UIC John Marshall Journal of Information Technology & Privacy Law

Volume 22
Issue 2 *Journal of Computer & Information Law - Winter 2004*

Article 5

Winter 2004

The Fourth Amendment and the Wiretap Act Fail to Protect Against Random ISP Monitoring of E-mails for the Purpose of Assisting Law Enforcement, 22 J. Marshall J. Computer & Info. L. 493 (2004)

Jim W. Ko

COMMENT

THE FOURTH AMENDMENT AND THE WIRETAP ACT FAIL TO PROTECT AGAINST RANDOM ISP MONITORING OF E-MAILS FOR THE PURPOSE OF ASSISTING LAW ENFORCEMENT

JIM W. KO†

I. INTRODUCTION

With the United States government's post 9-11 calls for public vigilance and assistance in the War on Terrorism[1] combined with the vast increase in crimes involving computers and the Internet,[2] challenges on privacy grounds of searches conducted by private actors including Internet Service Providers (ISPs) will be heard more and more in the courts.

The increased threat to our privacy in the computer age is evident in two recent Federal Circuit cases involving the same private vigilante child-porn fighter.[3] Despite the fact that the only incriminating evidence in either case was obtained by the vigilante's hacking into private home computers via the Internet, both Circuit courts allowed the evidence. Both courts not only failed to hold that the vigilante was constructively

† B.S., Biology, Duke University, December 1995. Ed.M., Harvard Graduate School of Education, June 1997. J.D., Case Western Reserve University School of Law, January 2004. Associate, Howrey Simon Arnold and White, LLP, starting Fall 2004. I would like to thank Professor Lewis R. Katz for his guidance on this project, and throughout my time in law school.

1. "And as government works to better secure our homeland, America will continue to depend on the eyes and ears of alert citizens." George W. Bush, *President Delivers State of the Union Address*, <http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html> (Jan. 29, 2002).

2. *See generally* Daniel A. Morris, *U.S. Attorney's Bulletin: Tracking a Computer Hacker*, <http://www.cybercrime.gov/usamay2001_2.htm> (updated July 10, 2001).

3. *U.S. v. Steiger*, 318 F.3d 1039 (11th Cir. 2003); *U.S. v. Jarrett*, 338 F.3d 339 (4th Cir. 2003). For a full discussion of these cases, *see infra*, pt. IV.C.iv.2.

working as a government agent even though the FBI agents had previously promised him amnesty from prosecution, but they failed to raise even the mildest of criticism toward the FBI agents for their acquiescence in, if not active encouragement, of such unlawful behavior. This threat to privacy will increase exponentially if courts allow such collusion when the private actor is an ISP, such as America Online (AOL), which has the capability to monitor (albeit in a limited fashion)[4] and record every single e-mail communication sent or received on its systems.

What protections exist against ISPs randomly monitoring our e-mails for the purpose of turning over any evidence of criminal activity so discovered to law enforcement officials? The two primary defenses against invasions of privacy in cyberspace are the Fourth Amendment and the *Omnibus Crime Control and Safe Street Act of 1968*[5] (popularly referred to as "Title III" or the *Wiretap Act*), as amended in 1986 by the *Electronic Communications Privacy Act* (ECPA) to also cover electronic communications such as e-mails.[6] This article, however, will demonstrate that these two statutory defenses provide little if any protection against this unprecedented threat to everyday privacy.

Part II of this article will provide a background discussion on the special privacy issues that arise in the context of computer technology and ISPs. Courts have yet to clearly define the level of society's expectation of privacy in e-mails stored in the systems of ISPs. In Part III, the *Wiretap Act*, as amended by the ECPA, will be analyzed to reveal that an implicit statutory prohibition against random surveillance by ISPs for the purpose of assisting law enforcement does in fact exist. The remedies for violations of this provision, however, are lacking as they include neither the exclusionary rule, nor criminal sanctions, and furthermore, are riddled with exceptions. Part IV will examine recent court decisions that collectively suggest the Fourth Amendment does not protect against evidence obtained from such ISP surveillance, even if the government encourages it through general cash rewards or promises of immunity from prosecution. Finally in Part V, this article will conclude by providing suggestions as to how the public's privacy interests against random ISP monitoring can and should be protected.

II. COMPUTER TECHNOLOGY, ISP'S, AND THE FOURTH AMENDMENT

Under current law, every e-mail we send or receive can be randomly monitored to some degree by ISPs, and then disclosed to the government.

4. *See infra*, pt. II.A.1.

5. Pub.L. 90-351, Title III, § 802, June 19, 1968, 82 Stat. 212.

6. Pub.L. 99-508, Title I, §101(a), (c)(1)(A), (4), Oct. 21, 1986, 100 Stat. 1848, 1851; Pub.L. 99-508, Title II, §201[a], Oct. 21, 1986, 100 Stat. 1860.

Admittedly, there is a reduced expectation of privacy in e-mail communications compared to protecting oral or telephone communications, because e-mails are stored and retrievable. Nevertheless, most people would view random monitoring of our e-mails by ISPs or the government as an unacceptable violation of privacy.[7] The courts have failed to clearly define what society's level of expectation of privacy is in e-mails as a whole, whether during transmission or while stored in an ISP's system.[8]

A. ISPs Have the Technology and the Incentive to Monitor All E-mail Communications Within Their Systems

ISPs have both the technology and the incentive to monitor all communications transmitted by their customers through their systems.[9] In the computer age, the possible scope of electronic surveillance is incomparable. Moreover, despite modern day society's heavy reliance upon e-mail as a primary means of communication, ISPs have a broader right to conduct random monitoring of their systems than telephone companies have under the *Wiretap Act*. Individuals and organizations also are more likely to conduct computer surveillance than other previous forms of surveillance, as it is more likely to go undetected by the victims. Furthermore, the government can and does raise a "special needs"[10] argument for a lessening of Fourth Amendment protections and for the aid of private citizens, including ISPs, to combat both child pornography and terrorism.[11]

1. *The Incomparable Potential Scope of Computer Surveillance*

With such tools as keyword searches,[12] key-logger[13] and Trojan horse[14] programs, the possible scope of computer surveillance is unprecedented.

---

7. *See* Sylvia Dennis, *ComputerUser.com News: Monitoring Worries Young Users*, <http://www.computeruser.com/newstoday/00/03/08/news13.html> (March 8, 2000).

8. *Infra*, pt. II.B.

9. *See e.g.* Laura Rohde, *PCWorld.com - Privacy Issues Plague Google's Gmail*, <http://www.pcworld.com/news/article/0%2Caid%2C115692%2C00.asp> (accessed July 8, 2004) (With its new free web-based e-mail service called Gmail, "Google is planning to scan e-mail and add advertisements that it thinks are relevant to the messages. Additionally, the Gmail privacy policy warns that messages, even if "deleted" by a user, may still be stored in the system, even long after users have closed their accounts. . . .").

10. *See infra*, pt. II.A.4.a.

11. *See infra*, pt. II.A.4.b.

12. *See infra*, pt. II.A.1.a.

13. *See infra*, pt. II.A.1.b.

14. *See infra*, pt. II.A.1.b.

a. Keyword searches

A user of the popular e-mail program Eudora who clicks on the send button after writing a somewhat vituperative or risqué e-mail message may be in for a surprise. If the setting for Eudora's "Mood Watch"[15] application is turned on, the user will hear a warning chime and discover that Eudora instantaneously has halted the transmission of this message. Eudora will post a warning that this message includes very strong language that might be offensive toward others, and will ask whether the user is certain he/she wants to send it. The user may feel like his/her privacy has been violated, and wonder who it was that read and evaluated the content and tone of this e-mail, all without permission.

This "Mood Watch" application of Eudora's serves as a perfect example of how keyword searches work, and how the public is both right and wrong in its fears of computer surveillance and the coming of Orwell's Big Brother. Nobody, not a Eudora employee, an ISP employee, or anyone else has read this e-mail. At least not yet. It is in fact exceedingly unlikely that anybody besides the recipient ever will.

Unless the "Mood Watch" setting is turned off, Eudora, and other e-mail programs like it, automatically run a keyword search on every e-mail sent or received. This keyword search operates somewhat like search engines such as Yahoo! and MSN do, or the "Find" feature on word processors such as Microsoft Word.[16] These e-mail programs keep a database of possibly offensive words in the English language, scan every word in a given e-mail, and cross-reference each word with this database. They run some sort of algorithm which assigns a point value for each offensive word and keeps a tally of an e-mail's total "offensiveness" score.[17] If this score exceeds some predetermined figure, then the programs temporarily halt transmission of the e-mail as described above.

This procedure is carried out in this case for the benefit of users, to help prevent them from inadvertently sending out what could be interpreted as offensive e-mails. This same exact procedure is executed by junk e-mail blocking filters, which run a similar keyword scan on the titles and/or contents of all incoming e-mails.[18]

Some people may argue that such a keyword search is in it of itself a violation of privacy. According to Raymond Ku, however, current Fourth

---

15. *See Eudora 6.1:Moodwatch* <http://www.eudora.com/email/features/moodwatch.html> (accessed July 8, 2004).

16. *See* Danny Sullivan, *SearchEnginewatch - How Search Engines Work*, <http://www.searchenginewatch.com/webmasters/article.php/2168031> (October 14, 2002).

17. *See Eudora 6.1: Moodwatch*, <http://www.eudora.com/email/features/moodwatch.html> (accessed July 8, 2004).

18. *See Help Prevent Junk E-mail Messages with Outlook 2003*, <http://www.microsoft.com/office/editions/prodinfo/junkmail.mspx> (accessed July 8, 2004).

Amendment law suggests that the use of this type of surveillance technology, employed for instance in part by the controversial FBI "Carnivore" program,[19] is not a search to begin with, as it is "[never] viewed by human eyes, thus minimizing intrusion, embarrassment, and inconvenience."[20]

This automated search, however, may very well lead to human eyes passing over documents flagged by this process, which does give rise to Fourth Amendment implications. In fact, in contexts other than the Eudora "Mood Watch" application, this may well be the very purpose for conducting the keyword search to begin with. The government can and does use information gained from keyword searches as the basis for warrant applications for continued investigations on individuals, both previously targeted and untargeted. Furthermore, ISPs, or more likely, individual overzealous ISP employees, may decide to keep track of certain individual users that consistently send high offensiveness scoring messages, and individually read their e-mails.

