3d 339 (4th Cir. 2003).

135. *Id.* at 341.

136. *Id.* at 341-42.

new information to Murphy's email address."¹³⁷ Subsequently Murphy received thirteen emails with the "evidence," and Murphy sent the information to the FBI, which promptly obtained a warrant, executed a search and arrested Jarrett.¹³⁸ Several days later, FBI Agent Duffy, unaware of the hacker's involvement in *Jarrett*, contacted him to inform him of Steiger's sentence and thanked him again for his assistance.¹³⁹ The unknown hacker replied, asking why he had not heard anything regarding Jarrett, and asked Agent Duffy to have FBI Agent Faulkner contact him.¹⁴⁰

Jarrett, who initially pleaded guilty, moved to reconsider his plea based on newly-discovered evidence that, shortly after his arrest, Faulkner sent the hacker an email thanking the hacker for his assistance, and requesting that he maintain email contact with her via her personal email.¹⁴¹ One of the messages Agent Faulkner sent read:

I can not ask you to search out cases such as the ones you have sent us. That would make you an agent of the federal government and make how you obtain your information illegal and we could not use it against the men in the pictures you send. But if you should happen across such pictures as the ones you have sent us and wish us to look into the matter, please feel free to send them to us. We may have lots of questions and have to email you with the questions. But as long as you are not 'hacking' at our request, we can [use the pictures]. We also have no desire to charge you with hacking. You are not a U.S. citizen and are not bound by our laws.¹⁴²

Jarrett sought to have the evidence against him excluded as the fruit of an unlawful search, which provided the basis to secure a warrant.¹⁴³ The District Court for the Eastern District of Virginia granted the motion, holding that the government and the hacker "expressed their consent to an agency relationship."¹⁴⁴ The "totality of all the contact between [the government] and [the hacker] encouraged [the hacker] to continue his behavior and remain in contact with the FBI."¹⁴⁵

137. *Id.* at 342.

138. *Id.*

139. *Id.*

140. *Jarrett*, 338 F.3d at 342.

141. *Id.* at 342-43.

142. *Id.* at 343.

143. *Id.*

144. *Id.*

145. *Id.*

The government appealed, and the Fourth Circuit reversed, holding that the hacker's post-search contact with police was insufficient to hold the hacker as an agent of the government.¹⁴⁶ The court further stated that if Agent Duffy's communication with unknown hacker was treated as creating an agency relationship, "virtually any Government expression of gratitude for assistance well prior to an investigation would effectively transform any subsequent search by [a private] party into a Government search."¹⁴⁷ The court failed to recognize that the FBI was aware of the hacker's conduct, and instructed Officer Murphy to inform the hacker to send him the evidence obtained.¹⁴⁸ Thus, it was not only mere "gratitude," but disingenuous avoidance of direct contact by allowing Murphy to obtain all the evidence needed prior to obtaining a warrant and executing the search, that involved the "government" prior to the search.

Kline, *O'Brien*, *Steiger*, and *Jarrett* illustrate the inconsistent legal treatment of evidence obtained by individuals using Internet technology to invade one another's privacy. In each case, state law was violated: by the wife's use of spyware in *O'Brien* and the hacker's use of Trojan virus in *Kline*, *Steiger* and *Jarrett*, notwithstanding the later fate of the admissibility of the evidence obtained thereby.¹⁴⁹

The acts of hacking in *Kline*, *Steiger*, and *Jarrett* are not isolated incidents. The perception that law enforcement has been slow to

146. *Jarrett*, 338 F.3d at 347-48.

147. *Id.* at 346.

148. *Id.* at 342.