The government can apparently run a keyword search program without first obtaining a search warrant, but if it wants to conduct subsequent and more thorough searches based on this initial search, it must first obtain a search warrant, or else risk having any evidence so obtained excluded under the Fourth Amendment. In contrast, however, unless ISPs are deemed by a court to be acting as an agent of the government, there is no such restraint, other than the threat of possible civil liability[21] against ISPs following up on initial keyword searches, or the government's use of evidence so obtained.

b. Key-logger and Trojan horse programs

Whereas keyword searches are typically applied to e-mails that have already been sent from personal computers into the World Wide Web, there are more intrusive computer searches such as key-logger and Trojan horse programs that invade home computers themselves. Key-logger programs, when installed on a home computer, record every keystroke entered on the computer.[22] Trojan horses can be inadvertently downloaded onto a home computer, much like a virus, and then used to allow outside users to enter, search, and use the computer undetected

19. Carnivore is an FBI device capable of collecting and monitoring all online activities, targeting particular forms of activity and/or activity from particular agents with fairly high specificity. *See* Raymond Ku, *Modern Studies in Privacy Law: Searching for the Meaning of Fourth Amendment Privacy after Kyllo v. United States*, 86 Minn. L. Rev. 1325, 1355-56 (2002).

20. *Id.* at 1356.

21. *See infra*, pt. III.B.4.

22. *U.S. v. Scarfo*, 180 F. Supp. 2d 572, 574 (D.N.J. 2001).

via the Internet.[23] Both key-logger and Trojan horse programs could conceivably be utilized by law enforcement officials (upon obtaining a proper search warrant) and ISPs to follow up on initial keyword searches.

In *United States v. Scarfo*, a New Jersey district court held that the use of key-logger programs by law enforcement officials to determine a suspect's computer password for opening encrypted files was not in violation of the *Wiretap Act*.[24]

U.S. courts have yet to hear a case involving the use of Trojan horse programs by the government. Trojan horses were, however, attached to pornographic images posted on the Internet as bait by a vigilante child-pornography fighter in the recent twin Circuit Court cases of *United States v. Steiger*,[25] and *United States v. Jarrett*.[26] In both cases, evidence obtained and discovered by this hacker for the purpose of assisting law enforcement officials was deemed admissible by the courts.

2. *Under the Wiretap Act, As Amended by the ECPA, ISPs Have Broader Rights to Conduct Random Monitoring Than Telephone Companies*

Unlike telephone companies, ISPs have the unrestricted right under the *Wiretap Act*, as amended by the ECPA, to randomly monitor their systems if necessary for the rendition of their services, or to protect their rights or properties.[27] Therefore, ISPs have the right to randomly monitor all e-mails sent or received on their systems for purposes including combating user fraud and scanning for viruses. A natural by-product of such random monitoring is that ISP monitors are more likely to accidentally come across evidence of criminal activity.

Courts have consistently held that any evidence of criminal activity obtained by service providers while conducting such monitoring for the protection of their systems is admissible.[28]

3. *Computer Surveillance is More Likely to Go Undetected Than Other Forms of Surveillance*

Computer surveillance, especially using keyword searches, is much more likely to go undetected than other forms of surveillance. A natural control against peeping toms or any form of illegal activity is the fear of

---

23. *Jarrett*, 338 F.3d at 341.

24. 180 F. Supp. 2d at 581.

25. 318 F.3d 1039 (11th Cir. 2003).

26. 338 F.3d at 339.

27. For a full statutory analysis of the relevant Title III provisions, *see infra*, pt. III.B.3.

28. For full discussion, *see infra*, pt. IV.C.2.

getting caught. When this fear is reduced to near zero, as is the case when advanced users decide to spy on the private lives or computers of everyday users, then incidents of illegal surveillance, public or private, naturally increase. This is particularly the case when criminal penalties and the exclusionary rule are not made available as remedies, as is the case with ISP surveillance of stored e-mails.[29]

The typical keyword search is impossible to defend against. They usually entail monitoring conducted by or with the assistance of ISPs within their own internal systems. The subject of the ISP search has no way of knowing that such a search is being conducted.

Advanced users can theoretically monitor and defend themselves against more invasive searches conducted on their own home computers through the Internet, such as key-logger programs and Trojan horses. Firewall and anti-virus programs can be installed and operated to guard against such forms of surveillance. Even the best defenses, however, can be penetrated, as is evident by the periodic news reports of widespread computer viruses successfully shutting down even highly protected networks such as those operated by the government or big business. More importantly, the average user simply does not have the know-how to install or maintain adequate defenses against such privacy threats.

Once a keyword search, key-logger, or Trojan horse program is successfully installed on a home computer, they will in most circumstances be able to run undetected indefinitely. For example, the author used the e-mail program Eudora for over a year before discovering (and only through Eudora's own disclosure) the "Mood Watch" feature's existence, despite the fact that Eudora had in all likelihood been running this keyword search with every e-mail sent and received the entire time.[30]

4. *The Government's "Special Needs" Argument for the Lessening of Fourth Amendment Protections and for the Aid of Private Citizens to Combat Child Pornography and Terrorism*

The New Jersey district court in *Scarfo* provided an overview of the tensions inherent in the Fourth Amendment implications of computer surveillance.[31] It first declared: "Let there be no doubt that the courts are indeed the last bastions of freedom in our society and serve to protect the individual liberty rights embedded in our Constitution."[32] It continued, noting the necessity for continual vigilance "against the evisceration of Constitutional rights at the hands of modern technology."[33]

29. For full discussion, *see infra*, pt. III.B.4.
30. *See supra*, pt. II.A.1.2.
31. *Scarfo*, 180 F. Supp. 2d at 574.
32. *Id.* at 582.
33. *Id.* at 583.

The court, however, reversed field in noting that:

> [I]t is likewise true that modern-day criminals have embraced technological advances and used them to further their felonious purposes. Each day, advanced computer technologies and the increased accessibility to the Internet means criminal behavior is becoming more sophisticated and complex. This includes the ability to find new ways to commit old crimes, as well as new crimes beyond the comprehension of courts. As a result of this surge in so-called 'cyber-crime,' law enforcement's ability to vigorously pursue such rogues cannot be hindered where all Constitutional limitations are scrupulously observed.[34]

Examples of such new challenges for law enforcement include the fight against child pornography and the War on Terrorism. The government raises, and the courts implicitly recognize, a "special needs" argument for the lessening of Fourth Amendment protections and the assistance of private citizens for combating these forms of crime(s).

a. Child pornography

In *United States v. Perez*, a New York district court outlines the difficult balance between protecting the Fourth Amendment and fighting child pornography.[35] The court notes that:

> On the one hand, child pornography and the sexual abuse of children are crimes that have been fueled by the [I]nternet, as those who would exploit children have sought to take advantage of the [I]nternet's vast and largely anonymous distribution and communications network. On the other hand, when law enforcement gathers information about the activity of individuals on the [I]nternet, the potential for unreasonable intrusions into the home – the chief concern of the drafters of the Fourth Amendment – is great.[36]

Although the *Perez* court itself fell on the side of upholding the Fourth Amendment due to the government agent's "deliberate [and] reckless misstatement in an affidavit [in this case,]"[37] it is hard to imagine that the courts do not factor in the egregiousness of the crimes of child exploitation, or the lack of power of the victims to protect themselves, into its holdings. Courts hearing child pornography cases seem strikingly reluctant to comment on these factors, likely to avoid the possibility of being reversed on these grounds.

The special needs argument surrounding the fight against child exploitation and pornography, however, clearly influenced the FBI agents in *United States v. Steiger* and *United States v. Jarrett*. Both agents went out of their way to tell an anonymous vigilante child pornography

34. *Id.* (internal citations omitted).
35. 247 F. Supp. 2d 459 (S.D.N.Y. 2003).
36. *Id.* at 461.
37. *Id.* at 478.

fighter informant that they would not prosecute him for his illegal intrusion into and search of private individuals' computers via the Internet.[38] Furthermore, the courts, likely influenced by the nature of the crimes before it, allowed the evidence so obtained without any negative comment toward the vigilante's or the FBI agents' actions.

This special needs argument was written into the *Wiretap Act* itself, as amended by the ECPA. One of the many exceptions to the prohibitions against ISPs voluntarily disclosing information to the government, including implicitly that obtained by random monitoring, includes disclosures to the National Center for Missing and Exploited Children to uphold the *Victims of Child Abuse Act of 1990*.[39]

b. The War on Terrorism

The government has openly raised the special needs argument surrounding the war on terrorism. The special nature of terrorism was the entire justification for the passage of the *Patriot Act*, shortly after the 9-11 attacks.[40] The most pressing symbol of the need for lessening Fourth Amendment protections in the context of terrorism is the Zaccarias Moussaoui case, involving a person implicated in the attacks. In the words of Alan Dershowitz:

> When Zaccarias Moussaoui was detained after trying to learn how to fly an airplane, without wanting to know much about landing it, the government did not even seek a national-security wiretap because lawyers believed a judge would not have granted one. If Moussaoui's computer could have been searched without a warrant, it almost certainly would have been.[41]

This special needs argument, applicable to terrorism, is also written into the *Wiretap Act* itself, as amended by the ECPA. Another exception to the prohibitions against ISPs voluntarily disclosing information to the government, which implicitly includes information obtained by unlawful random monitoring, is made when a provider, "in good faith[ ] believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating

38. *Steiger*, 318 F.3d at 1039; *Jarrett*, 338 F.3d at 342 (Shortly after Steiger was indicted, the FBI agent informed the vigilante that he would not be prosecuted for his assistance in apprehending Steiger), and at 343 ("We also have no desire to charge you with hacking"). For a full discussion of *Steiger* and *Jarrett*, *see infra*, pt. IV.C.iv.2.

39. 18 U.S.C. § 2702(b)(6).

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

41. Alan Dershowitz, *When All Else Falls, Why Not Torture?*, The Am. Legion Mag. (July 2002) (available at <http://www.legion.org/publications/pubs_2002/pubs_july02print.htm>).

to the emergency."[42]

B. Courts Have Not Established the Boundaries of Fourth Amendment Protections as Applied to E-mails Stored by ISPs

Courts have not yet firmly established the boundaries of Fourth Amendment protections as applied to e-mails stored by ISPs. According to the general Fourth Amendment standards established by the Supreme Court, the government is prohibited from any means of search or seizure of anything that by an individual's conduct reflects "an actual [subjective] expectation of privacy" that "society is [objectively] prepared to recognize as 'reasonable.'"[43] Reasonableness is "measured in objective terms by examining the totality of the circumstances."[44] The Supreme Court, however, has not established what this level of expectation of privacy is for e-mails stored by ISPs.

1. *Maxwell Addresses Society's Expectation of Privacy in E-mails, but Has Little Precedential Value in the Federal Courts*

United States v. Maxwell is the case most directly on point on the determination of society's expectation of privacy in stored e-mails.[45] In *Maxwell*, appellant, an air force colonel, was convicted by general court-martial of using his personal computer to e-mail child pornography.[46] One of the recipients of such an e-mail reported this first to the press, then to AOL representatives, and eventually to the FBI.[47] The FBI applied for and received a warrant to search AOL's computer bank for e-mails and images sent by eighty or more user names.[48] After the FBI seized the information and reviewed its contents, it discovered that an unidentified Air Force member was implicated in the investigated activities, which eventually led to the colonel's conviction.[49] The colonel appealed, arguing in part that the search of AOL's computer bank was based on a warrant that constituted an overly general search and not one based on probable cause directly connecting him to the incriminating e-mails.

The Court of Appeals for the Armed Forces denied the colonel's appeal. The C.A.A.F. noted in dicta that appellant did "possess[ ] a reasonable expectation of privacy, albeit a limited one, in the e-mail messages

42. 18 U.S.C. § 2702(b)(8).
43. *U.S. v. Katz*, 389 U.S. 347, 361 (1967) (internal citations omitted).
44. *U.S. v. Robinette*, 519 U.S. 33, 39 (1996).
45. 45 M.J. 406 (C.A.A.F. 1996).
46. *Id.* at 406.
47. *Id.* at 412.
48. *Id.* at 413.
49. *Id.* at 414.

that he sent and/or received on AOL."[50] It based this in part because, unlike other providers of e-mail services, it was AOL's practice to guard e-mails as "private communications" and only disclose them to third parties under a court order.[51] The court continued to point out, however, that this expectation of privacy in e-mails "incrementally diminishes" as they are sent out to more and more recipients, whether they are sent to the public at large in a "chat room" or via e-mail that is forwarded from correspondent to correspondent.[52] The court held that once the e-mails were turned over to the FBI by the recipient, their use for introduction into evidence and for procuring a search warrant was "fair game."[53] Once, however, the Government wanted to search the computer files further based upon these "chance scraps of information," a warrant was required.[54]

The *Maxwell* case, however, focused on a disclosure of e-mails to the government initiated by a recipient of an incriminating e-mail; not by any random surveillance conducted for the purpose of assisting law enforcement by the ISP, which is the subject matter of this article. Furthermore, even though *Maxwell* is regularly cited positively in federal circuit and district court cases,[55] a Virginia district court in *United States v. Hambrick* noted that *Maxwell* has "little or no precedential value" because it was the holding of a military court reviewing a court-martial; a process that is "entirely separate from" the federal appellate system.[56]

2. *Three Categories of Disclosures of Communications Affecting a Reasonable Expectation of Privacy Determination*

Courts have consistently held that there is no reasonable expectation of privacy for any information disclosed to a third party, whether intentionally or unintentionally. Orin Kerr has dubbed this concept, the "disclosure principle."[57] There are three categories of disclosures of information: intentional disclosures to the public; intentional disclosures to an intended recipient; and unintentional disclosures to third parties who accidentally or intentionally discovered the information, including hackers and thieves.

---

50. *Maxwell*, 45 M.J. at 417.

51. *Id.*

52. *Id.* at 419.

53. *Id.*

54. *Id.*

55. *U.S. v. Charbonneau*, 979 F. Supp. 1177, 1179 (S.D. Ohio 1997); *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001).

56. 55 F. Supp. 2d 504, 508 (W.D.Va. 1999).

57. Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't*, 97 Nw. U.L. Rev. 607, 627 (Winter 2003).

a. Intentional disclosures to the public

According to the Supreme Court, "[W]hat a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection."[58] As applied to the computer context, courts have held on this basis that there is no reasonable expectation of privacy against government searches of Web sites,[59] or Internet chatrooms.[60]

b. Intentional disclosures to an intended recipient

A sender of any communication via a service provider is disclosing information to not only the intended recipient of the communication, but also to the service provider as well in the form of address or "envelope" information. In addition, another unnoticed form of intentional disclosure includes the information provided by customers in order to use or subscribe to a service ("subscriber information"), for example: name, address, phone number, and perhaps credit card information. These all constitute in effect public disclosures, negating any expectation of privacy in the information that the sender might have held.

Furthermore, due to the non-intuitive manner in which e-mails are transmitted over intermediary computers in the World Wide Web, they inherently raise some unique disclosure issues for a reasonable expectation of privacy analysis.

i. Communications directed toward and received by recipient

Courts refuse to recognize any reasonable expectation of privacy in communications that have already been received by a recipient, who in turn discloses these communications to law enforcement officials. In *Gouled v. United States*, the Supreme Court established the principle that there is a reasonable expectation of privacy in a sealed letter, but once the letter is received and opened, the destiny of the letter then lies in the control of the recipient, not the sender.[61] Federal courts have applied this same principle to e-mails.[62] Federal courts, however, have not explicitly ruled on whether the fact that an e-mail has already been received by a recipient breaks *all* expectations of privacy as to the e-mail, including from unsolicited disclosures of their contents by ISPs to the government.

---

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

59. *J.S. v. Bethlehem Area Sch. Dist.*, 757 A.2d 412, 415, 422 (Pa. Cmmw. 2000) (holding student expelled from middle school had no expectation of privacy in his Web site containing threatening and derogatory comments about teacher and principal).

60. *Charbonneau*, 979 F.Supp. at 1184 (holding defendant in a child pornography case had no expectation of privacy in e-mail sent to others in an Internet chatroom).

61. *Gouled v. U.S.*, 255 U.S. 298, 302 (1921).

62. *Leis*, 255 F.3d at 333.

ii. Information directed toward service providers

A different sort of intentional disclosure of information to a recipient occurs when customers disclose "envelope" information and/or subscriber information to their service providers. A sender must provide envelope or address information in order to direct the provider to send the transmission to the appropriate recipient. A service provider customer must also disclose subscriber information, often times including contact information and a credit card, in order to sign up for and/or pay for the service.

a. Limited statutory privacy expectations in "envelope" information

In the postal system, there is no statutory protection for envelope information.[63] Pre-1986, there was no statutory protection for telephone call records either. According to the Supreme Court in *Smith v. Maryland*, a telephone customer had no legitimate expectation of privacy in telephone numbers he had dialed because he had voluntarily conveyed this information to the telephone company.[64] Under the pen register law enacted in 1986, however, Congress created a statutory criminal prohibition on the surveillance of envelope information for the telephone network, subject to some exceptions.[65] The government can conduct surveillance on telephone envelope information upon obtaining a court order, which only requires a showing that "the information likely to be obtained . . . is relevant to an ongoing criminal investigation."[66] The remedy for violations, however, is a criminal misdemeanor prosecution alone; the exclusionary rule does not apply.[67]

Regarding Internet e-mail envelope surveillance, before the *Patriot Act* the U.S. government had already concluded that pen register laws extended here as well.[68] The *Patriot Act*, however, specifically amended the pen register law to leave no doubt that it covered such Internet communications.[69] The *Patriot Act* continues to protect all envelope information, making it a federal crime to collect this information without a court order.[70]

---

63. Kerr, *supra* n. 57 at 631.

64. 442 U.S. 735, 742-44 (1979).

65. Kerr, *supra* n. 57, at 631-32 (citing *Electronic Communications Privacy Act of 1986*, Pub. L. No. 99-508, 301(a), 100 Stat. 1848, 1868).

66. *See* 18 U.S.C.A. § 3123(a).

67. *See id.*

68. Kerr, *supra* n. 57, at 631 (citing U.S. Dept. of Justice, *Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations* at 102 (July 2002) [hereinafter DOJ, *Searching and Seizing Computers*]).

69. *See* 18 U.S.C.A. § 3127(3)-(4).

70. *See* 18 U.S.C.A. § 3121(d).

b. Limited statutory privacy expectations in subscriber information

Courts have also consistently held that individuals have no constitutional expectation of privacy in subscriber information. An important case in this area was *United States v. Miller*, in which the Supreme Court held that a bank depositor had no legitimate expectation of privacy in bank records that the bank used in the ordinary course of its business, because he had voluntarily conveyed this information to the bank.[71]

Congress, however, provided limited statutory protections to subscriber information for customers of telephone companies and ISPs, with the passage of the ECPA in 1986. For the government to compel service providers to disclose basic subscriber account information, they must first obtain an administrative subpoena.[72] Before 9-11, subscriber information originally included only basic information such as the subscriber's name and address. A court order was required to compel the disclosure of more detailed information such as a subscriber's records of session times and durations, length of service, any temporarily assigned network address, and means and source of payment for such service (including any credit card or bank account number). After the passage of the *Patriot Act*, however, all of these became included under subscriber information, and can be compelled with only a subpoena.[73]

In *United States v. Kennedy*, a Kansas district court explicitly held in a child pornography case that the expectation of privacy in subscriber information was extremely limited.[74] An ISP had disclosed appellant's subscriber information pursuant to a court order that turned out to be based on an inadequate government application.[75] The court noted that when the defendant entered into an agreement with the ISP for Internet service, "he knowingly revealed all information connected to the IP address 24.94.200.54. He cannot now claim to have a Fourth Amendment privacy interest in his subscriber information."[76] This logic, however, does not apply to content information, for instance e-mails, for which an

71. 425 U.S. 435, 442 (1976).