149. See ALA. CODE 1975 § 13A-8-102 (West 2003); ALASKA STAT. ANN. §11.46.484 (West 1996); ARIZ. REV. STAT. § 44-7302(A) (West 2005); ARK. CODE ANN. § 5-41-203 (West 2001); CAL. PENAL CODE § 502 (West 2001); COLO. REV. STAT. ANN. § 18-5.5-102 (West 2007); CONN. GEN. STAT. ANN. § 53a-251 (West 1984); DEL. CODE ANN. tit.11, § 932 (West 1995); FLA. STAT. ANN. § 815.06 (West 2001), § 934.03 (West 2002); GA. CODE ANN. §16-9-93 (West 1991); HAW. REV. STAT. ANN. § 708-893 (West 2006); IDAHO CODE ANN. §18-2202 (West 1984); 720 ILL. COMP. STAT. ANN. 5/16D-3 (West 2008); IND. CODE ANN. 35-43-2-3 (West 2001); IOWA CODE ANN. § 714.1 (West 2005); KAN. STAT. ANN. 21-3755 (West 1984); KY. REV. STAT. ANN. § 434.850 (West 2002); LA. REV. STAT. ANN. § 14:73.7 (West 2001); ME. REV. STAT. ANN. tit. 17-A § 433 (West 1989); MD. CODE ANN., CRIM. LAW § 7-302 (West 2008); MASS. GEN. LAW ANN. ch. 266, §120F (West 1994); MICH. COMP. LAWS ANN. 752.795 (West 1997); MINN. STAT. ANN. §609.891 (West 2006); MO. ANN. STAT. § 569.095 (West 2002); NEB. REV. ST. ANN. § 28-1343.01 (West 2008); N.H. REV. STAT. ANN. § 638:17 (West 2003); N.J. STAT. ANN. § 20-23-20-36 (West 2003); N. M. STAT. ANN., § 30-45-5 (West 2006); N.Y. PENAL LAW § 156.05 (McKinney's 2006); N.C. GEN. STAT. ANN. § 14-454 (West 2000); N.D. CENT. CODE, 12.1-06.1-08 (West 2008); OHIO REV. CODE ANN. § 2913.04 (West 2004); R.I. GEN. LAWS § 11-52-3 (West 2007); S.C. CODE ANN. § 16-16-20 (West 2002); TENN. CODE ANN. § 24.052 (effective 2009); VA. CODE ANN. § 4102 (West 1999); WIS. STAT. ANN. 943.70 (West 2002); W. VA. CODE ANN. §61-3C-5 (West 1989); WYO. STAT. ANN. § 6-3-504 (West 2008).

respond to growing computer crime has resulted in the formation of hacker groups that have targeted crimes such as child pornography.¹⁵⁰ Once these computer vigilante groups become aware of a possible problem, they report it to law enforcement, and if nothing is done, gain access to the suspect's computer and erase the suspected illegal material.¹⁵¹ Whether this is due to police inaction or impatience, such actions demonstrate police failure to react. Some people in the law enforcement community (and perhaps the general public) see child pornography as such a horrible crime that they do not mind the hackers invading the sanctity of a computer.¹⁵² Others believe that allowing such intrusion in the "cyber" world encourages physical intrusions that are unanimously held to be unacceptable.¹⁵³

The Fourth Amendment analysis in *Kline*, *Steiger* and *Jarrett* is troubling. Although the circuit courts have been consistent with each other, there is an underlying problem with Fourth Amendment jurisprudence in the digital age that becomes evident when one compares the appellate and trial courts. Whether an individual is a government agent is a fact-specific inquiry within the sound discretion of the trial judge. However, without a clear factor-specific test for government acquiescence and knowledge regarding hackers who intend to assist law enforcement, decisions in the courts at the trial and appellate level will remain inconsistent. The Courts of Appeal have interpreted the agency relationship as a question of law and have taken the discretion away from the trial judges.¹⁵⁴ The inconsistency becomes apparent when cases such as *Kline* and *Jarrett* are compared with *Steiger*. Today, a clear definition or set of factors to determine when a person qualifies one as an agent of the state, especially in the context of computer invasions, is crucial.

In *Steiger*,¹⁵⁵ the unknown user was really unknown to the government.¹⁵⁶ There were no facts to suggest that he ever contacted the government, assisted in any government operations regarding computer crime and never was at the mercy of governmental prosecutorial discretion regarding any previously committed crimes. Therefore, the court in *Steiger* rightly concluded that the unknown

150. MOORE, *supra* note 1, at 53.

151. *Id.* at 53-54.