72. *See* 18 U.S.C. § 2703(c)(2).

73. 18 U.S.C. § 2703(c)(1)(c).

74. 81 F. Supp. 2d 1103 (D. Kan. 2000). *See also U.S. v. Hambrick*, 55 F. Supp. 2d 504 (W.D. Va. 1999), *Guest v. Leis*, 225 F.3d 325 (6th Cir. 2001) (holding there was no reasonable expectation of privacy in subscriber information to a BBS).

75. *Kennedy*, 81 F. Supp. 2d at 1109-1110.

76. *Id.* at 1110. An Internet Protocol or "IP" address "is the unique address assigned to a particular computer connected to the Internet. All computers connected to the Internet have an IP address." *U.S. v. Steiger*, 318 F.3d 1039 (11th Cir. 2003) (citing Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L.Rev. 1083, 1145 (2002)).

ISP is clearly not the intended recipient.[77]

iii. E-mail transmissions present a unique problem for a reasonable expectation of privacy analysis

Because of the non-intuitive manner by which e-mails "travel", the interception of e-mails during transmission present unique disclosure issues for a reasonable expectation of privacy analysis. These special issues, however, disappear when the e-mails have already been sent and received, and are held in storage on an ISP's system.[78]

During transmission from sender to recipient, e-mails are passed through several intermediate computers connected to the World Wide Web that act as relay stations. In *ACLU v. Reno*, a Pennsylvania district court notes that unencrypted e-mails "can be accessed or viewed on [these] intermediate computers between the sender and recipient."[79] Based on this, a court may argue that there is a diminished expectation of privacy in e-mails.[80]

Unlike any other form of normal communication, e-mails are not relayed from station to station completely intact. The Internet is a "packet switched" network, which means that every communication sent over the Internet is broken down into individual packets.[81] These packets are transmitted individually, perhaps along different routes.[82] Each packet of information contains a combination of "envelope" information" and "content information."[83] All of the individual packets for a particular e-mail are received and reassembled by the recipient computer.[84]

Because of this unique means of transmission, courts could in theory apply existing case law to e-mails in two completely divergent manners. One view would be that a reasonable expectation of privacy does exist for e-mail transmissions as to the relay stations, because any individual relay station only receives fragments of any given e-mail, and the only feasible locations from which a particular message can be intercepted are the sender's and recipient's host computers.[85] Another, view, however, is

77. *Infra,* pt. II(B)(2)(b)(i) (discussing computer technology and the Fourth Amendment).

78. *See infra*, pt. III.B.2.

79. 929 F. Supp. 824, 834 (E.D. Pa. 1996).

80. *See Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 Harv. L. Rev. 1591, 1597 (May 1997) [hereinafter *Keeping Secrets*].

81. Kerr, *supra* n. 57, at 613 (quoting Preston Gralla, *How The Internet Works* (Greg Wiegand et al. eds. 1999)).

82. *Keeping Secrets*, *supra* n. 80, at 1597-98.

83. Kerr, *supra* n. 57, at 614 (quoting Preston Gralla, *How The Internet Works* (Greg Wiegand et al. eds. 1999)).

84. *Id.*

85. *Keeping Secrets*, *supra* n. 80, at 1597-98.

that "because the contents of Internet communications are mixed together with envelope information and disclosed to the ISP, it is at least possible that courts will find that Internet users cannot have a reasonable expectation of privacy in Internet content information, much like postcards or cordless phones."[86]

When we shift our analysis, however, from e-mail interception during transmission to searches of e-mails post-transmission that are stored on the user's account by an ISP, the reasonable expectation of privacy analysis shifts strongly toward a finding of a lack thereof. This will be discussed in depth later in this article.[87]

c. No intent to disclose, but left vulnerable to intentional or accidental discovery by a third party

It is well-settled that private party searches of property, even if wrongfully conducted, do not raise Fourth Amendment protections.[88] Examples of third parties who may intentionally or accidentally discover incriminating evidence and disclose it to law enforcement officials include roommates and/or family members, repairmen and other licensees, service providers, hackers, and thieves. Furthermore, law enforcement officials have license to conduct warrantless searches themselves using certain technologies readily available to the public, under the theory that defendants hold no reasonable expectation of privacy in items they leave vulnerable to discovery by the public.

The protection provided by the Fourth Amendment proscribes only governmental action.[89] A significant exception is made if courts deem the private party to have acted as a government agent.[90] A significant limitation to this exception exists, in that the government is free to replicate a private search already conducted, but can not exceed the scope of the original private search without a warrant.[91]

i. Discovery by roommates and/or family

Evidence obtained through private searches conducted by roommates and/or family members, not acting as government agents, is not protected under the Fourth Amendment. Not only is the evidence turned over by the initial search admissible, but according to *United States v. Smith*, a subsequent police search is sometimes allowed under a theory

86. Kerr, *supra* n. 57, at 629.

87. *Infra*, pt. III.B.2.

88. *U.S. v. Paige*, 136 F.3d 1012, 1017 (5th Cir. 1998).

89. *Id.* at 1017.

90. *Infra*, pt. IV (discussing the determination of whether not a government agency relationship exists).

91. *U.S. v. Jacobsen*, 466 U.S. 109, 115 (1984).

of consent, even if it exceeds the scope of the original private party search.[92] The Illinois district court held in this child pornography case that the housemate had either actual or apparent authority to consent to a search of defendant's computer because the computer was located in an open area, was not password protected, and was occasionally used by the housemate's children to play games, sometimes in defendant's absence.[93]

ii. Discovery by licensees, such as repairmen

Evidence obtained by accidental or intentional discovery by licensees is also admissible. In *United States v. Paige*, appellant was convicted of marijuana possession with intent to distribute, based on the disclosure of evidence found accidentally in appellant's garage by a roof repairman hired by appellant.[94] The Fifth Circuit denied the appeal, holding that the discovery by the repairman did not constitute a protected search, because "private party searches of property, even if wrongfully conducted, do not raise Fourth Amendment implications."[95] The court continued to point out that appellant had no reasonable expectation of privacy as to the garage's contents, as such an accidental discovery by hired repairmen was "reasonably foreseeable."[96]

In *United States v. Barth*, defendant was arrested for possessing child pornography after the police conducted an expansive search of defendant's entire hard drive based on the disclosure of evidence found by defendant's computer repairman.[97] The Texas district court suppressed this evidence.[98] The court noted that there is a reasonable expectation of privacy against a governmental search in the contents of a computer hard drive that is not yielded when one gives it to a computer repairman.[99] Once a repairman searches the hard drive and discloses its contents to the government, a subsequent police search is allowed.[100] This search, however, must be limited to the scope of the private party's original search, which the police failed to do in this case.[101]

92. 27 F. Supp. 2d 1111, 1116 (C.D. Ill. 1998).
93. *Id.* at 1116.
94. *Paige*, 136 F.3d at 1014-15.
95. *Id.* at 1017.
96. *Id.* at 1021.
97. 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998).
98. *Id.* at 936-37.
99. *Id.*
100. *Id.* at 937.
101. *Id.* at 937. *Cf. U.S. v. Runyan*, 275 F.3d 449 (5th Cir. 2001) (admitting evidence of child porn discovered by defendant's ex-wife who had discovered the evidence after breaking into defendant's ranch). The Fifth Circuit in *Runyan* applied this same principle, but interpreted it expansively in the computer context, holding that once a third party examines a single file on a computer, then this allows law enforcement to conduct warrantless searches on the computer's entire contents. *Id.* at 464-65.

iii. Discovery by service providers

As service providers must protect their services against hackers and thieves, service providers have a justification for the random monitoring of their systems that most third party private searchers do not. This is particularly the case for employers and universities acting as service providers, who have both economic and societal interests in preventing misuse of their systems. The question remains, however, whether this justification alone saves evidence obtained during such monitoring against the application of the exclusionary rule when such service providers conduct random monitoring primarily for the alternative purpose of assisting law enforcement.

a. Employers as service providers

There is no reasonable expectation of computer privacy for employees working on their employer's computers or servers, in particular if the employer has posted notice of a computer monitoring policy. The Supreme Court addressed the issue of employee privacy in general in *O'Connor v. Ortega*, holding that employees may have a reasonable expectation of privacy, for the purposes of the Fourth Amendment, in locked, unshared desks or filing cabinets in their offices.[102] As Justice Blackmun noted in his dissent, however, office practices, procedures, or regulations [such as monitoring policies] may reduce such legitimate privacy expectations.[103] Applying this logic, the Fourth Circuit held in *United States v. Simons* that a remote warrantless search of defendant's office computer by his government employer on suspicion of child pornography was admissible because his employer had posted a clear Internet monitoring policy.[104]

b. Universities as service providers

A Maine district court held in *United States v. Butler* that there are no privacy rights in a student's use of a university computer to receive and view child pornography.[105] The court denied the student's motion to suppress the computer logs showing that he had used the university computers, as well as the contents of the computer hard drives.[106] The court held that the public nature of school computers, the student's failure to take any privacy measures, as well as the lack of any computer privacy policies at the university, precluded the student's Fourth

102. 480 U.S. 709 (1987).
103. *Id.* at 717.
104. 206 F.3d 392, 398 (4th Cir. 2000).
105. 151 F. Supp. 2d 82 (D. Me. 2001).
106. *Id.* at 84.