152. *Id.* at 54.

153. *Id.*

154. *See generally Kline*, 112 F. App'x at 564; *Jarrett*, 338 F.3d at 345-46.

155. 318 F.3d 1039 (11th Cir. 2003).

156. *See id.* at 1046.

hacker was a private party and the search did not implicate Fourth amendment protection.¹⁵⁷ For this reason, Steiger was forced to turn to the Federal Wiretap and Stored Communications Acts to argue against the evidence.¹⁵⁸

The background facts in *Kline* and *Jarrett* tell a different story, and demonstrate the importance of a factor-based test in interpreting governmental acquiescence and knowledge. Willman, the “hacker-hero” of *Kline*, was a Canadian citizen who held himself out as a law enforcement informant who had “provided ‘evidence packages’ in various cases to law enforcement in the United States . . . since 1998 or 1999.”¹⁵⁹ Willman had worked with American law enforcement in the past, prior to the search of Kline’s computer; he was requested by United States law enforcement to provide assistance regarding a Russian pornography ring.¹⁶⁰ In addition, “[h]e was known to the United States law enforcement agencies to possess and sell large amounts of child pornography in the United States.”¹⁶¹ Willman himself was arrested at a child sex solicitation scene and when he provided information to Canadian authorities, he was released and never charged.¹⁶² Through the use of “Pedowatch,” an Internet-based watchdog group, Willman arranged a meeting with Detective Carr of the Irvine Police Department and informed him that he “considered himself an informant who worked for United States Customs.”¹⁶³ At the meeting, he informed Carr of 2,000-3,000 prior invasions similar to his invasion of Kline’s computer.¹⁶⁴ Also, although Willman did not receive “financial compensation and [was] not logged as a United States informant, he was offered financial consideration and promised he would not be arrested and [be] a suspect in any crime.”¹⁶⁵ Willman was subsequently offered “two new hard drives . . . [and] although it was known to law enforcement that Willman possessed an extensive collection of child pornography . . . he was never arrested or searched and was permitted to keep his . . . collection.”¹⁶⁶ Willman, a possessor

157. *See id.* at 1045.

158. *Id.* at 1046.

159. Petition for Writ of Cert., *supra* note 7 at *3.

160. *Id.* at *5.

161. *Id.* at *4.

162. *Id.*

163. *Id.* at *6.

164. *Id.*

165. Petition for Writ of Cert., *supra* note 7 at *6.

166. *Id.* at *7.

of child pornography himself, received immunity for helping law enforcement and not only went unpunished, but was rewarded.

Similarly in *Jarrett*,¹⁶⁷ the unknown hacker provided information to FBI agents prior to his search of Jarrett's computer.¹⁶⁸ The hacker was informed by the FBI that he would not be prosecuted and was "encouraged" to bring more information forward.¹⁶⁹ He wrote to FBI Agent Duffy who was stationed in Turkey, asking him why the FBI Agent Faulkner had not contacted him.¹⁷⁰ This communication shows the hacker's subjective belief that the FBI was one entity, and assumed that all agents know of what is going on in the agency. Even if this communication is found insufficient, the court concluded that the email Agent Faulkner sent to the unknown hacker can "only be characterized as [a] proverbial 'wink and a nod.'"¹⁷¹

Although the trial courts in both cases held that the hacker was an agent of the state and the consent and knowledge of the government was sufficient, the circuit courts in both cases reversed.¹⁷² Such inconsistency proves the necessity of establishing not only a test to apply to private individual participating in unauthorized computer invasions when helping law enforcement, but a test to require the courts to balance factors in determining the level of acquiescence and government knowledge.

Such factors should include, but are not limited to: prior connection between the hacker and the government, the extent of the communication, the substance and purpose of it, the way the hacker and the government communicate, if the hacker obtains any gain from dealing with law enforcement (such as monetary payments, gifts, and immunity from prosecution), prior acts of the hacker (such as any illegal activity and criminal record), and any private gain obtained by the hacker in his actions of intruding another's computer. These factors will assure that the hacker is truly independent of law enforcement and is not hacking with malicious intent or intending to cover up his or her own wrong doing by shifting the blame and attention of wrong doing to another party.

167. 338 F.3d at 342.

168. *Id.* at 341 (referring to evidence presented to law enforcement officers that resulted in arrest of the defendant in *United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003)).

169. *Id.* at 343.

170. *Id.* at 342.

171. *Id.* at 343.

172. See *Kline*, 112 F. App'x at 562; *Jarrett*, 338 F.3d at 339.

Further, the contact with law enforcement should be applied broadly. The government should not be allowed to impliedly consent to a hacker's illegal activities and "turn the blind eye" to such activity. If an FBI agent knows and impliedly acquiesces in a hacker's intrusive search, without informing the hacker that he is participating in an illegal activity and should refrain from doing so, this gives the hacker an impression that the United States government is fully aware of, and acknowledges, his activities. In addition, the lack of explicit directions to refrain from such actions provides an incentive for the hacker to keep engaging in illegal actions, knowing that he will not be punished.

The narrow interpretation given to the consent and knowledge of the government by the court makes the "agent" test illusory. By applying it, the courts suggest that a hacker is only deemed an "agent of the state" if he is an "agent of the city," an "agent of the governmental agency," or an "agent of a governmental agent" who had specific knowledge of his activity. Such narrow application is preposterous and unnecessary.

Law enforcement has other ways to seek out criminals, such as Stieger, Kline and Jarrett. A law enforcement officer can enter a chat room and request that someone send pictures over the Internet. Once such pictures are sent, the subjective expectation of privacy disappears; law enforcement has now acquired lawful probable cause and may pursue further action. The Fourth Amendment applies to searches by the government or its agent of areas where one has an expectation of privacy which society is willing to accept as reasonable. Once exposure takes place, the Fourth Amendment protection disappears. If bank documents are given to a bank, the privacy interests in the documents disappear,¹⁷³ and the government may inspect them without obtaining a warrant.¹⁷⁴ But there is a substantial difference between having the document stolen out of a home or a computer, and the document or image being voluntarily discarded or transmitted to a third party, thus abandoning the expectation of privacy.

The Internet works through the sharing and disclosure of information to any other computer connected to the network.¹⁷⁵ The moment a computer connects to the Internet, information is exchanged between the computer and the server, the server and the websites a user

173. See *United States v. Miller*, 425 U.S. 435, 443 (1976).

174. See *California v. Greenwood*, 486 U.S. 35, 40-41 (1988); *Miller*, 425 U.S. at 443.

175. See Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How A Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 813 (2003).

visits, and the computer and another computer. At least one commentator has suggested that the Fourth Amendment may never be applicable when the Internet is involved because “the Fourth Amendment does not protect information that has been disclosed to third-parties, and the [I]nternet works by disclosing information to third parties.”¹⁷⁶ So what protections do individuals have when computer technology and crime are at issue and the Fourth Amendment is inapplicable? Is Congress allowing the Internet to eviscerate constitutional guarantees?

III. STATUTORY APPROACHES TO THE PROTECTION OF COMPUTER PRIVACY

Bearing in mind the problems posed by the advancement of technology and the Fourth Amendment, Congress enacted statutes attempting to preserve the right of privacy.¹⁷⁷ Congress’s “answer” to *Katz* is found in Provision III of The Omnibus Crime Control and Safe Streets Act of 1968.¹⁷⁸ Provision III of the Act had a dual purpose: “1) protecting the privacy of wire and oral communications, and 2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized.”¹⁷⁹ In *Gelbard v. United States*,¹⁸⁰ the Court commented on Title III, saying that “although [it] authorizes invasion of individual privacy under certain circumstances, the protection of privacy was an overriding congressional concern.”¹⁸¹ Even with the development of new technology, Congress was still adamant about individual privacy and the Court extended the judge-made exclusionary rule to this context, stating that “the perpetrator must be denied the fruits of his unlawful action in civil and criminal proceedings.”¹⁸²

Congress realized that computers would not only pose invasion of privacy problems, but problems with the courts’ application of the Fourth Amendment to computers, and therefore amended the Wiretap Act to include electronic communication.¹⁸³ The Omnibus Crime Control and Safe Streets Act of 1968 was amended by Title I of the

176. *Id.* at 814.