Amendment challenge.[107]

c. Publicly available Internet Service Providers (ISPs)

The courts, however, have not directly addressed whether publicly available ISP subscribers have a legitimate expectation of privacy giving rise to Fourth Amendment protections against ISP random surveillance of their accounts for the purpose of assisting law enforcement. As discussed above, the *Maxwell* court noted in dicta that given AOL's privacy policy, AOL users do possess a limited reasonable expectation of privacy as to e-mails sent or received on AOL.[108] This holding, however, is directed toward government compulsion of the release of stored e-mails, as opposed to an ISP's independent surveillance and disclosure of stored e-mail contents. Furthermore, *Maxwell* was the holding of a military court reviewing a court-martial, and therefore, holds little precedential value for federal courts.[109]

For such an expectation of privacy to be reasonable, the actions of the government and the ISP would have to be deemed by a court to give rise to a government agency relationship. This topic will be fully discussed later in this article.[110]

iv. Admissible due to ease of interception

The interception of certain private transmissions by law enforcement officials may be admissible not due to the fact that it was actually conducted by any third party, but because it easily could have been with the aid of readily available technology. This is in a sense a harsher version of the general rule that anything disclosed to the public is not protected by the Fourth Amendment.

According to the logic applied by several courts, a person does not have a reasonable expectation of privacy in communications transmitted in a form that is easily intercepted. This extends even to cordless phone calls, which several circuit courts have held are not protected under the Fourth Amendment. Although the average lay person probably does not even contemplate the possibility of cordless phone calls being intercepted as opposed to regular phone calls, these courts have held that people know their conversations are traveling via radio waves which are "easily intercepted" and overheard by others.[111] "Of course, Congress can pro-

107. *Id.*

108. *See supra*, pt.II.B.1.

109. *Hambrick*, 55 F. Supp. 2d at 508.

110. *See infra*, pt. IV.

111. *Keeping Secrets*, *supra* n. 80, at 1598 (citing *McKamey v. Roach*, 55 F.3d 1236, 1239 (6th Cir. 1995)); *In re Askin*, 47 F.3d 100, 103 (4th Cir.); *Tyler v. Berodt*, 877 F.2d 705, 706-07 (8th Cir. 1989); *cf. U.S. v. Smith*, 978 F.2d 171, 180 (5th Cir. 1992) (explaining that

tect such calls when the Fourth Amendment does not, and Congress added a statutory protection against cordless phone call interception in 1994."[112]

The courts have not explicitly ruled on whether this logic applies to e-mails stored on ISPs. However, Congress has passed legislation in Title II of the ECPA that provides limited privacy protections of such e-mails.[113]

v. Discovery by hackers and thieves

Applying the general rule that the Fourth Amendment and the exclusionary rule does not apply to even unlawful searches conducted by private parties, evidence discovered by hackers and thieves and disclosed to the government is admissible in court. As described above, recently the Fourth and the Eleventh Circuits found admissible evidence disclosed by the same private vigilante child porn fighter who had obtained the information by hacking into private computers.[114] This already considerable threat to privacy would increase exponentially if a court applies this same logic to searches conducted by ISPs.

III. TITLE III, AS AMENDED BY THE ECPA, IMPLICITLY PROHIBITS RANDOM SURVEILLANCE BY ISPS FOR THE PURPOSE OF ASSISTING LAW ENFORCEMENT, BUT THE REMEDIES FOR VIOLATIONS OF THIS ACT FAIL TO INCLUDE THE EXCLUSIONARY RULE OR CRIMINAL PENALTIES

In the words of Professor Kerr, "[t]o a surprising extent, Internet privacy is statutory privacy, [not Constitutional privacy]."[115] Congress enacted extensive legislation regulating the interception of communications in the *Omnibus Crime Control and Safe Street Act of 1968*, often called "Title III" and/or the *Wiretap Act*.[116] The *Wiretap Act* as it was originally drafted proscribed the interception of oral and wire communications such as telephone calls.[117] Judicial interpretations of the *Wiretap Act* are often strained, as in the words of the Fifth Circuit, the *Wiretap Act* is "famous (if not infamous) for its lack of clarity."[118]

The *Electronic Communications Privacy Act*, passed in 1986, expanded the *Wiretap Act* to add protections for electronic communications

whether an expectation of privacy in a conversation on a cordless phone is reasonable will depend upon the particular characteristics of the phone).

112. Kerr, *supra* n. 57, at 629, n.96.

113. For full discussion, *see infra*, pt. III.B.2.

114. *See supra*, pt. II.A.4.a. For full discussion on these cases, *see infra*, pt. IV.C.iv.2.

115. Kerr, *supra* n. 57, at 627.

116. 18 U.S.C. §§ 2510-2521 (2002).

117. *Steve Jackson Games v. U.S. Secret Serv.*, 36 F.3d 457, 460 (5th Cir. 1994).

118. *Id.* at 462.

such as e-mails. Title I of the ECPA amended the *Wiretap Act* to add the proscription of real-time interception of electronic communications.[119] Title II of the ECPA prohibits the intentional access, without authorization, to stored communications.[120] Unlike with telephone companies under the *Wiretap Act*, however, the ECPA specifically does not apply the exclusionary rule to evidence obtained via ISPs and disclosed to the government in violation of these provisions.

A. The Original *Wiretap Act* Was Directed Only Toward the Real-time Interception of Oral and Wire Communications Such as Telephone Calls

The *Wiretap Act* as originally drafted only prohibited the real-time interception of oral and wire communications such as telephone calls.[121] It implicitly prohibited telephone companies from randomly monitoring their systems for the purpose of assisting law enforcement. The Act provided the exclusionary rule as a remedy for violations of the act, whether carried out by the government or private individuals.[122]

1. *The Original Wiretap Act Only Prohibited the Real-time Interception of Communications, and Did Not Apply to a Government or Private Search of Stored Electronic Communications Such as E-mails*

The *Wiretap Act* as originally drafted only prohibited the real-time interception of communications, and did not apply to a search of electronic communications such as e-mails stored on an ISP account.[123] The ECPA was passed in 1986 in part to address this situation.

2. *The Original Wiretap Act Implicitly Prohibited Only Telephone Companies from Randomly Monitoring Their Systems for the Purpose of Assisting Law Enforcement*

The *Wiretap Act* as originally drafted implicitly prohibited telephone companies from randomly monitoring their systems for the purpose of disclosing any evidence of criminal activity so obtained to the government. Under the "provider exception" to the exclusionary rule in the *Wiretap Act* as originally drafted, an employee of a wire service provider is permitted to "intercept[ ] a communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property

119. 18 U.S.C. §§ 2510-2521 (2002); *Steve Jackson Games*, 36 F.3d at 459.
120. 18 U.S.C. §§ 2701-2711(2002); *Steve Jackson Games*, 36 F.3d at 459.
121. *See infra*, pt. III.A.2.
122. *See infra*, pt. III.A.3.
123. 18 U.S.C. § 2511(1)(a).

of the provider of that service."[124] Therefore, any such evidence obtained by the government is admissible in court.

A limitation to the provider exception exists, however, specifically for wire communication service providers. Wire communication service providers such as telephone companies "shall not utilize service observing or random monitoring."[125] An exception to this exception is made, allowing for interceptions for routine "mechanical or service quality control checks."[126]

This provider exception was applied in *United States v. McLaren*, in which a Florida district court held admissible interceptions of phone calls conducted by a phone company.[127] The court admitted the evidence so obtained because the phone company carried out the surveillance, upon individualized suspicion, to stop a cloning scam.[128]

In *Bubis v. United States*, the Ninth Circuit, interpreted the *Wiretap Act's* predecessor statute, and established boundaries for the provider exception.[129] In *Bubis*, a phone company monitored and recorded all of appellant's phone calls in response to suspicions that he was circumventing the company's record-keeping equipment to avoid long distance charges.[130] The company maintained this surveillance for three months, long after it had collected the necessary evidence.[131] The company finally disclosed to the U.S. Attorney's office that it was clear from these phone calls that appellant had also participated in the separate crime of interstate transmission of wagering information.[132] The Ninth Circuit in *Bubis* reversed the conviction. Although monitoring for the protection of the rights and property of the company is allowed, the court held that the monitoring in this case went well beyond the scope and duration of what was necessary.[133] Furthermore, the court noted in a footnote that "disclosure of what was *said* in appellant's telephone conversations (as distinguished from the fact that the long distance calls were made and not paid for) had no relationship to protecting the telephone company's property."[134]

---

124. 18 U.S.C. § 2511(2)(a)(i).

125. *Id.*

126. *Id.*

127. 957 F. Supp. 215 (M.D. Fla. 1997).

128. *Id.* at 215. A cellular telephone "cloning" operation is a scheme to defraud in which access numbers issued by the service provider to subscribers are stolen and reprogrammed on a nonsubscriber's cellular phone. *See U.S. v. Pervaz*, 118 F.3d 1, 3 (1st Cir. 1997).

129. *Bubis v. U.S.*, 384 F.2d 643 (9th Cir. 1967).

130. *Id.* at 644-45.

131. *Id.* at 645.

132. *Id.* at 645.

133. *Id.* at 648.

134. *Bubis*, 384 F.2d at 648, n. 5 (emphasis added).

Even though *Bubis* is a 1967 case based on an older statute, it is still good law and possibly applicable in the Internet context. In fact, the DOJ cites *Bubis* in recognition that "although providers legitimately may protect their rights or property by gathering evidence of wrongdoing for criminal prosecution, they cannot use the [ ] property exception to gather evidence of crime unrelated to their rights or property."[135] A continued search based on such an accidental discovery can only be conducted by the government upon obtaining a proper search warrant.[136]

3. *The Original Wiretap Act Applied the Exclusionary Rule to Evidence Obtained Without a Warrant Through the Interception of Only Oral and Wire Communications*

Under the *Wiretap Act* as originally drafted, no information obtained through the interception of a wire or oral communication is admissible in court.[137] This exclusionary rule is applied whether the interception is conducted by the government, or by private individuals.[138] The *Wiretap Act* did not make any mention of any equivalent prohibition directed toward the interception of e-mails, as this form of communication did not exist in 1968.