177. *See Gelbard v. United States*, 408 U.S. 41, 48 (1972).

178. Codified in 18 U.S.C. § 2510-2520 (2006).

179. *Gelbard*, 408 U.S. at 48.

180. 408 U.S. 41 (1972).

181. *Id.* at 48.

182. *Id.* at 50.

183. 18 U.S.C. § 2510 (2006).

Electronic Communications Privacy Act (ECPA) in 1986, which was codified as the “Federal Wiretap Act.”¹⁸⁴ At the same time, Title II of the ECPA created the Stored Communication Act (SCA) to cover access to stored communications and records.¹⁸⁵ The enactment and codification of the statutes prove that Congress is attempting to deal with the ever-growing “virtual world” privacy problem.

The Federal Wiretap Act makes it illegal for any person to intentionally intercept, disclose or use, or procure another to intercept, disclose or use any electronic communication, knowing the information was obtained through a violation of the Act.¹⁸⁶ This expressly shows that Congress intended the Act to apply to both the government and private individuals by use of the language “any person.”¹⁸⁷ The Act also prohibits any person from intentionally sending, manufacturing, assembling, possessing or selling any electronic, mechanical or other device, knowing or having reason to know that the design of such device is to be used primarily for the purpose of surreptitious interception of oral, wire or electronic communication.¹⁸⁸ Any device used in violation of sections 2511 and 2512 of the Act may be seized and forfeited to the United States government.¹⁸⁹ In addition, “[w]henever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence.”¹⁹⁰

But under the prevailing interpretation of the Wiretap Act, some individuals who have been accused on the basis of electronically-obtained evidence have been left without a possible defense.¹⁹¹ This has occurred for two reasons. First, unlike the Fourth Amendment, violation of the Wiretap Act does not trigger the exclusionary rule, which would require suppression of evidence gained through intercepted *electronic* communications.¹⁹² The Act specifically left evidence derived from interception of electronic communication admissible. Section 2515 states that “whenever any *wire or oral* communication has been intercepted, no part of such communication

184. 18 U.S.C. §§ 2510-2520 (2006).

185. 18 U.S.C. § 2701(a) (2006).

186. 18 U.S.C. § 2511 (2006).

187. 18 U.S.C. § 2511(1) (2006).

188. 18 U.S.C. § 2512(1)(a) and (b) (2006).

189. 18 U.S.C. § 2513 (2006).

190. 18 U.S.C. § 2515 (2006).

191. See *Jarrett*, 338 F.3d at 339; *Steiger*, 318 F.3d at 1039; *Kline*, 112 F. App'x at 562.

192. 18 U.S.C. § 2515 (2006).

and no evidence derived therefrom may be received in evidence in any trial”¹⁹³

This major flaw leaves individuals whose privacy has been violated illegally without the most powerful remedy known to American criminal law. The only remedy provided by the Act to victims of wrongful interception of electronic communication is a civil suit for damages, under § 2520 of the Act which provides that “any person whose . . . electronic communication is intercepted, disclosed or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in th[e] violation such relief as appropriate.”¹⁹⁴ However, in criminal cases, few people even bother to sue, because most victims “care more about staying out of jail than bringing a lawsuit against the[ir] [intruder] for money damages.”¹⁹⁵

Second, the “protection gap” against unlawful computer intrusion created by the Act becomes even more apparent when one understands how certain terms are defined. “Electronic communication” under the Wiretap Act is broadly defined as “any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by . . . electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.”¹⁹⁶ “Interception” is defined as “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.”¹⁹⁷ “Interception” has been held only to apply to contemporaneous acquisitions.¹⁹⁸

The problem with this interpretation was identified in *Steiger*, when the court noted that “there is only a narrow window during which an E-mail interception may occur—the seconds or milli-seconds before . . . [the] message is saved to [a] temporary location . . . [t]herefore . . . interception of E-mail within the prohibition of the Wiretap Act is virtually impossible.”¹⁹⁹ Therefore, the Wiretap Act functions differently with regard to protecting victims of spyware as opposed to victims of the Trojan virus, the more intrusive of the two.

193. 18 U.S.C. § 2515 (Emphasis added).

194. 18 U.S.C. § 2520(a) (2006).

195. Kerr, *supra* note 175, at 812.

196. 18 U.S.C. §2510 (12) (2006).

197. 18 U.S.C. §2510 (4) (2006).

198. See *Konop v. Hawaiian Airlines, Inc.* 302 F.3d 868, 878-79 (9th Cir. 2002); *Steve Jacksons Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 460 (5th Cir. 1994).

199. *Steiger*, 318 F.3d at 1050 (quoting Jarrod J. White, *E-mail @Work.com: Employer Monitoring of Employee Email*, 48 ALA. L.REV. 1079, 1083 (1997)).

Spyware “copies the communication as it is transmitted and routes the copy to a storage file in the computer.”²⁰⁰ In *O’Brien*, the wife “intercepted” (in the Act’s terms)—“electronic communication,” and the court, utilizing judicial discretion, discarded the evidence.²⁰¹ In the criminal cases discussed, the Trojan virus was used to enter the unknown victim’s hard drive. Because the virus gives access to everything, it captured much *more* than what the Act defines as “interception” of “contemporaneous communications.”²⁰² So what protection does stored information and communications have?

The “Stored Communications Act” (SCA) was enacted specifically to address access to stored electronic communication and transactional records.²⁰³ But the SCA only protects against intrusions into “facilit[ies] through which an electronic communication service is provided.”²⁰⁴ Such unauthorized access has criminal and civil penalties, but no exclusion remedy if one “obtain[s], alter[s], or prevent[s] unauthorized access. . . while it is in electronic storage in a [facility].”²⁰⁵ It further provides that electronic communication service is “any service which provides users. . . the ability to send or receive . . . electronic communication.”²⁰⁶ Thus, under this definition the SCA protects Internet Service Providers from intrusions, but not personal hard drives on computers. In the case of *Kline, Steiger, and Jarrett*, the SCA did not apply because “there is no evidence to suggest that [the] computer maintained any ‘electronic communication service.’”²⁰⁷

The two statutes have caused much confusion in the courts. For example, *Stieger*, without a Fourth Amendment defense, hoped to rely on the Federal Wiretap Act, to suppress the evidence against him.²⁰⁸ The court described its frustration with the interpretation of the Federal Wiretap Act, stating

[T]he intersection of these two statutes is a complex, often convoluted area of law. The difficulty is compounded by the fact that the ECPA was written prior to the advent of the [Internet]. As a result, the existing statutory framework is ill-

200. *O’Brien*, 899 So. 2d at 1137.

201. *Id.* at 1037-38.

202. *Steiger*, 318 F.3d at 1050.

203. *See Hawaiian Airlines, Inc.*, 302 F.3d at 874 (citing S. REP. NO. 99-541, at 3 (1986)).

204. 18 U.S.C. § 2701 (a)(1) (2006).

205. 18 U.S.C. § 2701(a); *see also* 18 U.S.C. §§ 2707, 2708 (2006).

206. 18 U.S.C. § 2510 (15) (2006).

207. *Steiger*, 318 F.3d at 1051.

208. *See id.* at 1051.

suites to address modern forms of communications . . . Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying result[s].²⁰⁹

Nevertheless, the *O'Brien*²¹⁰ court held that the “conspicuous[] absen[ce] from the provisions of the [Act of] any reference to electronic communication [shows that]. . . Congress intended that such communications not be excluded under the Federal Wiretap Act.”²¹¹ At the same time, however, the enactment of the ECPA and SCA shows an intention to protect individual privacy.²¹² There is no reason to assume that Congress’ lack of reference to electronic communications shows an intention to permit intrusion and invasion of privacy by hackers. Although 18 U.S.C. §2518(10)(a) explains that the only remedies available are the sanctions described in the chapter, subsection 101(e) of the Electronic Communications Privacy Act provides that if the violation of law is of constitutional magnitude, the court involved will apply existing constitutional law with respect to the exclusionary rule.²¹³ But when any court fails to recognize the findings of fact in relation to the Fourth Amendment agency relationship, such protection under the ECPA becomes minuscule.