B. THE ECPA AMENDED THE *WIRETAP ACT* TO ALSO ADD LIMITED PRIVACY PROTECTIONS TO ELECTRONIC COMMUNICATIONS SUCH AS E-MAILS

The ECPA amended the *Wiretap Act* in 1986 to protect the privacy of electronic communications such as e-mails. It added e-mails to the list of communications protected from interceptions.[139] The ECPA also added an entirely new section, although one with many exceptions, proscribing the accessing of stored e-mails. Unlike with telephone companies, however, the ECPA did not provide the exclusionary rule as an available remedy for "nonconstitutional" violations of the Act by ISPs.[140] Furthermore, under the *Wiretap Act*, as amended by the ECPA, ISPs have broader rights to conduct random monitoring than do telephone companies.

---

135. DOJ, *Searching and Seizing Computers*, *supra* n. 68, pt. IV.D.3.c.

136. *Id.*

137. 18 U.S.C. § 2515.

138. *See id.*

139. *See infra*, pt. III.B.1.

140. 18 U.S.C. § 2708. If ISPs, however, conduct random monitoring pursuant to a request from the government, this would be a constitutional violation of the Fourth Amendment, and the exclusionary rule would apply. *See infra*, pt. IV.

1. *Title I of the ECPA Prohibits the Interception of E-mails*

Title I of the ECPA amended already existing provisions in the *Wiretap Act* to also prohibit the real-time interception of electronic communications such as e-mails.[141]

In *Steve Jackson Games v. United States Secret Service*, appellant publishers claimed the Secret Service violated the *Wiretap Act*, as amended by Title I of the ECPA, by "intercepting" their stored e-mails sent to an electronic bulletin board, but not yet read by the intended recipients.[142] The Service had obtained a warrant under the false notion that appellant had a sensitive, proprietary computer document that had been wrongfully made available to the public through a computer bulletin board.[143] The Fifth Circuit analyzed the language of 18 U.S.C. §2510(12), and held that Congress "did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'"[144] Therefore, the court held that while the Secret Service did violate Title II of the ECPA regarding accessing of stored communications,[145] it did not violate Title I of the ECPA regarding real-time interceptions of such communications.[146]

2. *Title II of the ECPA Proscribes the Accessing of Stored E-mails*

Title II of the ECPA added an entirely new section to the *Wiretap Act*, and proscribes the accessing of stored communications such as e-mails.[147] This new section governs both the voluntary disclosure of customer communications or records,[148] and the compelled disclosure of the same by the government.[149]

In drafting the ECPA, Congress made the level of court permission required for a governmental compulsion of a subscriber's account information from ISPs commensurate with the level of intrusiveness of the search. Only a subpoena is required to compel disclosure of subscriber information.[150] For governmental compulsion of content information, such as in stored e-mails, a warrant is required.

---

141. 18 U.S.C. § 2511(1)(a).
142. 36 F.3d at 460.
143. *Steve Jackson Games, Inc v. U.S. Secret Serv.*, 816 F.Supp. 432 (W.D. Tex. 1993).
144. *Steve Jackson Games*, 36 F.3d at 461-462.
145. For discussion of Title II of the ECPA, *see infra*, pt. III.B.2.
146. *Steve Jackson Games*, 36 F.3d at 461-62.
147. 18 U.S.C. §§ 2701-2712.
148. 18 U.S.C. § 2702.
149. 18 U.S.C. § 2703.
150. *Id.*

a. For governmental compulsion of stored e-mails on ISPs, a warrant is required

The government can compel disclosure by an ISP of an e-mail in storage in the system for 180 days or less, only pursuant to a warrant.[151] For e-mails in storage for more than 180 days, a court order or a subpoena is enough, depending upon different circumstances including whether or not notice is provided to the subscriber.[152]

Some courts have overturned convictions based on compelled information obtained through defective warrants, whereas others have affirmed them. As stated above, in *Steve Jackson Games*, involving the Secret Service accessing of stored e-mails sent to an electronic bulletin board, but not yet read by the recipients, the Fifth Circuit held that the Secret Service violated Title II of the ECPA, as they in fact accessed "stored electronic communications," based on an improper warrant.[153] The court assigned civil liability to the Secret Service in excess of $50,000 in actual damages, plus over $250,000 in attorneys' fees and costs, for its seizure of the appellant publisher's computers, disks, and other materials.[154]

In *United States v. Perez*, another case in which the court overturned a verdict due to a faulty warrant, DOJ agents searched and seized images of child pornography on several home computers, including the defendant's, as a part of Operation "Candyman."[155] The agents' probable cause was based not on any evidence that the suspects had uploaded, downloaded, or discussed the images, but rather solely because they had joined the Egroup of the "Candyman" Web site.[156] The agents obtained the warrants to search defendants' home computers based on faulty affidavits stating that users automatically received e-mailed child porn when they joined the Egroup, despite clear evidence that "Candyman" members had three e-mail delivery options, one of which included "no e-mail receipt at all."[157] A New York district court applied the Supreme Court's *Franks* test,[158] and granted the appellant's motion to suppress

151. 18 U.S.C. § 2703(a).

152. *See* 18 U.S.C. § 2703(a)-(b).

153. *Steve Jackson Games*, 36 F.3d at 461-62.

154. *Id.* at 459.

155. 247 F. Supp. 2d at 462.

156. *Id.* at 461.

157. *Id.* at 463.

158. *Id.* at 472 (citing *Franks v. Del.*, 438 U.S. 154 (1978)). The Supreme Court held in *Franks v. Del.* that if a defendant shows, by a preponderance of the evidence, that a law enforcement agent obtained a search warrant based on an affidavit containing deliberately or recklessly false or misleading material, and that without this false material, the court would not have issued the search warrant, the warrant must be voided and the evidence so-obtained must be suppressed.

the evidence so obtained, due to the DOJ's reckless disregard for the falsity of its warrant application.[159]

Cases that appear to favor overlooking minor warrant defects include *United States v. Bach*.[160] In *Bach*, the government appealed the lower court's suppression of evidence based on a search warrant that was executed only by the ISP's personnel, without the presence of a law enforcement official as required by law.[161] The Eighth Circuit reversed, holding that the resultant e-mails containing child pornography should have been admitted, because the statute requiring the presence of law enforcement officials when executing search warrants only applies to federal officials, not state.[162]

In a recent case, *State v. Evers*, the New Jersey Supreme Court held that the state of California's compulsion of a subscriber's information from an ISP using a warrant that may not have been enforceable in the ISP's state of Virginia was insufficient to overturn a verdict.[163] Shockingly, the court noted in dicta that even if the warrant was defective, the ISP chose to hand over the information voluntarily, and therefore the e-mails were admissible.[164] This logic, if applied universally, would seemingly encourage law enforcement officials and even courts to serve warrants known to be faulty on ISPs no matter what, as the mere failure of the ISPs to object to them might be sufficient to cure any defects. The court, however, may tacitly have been taking into account the fact that, as described previously, a warrant is not necessary to compel disclosure of subscriber information to begin with; all that's required is a subpoena.[165]

b. Requirements for an ISP's voluntary disclosure of customer communications

Under Title II of the ECPA, an ISP "shall not knowingly divulge to any person or entity [including the government] the contents of a communication" that is "in electronic storage by" or "carried or maintained on" that service.[166] There, however, is a long list of exceptions to this rule.

159. *Id.* at 478-79.

160. 310 F.3d 1063 (8th Cir. 2002).

161. *Id.* at 1066.

162. *Id.* at 1067.

163. 175 N.J. 355 (2003).

164. *Id.* at 379.

165. *See supra*, pt. III.B.2.

166. 18 U.S.C. § 2702(a)(1)-(2).

i. ISP voluntary disclosure of content information such as e-mails

The most notable exceptions are that ISPs can disclose the contents of a subscriber's e-mails "as may be necessary incident to the rendition of the service or to the protection of the rights of the provider of that service;"[167] to the National Center for Missing and Exploited Children when appropriate;[168] to law enforcement if the contents were inadvertently obtained by the ISP and they "appear to pertain to the commission of a crime;"[169] and most broadly, to any government entity if the provider, "in good faith" believes there's an emergency involving danger of death or serious bodily injury that requires disclosure without delay.[170] There is no case law to date providing guidance on these provisions.

The exceptions for cases of child exploitation and emergencies involving danger or death are applications of the "special needs" argument discussed previously for the lessening of Fourth Amendment protections in cases of child abuse and terrorism.[171]

ii. ISP voluntary disclosure of customer records

The requirements for ISPs to be able to voluntarily disclose customer records such as subscriber information are much lower. The "necessary incident to the rendition of the service" exception applies as above,[172] as does the child abuse exception. The "emergency exception," however, only requires the provider to "reasonably believe" in the danger.[173] Notably, unlike with content information which ISPs can only disclose to a government entity if at all, under Title II of the ECPA, ISPs can divulge subscriber information at any time to "any person other than a governmental entity."[174] A Virginia district court upheld this principle in *United States v. Hambrick*, noting that "the ECPA's concern for privacy extends only to government invasions of privacy. ISPs are free to turn stored data and transactional records over to nongovernmental entities."[175]

167. *Id.* at § 2702(b)(5).

168. *Id.* at § 2702(b)(6).

169. *Id.* at § 2702(b)(7)(ii).

170. *Id.* at § 2702(b)(8).

171. *Supra*, pt. II.A.4.

172. 18 U.S.C. § 2702(c)(3), (5).

173. *Id.* at § 2702(c)(4).

174. *Id.*

175. 55 F. Supp. 2d 504 (W.D. Va. 1999).

3. *Under the Amended Wiretap Act, However, ISPs Still Have Broader Rights to Conduct Random Monitoring Than Telephone Companies*

Under the *Wiretap Act*, as amended by the ECPA, ISPs have broader rights to randomly monitor its systems than do telephone companies. ISPs have the same right to randomly monitor all e-mails sent or received on its systems for purposes including combating user fraud and scanning for viruses. ISPs, however, are unbound by the additional restrictions on random monitoring imposed by Congress on telephone companies.[176] Given the incomparable scope of ISP surveillance relative to that possible by telephone companies, it is unclear why Congress should choose to make prohibitions of random monitoring stronger for telephone companies than for ISPs.

4. *The ECPA Fails to Apply the Exclusionary Rule or Criminal Penalties for Violations of This Act*

The *Wiretap Act*, as amended by the ECPA, only applies the exclusionary rule to the interception of oral or wire communications, and does not apply it to the real-time interception of e-mails, or the accessing of stored e-mails. Furthermore, ISPs who unlawfully access stored e-mails are exempt from criminal prosecution.[177]

If an ISP intercepts e-mail communications for the purpose of assisting law enforcement, the exclusionary rule is not available as a remedy.[178] According to 18 U.S.C. section 2515, "[w]henever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived there from may be received in evidence in any trial, hearing, or other proceeding in or before any court. . . ." There is no mention of this rule applying to the illegal interceptions of electronic communications as well. The only available remedy for this type of violation is civil litigation under 18 U.S.C. section 2520.[179] This distinction, however, is not important in practice, as there is no reason for the government to conduct real-time interceptions of e-mail communications. Unlike with oral and wire communications, such real-time interception of e-mail communications is already effectively and automatically carried out by the storage procedures inherent in running

176. *See supra*, pt. III.A.2.

177. *See* 18 U.S.C. § 2701.

178. *Steiger*, 318 F.3d at 1050 (holding that under Title III, suppression is not an available remedy to private tapping of electronic communications).

179. 18 U.S.C. § 2520 states that in general, "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of [Title III] may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

an ISP. All the government would need to do to gain access to any e-mail communication is compel disclosure of such stored communications under Title II of the ECPA (18 U.S.C. sections 2701-12).

Significantly, however, the exclusionary rule is not an available remedy for the illegal accessing of stored e-mails either. The *Wiretap Act* includes a provision (18 U.S.C. section 2515) entitled "Prohibition of use as evidence of intercepted wire or oral communications." Title II of the ECPA[180] governing stored wire and electronic communications, contains no equivalent provision.[181] Title II of the ECPA makes civil actions the exclusive remedy for illegal access to stored e-mails.[182]

If, however, a court deems the ISP to have been acting as a government agent in conducting its surveillance, its actions may constitute a Fourth Amendment violation leading to the exclusion of the evidence obtained. This will be discussed in full later in this article.[183]

According to *United States v. Hambrick*, "the ECPA is hardly a legislative determination that [society's expectation of privacy for e-mails] is one that rises to the level of 'reasonably objective' for Fourth Amendment purposes."[184] In *Hambrick*, a defendant in a child pornography case moved to suppress evidence that had been obtained from his ISP.[185] A

180. 18 U.S.C. §§ 2701-2712.

181. *See generally* 18 U.S.C. §§ 2707-2708.

182. *See generally* 18 U.S.C. §§ 2707-2708. The rationale behind applying the exclusionary rule to unlawful interceptions of oral and telephone communications but not of e-mail communications is not discussed in Title II of the ECPA, the legislative history (which only states that this legislative distinction was the result of "discussions with the Justice Department." S.Rep. No. 99-541, 99th Cong, 2d Sess. 23 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577), or the relevant caselaw (*See Steve Jackson Games*, 36 F.3d at 461 n.6). There are, however, at least two justifications for this distinction:

> 1.) There is an inherent reduced level of expectation of privacy in e-mail communications as it is common knowledge that e-mails are stored and retrievable, unlike oral or telephone communications. For a full discussion of counterarguments to this position, *see supra* pt. II.A.;
>
> 2.) Unlike surveillance of stored communications, real-time surveillance "tends to raise difficult questions of how the communications should be filtered down to the evidence the government seeks."

Kerr, *supra* n. 57 at 616. Minimization requirements and the exclusionary rule are applied to protect privacy interests in communications completely irrelevant to an investigation. In contrast, surveillance of stored communications can be contained through filtering techniques such as keyword searches. Therefore the protection of the exclusionary rule is less necessary. The availability of filtering techniques, however, does not necessarily mean that they are adequately or conscientiously applied in all cases without judicial oversight. Furthermore, while minimization requirements may justify the privacy intrusions of surveillance when law enforcement officials already have probable cause against an individual, they do not justify the privacy intrusion inherent in random surveillance without any cause whatsoever.

183. *See infra*, pt. IV.

184. 55 F. Supp. 2d at 507.

185. *Id.* at 505.

Virginia district court denied this motion, holding that according to the ECPA, "[w]hen an ISP discloses stored communications or transactional records to a government entity without the requisite authority, the aggrieved customer's sole remedy is damages."[186] Similarly in *United States v. Bach*, the Eighth Circuit noted in dicta that although Congress "intended to create a statutory expectation of privacy in e-mail files, it is less clear that an analogous expectation of privacy derives from the Constitution."[187]

The *Hambrick* court continues to note in dicta that even absent the availability of the exclusionary rule or criminal penalties for violations of Title II of the ECPA, the court's decision "does not leave members of cybersociety without privacy protection."[188] The fact that ISPs are civilly liable, under the ECPA,[189] when they voluntarily access and disclose subscriber e-mail contents to the government is "a powerful deterrent protecting privacy in the online world and should not be taken lightly."[190] Whether this argument should carry the day or not will depend in large part on whether any case is ever heard in which a court actually imposes a heavy fine on an ISP for such misconduct. This seems unlikely, however, because the very areas in which ISPs or their employees may conduct surveillance are the very areas in which the ISPs are exempted from civil liability. The amended *Wiretap Act* itself, effectively provides free license to ISPs for their searches, however, illegal, should the information they disclose to the government be related to child exploitation, or to an emergency situation with the risk of death or serious injury.[191]

IV. RECENT COURT DECISIONS SUGGEST THAT THE FOURTH AMENDMENT DOES NOT PROTECT AGAINST EVIDENCE OBTAINED FROM ISP RANDOM SURVEILLANCE FOR THE PURPOSE OF ASSISTING LAW ENFORCEMENT

As the *Wiretap Act*, as amended by the ECPA, does not provide adequate protections for the public against random ISP monitoring for the purposes of assisting law enforcement, the only other possible source of protection is the Fourth Amendment. If courts were to deem that such monitoring rises to the level of a government agency relationship, any

186. *Id.* at 507.

187. *Bach*, 310 F.3d at 1066; *But see McCelland v. McGrath* in which an Illinois district court noted in dicta that "the Fourth Amendment binds government actors and their agents, who to avoid violating it must comply with the judicial authorization provisions of Title III." 31 F. Supp. 2d 616, 614 n. 3 (N.D. Ill. 1998).

188. *Hambrick*, 55 F. Supp. 2d at 509.

189. *See* 18 U.S.C. §§ 2703(e), 2707(a), 2708.

190. *Hambrick*, 55 F. Supp. 2d at 509.

191. *See* 18 U.S.C. § 2702(b)(6), (8). For full discussion, *see infra*, pt. IV.C.4.i.

evidence so obtained would be excluded under the Fourth Amendment. Recent case law, however, strongly suggests that courts would refuse to extend Fourth Amendment protections here.

Even the DOJ acknowledges that the Supreme Court has "offered little guidance on when private conduct can be attributed to the government."[192] The Fourth Amendment protects against unreasonable searches and seizures by government officials and those private individuals acting as "instrument[s] or agent[s]" of the government.[193] It does not, however, provide protection against searches by private individuals acting in a private capacity.[194] Determining whether the requisite agency relationship exists "necessarily turns on the degree of the government's participation in the private party's activities, . . . a question that can only be resolved in 'light of all the circumstances.'"[195] Mere governmental authorization of a private search, in the absence of more active participation or encouragement, is not enough to make the private actor an agent of the government.[196]

A. *Barth* Provides a Framework for a Government Agency Analysis in the Computer Context

Basic boundaries defining whether or not a government agency relationship exists in the computer context are clearly illustrated in *United States v. Barth*.[197] In *Barth*, the defendant brought his computer to a computer technician for repairs.[198] The repairman found child pornography on this computer, and disclosed it to the FBI.[199] The FBI then told the repairman to copy all the files on the hard drive onto disks for FBI examination.[200] The repairman continued searching the computer and

192. DOJ, *Searching and Seizing Computers*, *supra* n. 68, pt. I.4.

193. *Coolidge v. N.H.*, 403 U.S. 443, 487 (1971).

194. *Jacobsen*, 466 U.S. at 113 (holding that the Fourth Amendment is "wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official"). *Walter v. U.S.*, 477 U.S. 649, 662 (1980). *See also U.S. v. Lambert*, 771 F.2d 83, 89 (6th Cir. 1985) The court allowed evidence obtained by an FBI informant who took drug paraphernalia from defendant's house and delivered it to the FBI because the record failed to show the FBI instigated, encouraged, or participated in the search, and noted that the Fourth Amendment "proscribes only governmental action and does not apply to a search or seizure, even an unreasonable one, conducted by a private individual not acting as an agent of the government or with the participation or knowledge of any governmental official." *Jacobsen*, 466 U.S. at 109.

195. *Skinner v. Ry. Labor Exec. Assn.*, 489 U.S. 602, 614-15 (1989).

196. *U.S. v. Miller*, 688 F.2d 652, 657 (9th Cir. 1982); *U.S. v. Walther*, 652 F.2d 788, 791 (9th Cir. 1981).

197. 26 F. Supp. 2d at 929.

198. *Id.* at 932.

199. *Id.*

200. *Id.*

discovered more images of child pornography.[201] Only then did law enforcement get a warrant to search the hard drive.[202]

A Texas district court held in *Barth* that the repairman's initial search and disclosure to law enforcement was admissible, as it was a private search.[203] The court held, however, that the second search was not done for "opening private files in an effort to repair the machine," but rather "for the purpose of assisting law enforcement officials."[204] Since he did this at the bequest of the FBI, he was acting then as an agent of the government, and the evidence developed from this warrantless search was held inadmissible.[205]

B. There Is a Circuit Split in Developing Guidelines for Determining Whether a Private Actor Is Acting As a Government Agent

There is a circuit split in developing guidelines for determining whether a private actor who obtains and discloses evidence to the government is acting as a government agent. About half of the circuits apply a "totality of the circumstances" three-factor approach. The other half applies more rule-like formulations, focusing on only two of these factors.