CONCLUSION

The Ninth Circuit has noted,

The ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication . . . Until congress brings the laws in line with modern technology, protection of the Internet . . . will remain a confusing and uncertain area of the law.²¹⁴

Congress should enact a statute which allows a suppression remedy for illegally-obtained evidence in both civil and criminal trials. Because the Federal Wiretap Act only protects contemporaneous

209. *Id.* at 1046 (quoting *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002)).

210. 899 So. 2d at 1133 (Fla. Dist. Ct. App. 2005).

211. *Id.* at 1138.

212. The language of the ECPA and SCA punishes various forms of intentional disclosure of information, and use of information obtained by intercepting oral, wire or electronic communication.

213. 18 U.S.C. § 2518(10)(c) (2006).

214. *Steiger*, 318 F.3d at 1047 (quoting *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002)).

communications and the Stored Communications Act protects only information stored on a facility which provides service to sending or receiving electronic communication, there is no protection for someone who has been prosecuted or convicted on the basis of illegally-obtained evidence.

More privacy protection will be afforded if a combination of the Wiretap Act and the SCA are combined to create a statute which reads:

(a) Whoever —

(1) intentionally accesses, endeavors to access, or procures any other person to access a personal, commercial or any other computer without authorization or exceeding authorized access by the use of any electronic, mechanical or any other device; or

(2) Intentionally discloses, endeavors to disclose, or procures any other person to disclose, to any other person the contents of any information obtained by section (1),

shall be subject to forfeiture, to the agency involved in the investigation, of the electronic, mechanical or any other device used in the access and/or disclosure of the information obtained by section (1).

(b) Whenever any oral, wire or electronic communication and/or information has been obtained or disclosed in violation of this chapter, no part of the contents and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States.

The evolution of technology requires such protection to preserve the right to privacy we all seek. Such means that are available in the real, material and tangible world disappear when taken place in the virtual world.

One need not be indifferent to any of the crimes committed by the defendants in the cases discussed herein to believe those defendants deserve the same due process when their life and liberty is at stake, as any other criminal possesses in our society. Whether the courts have let the nature of the crime affect the decision and “taint” the application of the law is unclear, but perhaps the perspective would be different if, instead of child pornography, the government “merely acquiesced” or used intermediary “watchdog” Internet groups to contact hackers who obtained financial records from hard drives in a search for evidence of tax fraud or a similar offense.

A statute targeting the invasion of a personal hard drive by hacking which subjects a computer hacker to a search of the computer used for

his crimes, and provides a suppression remedy for his victim, will discourage law enforcement from “turning the blind eye” or using intermediaries to either contact or request information from hacker and evade the Fourth Amendment. It will also prevent hackers with dubious motives from “covering” their own crimes by shifting the blame to another. A factor-based test in regards to the level of government acquiesce and knowledge to a hacker, as mentioned above, is also necessary to provide a balance between protection of society from immoral crimes and the right to freedom and privacy ever so enumerated in our constitution. “The compilation of data [in our personal computers] about the intimate details of our day-to-day existence may impair fundamental rights [such as] privacy guaranteed by the constitution,”²¹⁵ if nothing is done about the preservation of privacy in the face of hacking.

*Sagi Schwartzberg**

215. JONATHAN ROSENOER, CYBER LAW: THE LAW OF THE INTERNET 51 (Springer Publishing 1996).

* J.D. expected 2010, University of La Verne College of Law. Thank you Professor Diane J. Klein and Phillip Argento for their tremendous assistance and guidance during this process. I would also like to thank my family and friends for your patience and understanding throughout.