The totality of the circumstances approach for determining the existence of government agency takes into account three factors: 1) whether the government knows of or acquiesces in the intrusive conduct; 2) whether the party performing the search intends to assist law enforcement efforts at the time of the search; and 3) whether the government affirmatively encourages, initiates or instigates the private action. This approach has been adopted by the First,[206] Seventh,[207] Eighth,[208] and Tenth Circuits.[209]

For establishing government agency, other circuits have adopted more rule-like formulations that focus on only two of the factors listed above. The Ninth Circuit applies a two factor test: "1) whether the gov-

201. *Id.* at 932-933.

202. *Id.* at 933.

203. *Barth*, 26 F. Supp. at 935.

204. *Id.* at 936.

205. *Id.*

206. *Pervaz*, 118 F.3d at 5-6.

207. *U.S. v. McAllister*, 18 F.3d 1412, 1418 (7th Cir. 1994) (affirming conviction for manufacture of marijuana, because defendant had failed to show that a confidential informant was acting as a government agent).

208. *U.S. v. Malbrough*, 922 F.2d 458, 462 (8th Cir. 1990) (denying appeal of defendant's conviction for manufacturing marijuana because the informant who had discovered the marijuana while trespassing on defendant's property was not acting as an agent of the state).

209. *U.S. v. Smythe*, 84 F.3d 1240, 1242-1243 (10th Cir. 1996).

ernment knew of and acquiesced in the intrusive conduct; and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends."[210] The Sixth Circuit applies a more restrictive two factor test: "1) the police must have investigated, encouraged, or participated in the search; 2) the individual must have engaged in the search with the intent of assisting the police in their investigative efforts."[211] The Fourth and Fifth Circuits also apply a two factor test.[212]

C. Circumstances Where the Courts Have Refused to Extend Fourth Amendment Protections Against Evidence Obtained from Private Searches.

There is a "gray area" between the extremes of overt governmental participation in a private search and the complete absence of such participation.[213] Cases falling within this "gray area" are best resolved on a case-by-case basis.[214]

There are two situations in which it is well settled that a private actor conducting a search is deemed to be not acting as a government agent: if the government merely knows of or acquiesces in a lawful private search; and if a service provider independently conducts random monitoring for the purpose of protecting its services from hackers and/or theft.[215]

What if, however, the government indirectly solicits private parties with incentives such as general cash rewards or tax cuts to conduct random surveillance for the purpose of assisting law enforcement? Or what if the government assures such private actors that they will not be prosecuted for their otherwise unlawful searches? The courts that have heard cases touching on these areas have all refused to apply Fourth Amendment protections, but the Supreme Court has still not weighed in on these issues.

1. *If the Government Merely Knows of or Acquiesces in a Lawful Private Search, the Private Actor Is Not Acting As a Government Agent*

If the government merely authorizes a lawful private search, without providing any greater form of encouragement, courts have consistently held that the private actor is not acting as a government agent.

---

210. *Miller*, 688 F.2d at 657.
211. *U.S. v. Lambert*, 771 F.2d 83, 89 (6th Cir. 1985).
212. *Jarrett*, 338 F.3d at 345; *U.S. v. Paige*, 136 F.3d 1012 (5th Cir. 1998).
213. *Walther*, 652 F.2d at 791.
214. *See id.*
215. *See infra*, pt. III.C.1. & III.C.2.

In *United States v. Miller*, a theft victim asked the FBI if he himself could go to the future defendant's place of business during business hours to search for goods previously stolen from him.[216] The FBI agent said, he "didn't see anything wrong with that at all."[217] The court held that this conversation did not render the victim an agent of the government. Because the victim hadn't proposed to do anything illegal, the court saw "no reason why the officers should have restrained him or discouraged him from visiting [the] property."[218] *Miller*, however, does not address situations where the FBI acquiesces in unlawful private searches.

2. *If a Service Provider Discloses Evidence Obtained as a By-product of Its Random Monitoring for the Purpose of Protecting Its Services From Hackers and/or Theft, the Provider Is Not Acting As a Government Agent*

According to the provider exception to the *Wiretap Act*,[219] if a service provider independently gathers information on a subscriber while monitoring the security of its system, any such information that it accidentally comes across and then discloses to the government is admissible. The service provider is not considered an agent of the government under these circumstances, and there is no warrant requirement imposed. Any information, however, gathered by law enforcement officials after the service provider's disclosure that is outside the scope of the original private search is not admissible unless obtained with a warrant.[220]

In *United States v. Pervaz*, the Secret Service warned a cellular company that a disproportionately large number of international calls were being made from a particular cell phone.[221] The phone company investigated, leading to defendants' conviction for taking part in a telephone "cloning" operation.[222] The court noted that there was no evidence that the government agent had authorized the search or knew about it.[223] It upheld the conviction because the phone company had "a legitimate independent [and statutorily sanctioned] motivation for its search: to prevent fraud from being perpetrated on its customers."[224]

The Tenth Circuit in *United States v. Smythe* also affirmed the denial of defendant's motion to suppress, in part because the recipient-in-

216. 688 F.2d at 657.
217. *Id.* at 655.
218. *Id.* at 657.
219. *See supra*, pt. III.A.2.
220. *Barth*, 26 F. Supp. 2d at 939.
221. 118 F.3d at 2-3.
222. *Id.*
223. *Id.* at 6.
224. *Id.*

formant also had a "legitimate, independent motivation" to search the package in question.[225] In *Smythe*, a recipient of a package containing narcotics was suspicious of its contents and contacted the local police.[226] A police officer said that he himself could not open the package, and directed the receiver to open it instead.[227] The Tenth Circuit noted that while government agents "may not circumvent the Fourth Amendment by acting through private citizens, they need not discourage private citizens from doing that which is not unlawful."[228]

In contrast, in *McClelland v. McGrath*, in what a district court of Illinois described as the "very definition of chutzpah," the plaintiff sued the City of Chicago for asking a phone company to assist in a kidnapping investigation and intercept a call he made on a cloned cellular phone.[229] Unlike in *Pervaz* and *Smythe*, the *McClelland* court awarded summary judgment for the plaintiff and excluded the evidence. The *McClelland* court held that while phone companies are allowed to conduct such monitoring to protect themselves against cell phone cloning, the company's impetus in this case for carrying out its surveillance was not for this purpose but rather to help law enforcement in its kidnapping investigation.[230] In the eyes of the court, the phone company was clearly "motivated by its desire to help the officers rather than to protect its own property."[231] As the phone company did this as a result of a direct solicitation by the police, the court held that the phone company was acting as a government agent.[232]

McClelland, however, does not apply to circumstances where the service provider, on its own accord, initiates surveillance of its system for the purpose of assisting law enforcement, which is the subject of this article.

3. *If the Government Indirectly Solicits Private Parties With Incentives to Conduct Random Surveillance for the Purpose of Assisting Law Enforcement, Does This Give Rise to a Government Agency Relationship?*

The courts have not explicitly ruled on whether Fourth Amendment protections apply when private parties such as ISPs conduct random surveillance for the purpose of assisting law enforcement after the government has offered incentives such as a general cash reward or tax cuts.

225. 84 F.3d at 1243.
226. *Id.* at 1242.
227. *Id.*
228. *Id.* at 1243.
229. 31 F. Supp. 2d at 616.
230. *Id.* at 619.
231. *Id.*
232. *Id.*

Does the government's recent practice post 9-11 of offering rewards for private individuals' vigilance and disclosure of any suspicious activity possibly related to terrorism by itself give rise to an agency relationship under the Fourth Amendment? Only one circuit court has ruled on this general issue, but in a non-ISP and non-terrorism context.

The Ninth Circuit has held that this did in fact constitute a government agency relationship in a common carrier context in which the private actor had been awarded a cash reward by the government agency for similar disclosures in the past. In *United States v. Walther*, an airline employee searched a package in which cocaine was found and disclosed it to the Drug Enforcement Administration (DEA).[233] This same employee had acted as a confidential informant for the DEA in the past, providing information to the DEA on at least eleven occasions for which he received a total of $800.00 in rewards.[234] The court affirmed the suppression of this evidence, holding that the government "cannot knowingly acquiesce in and encourage directly or indirectly a private citizen to engage in activity which it is prohibited from pursuing where that citizen has no motivation other than the expectation of reward for his or her efforts."[235] The employee had specifically testified that the only reason he opened the case was his suspicion that it contained illegal drugs, leading the court to conclude that legitimate business considerations were not a factor.[236] The court held that the employee had the requisite mental state of an agent as he had opened the case "with the expectation of probable reward from the DEA."[237] The court also held that the employee's prior experience with the DEA provided "proof of the government's acquiescence in the search."[238] The court noted that even though the DEA had "no prior knowledge that this particular search would be conducted. . . it had certainly encouraged [the employee] to engage in this type of search."[239]

In *United States v. Snowadzski*, however, the Ninth Circuit limited its previous ruling in *Walther*.[240] In *Snowadzski*, an employee turned in a fellow employee for tax evasion. The court held that even though this informant "may have acted in part from a desire for a reward, there [was] no evidence that the seizure was motivated by IRS prompting or encouragement."[241] Apparently the mere existence of a government

233. 652 F.2d at 790.
234. *Id.*
235. *Id.* at 793.
236. *Id* .at 792.
237. *Id.*
238. *Id.* at 793.
239. *Id.*
240. 723 F.2d 1427 (9th Cir. 1984).
241. *Id.* at 1430.

award combined with a private actor's assistance of law enforcement in order to obtain it, is insufficient to establish a government agency relationship in the eyes of the Ninth Circuit.

Walther and *Snowadzski* have neither been strongly followed nor rejected by other circuits, which have not heard cases on this issue. The lack of judicial discussion on this topic, however, suggests that most courts are not as receptive to this concept as is the Ninth Circuit. Even if followed, however, it is unclear how directly applicable these cases involving cash rewards directed at individuals would be to cases involving service providers. How much and in what form the incentives would need to be in order for an ISP to be deemed an agent of the government has yet to be determined.

4. *If the Government Assures Private Actors That They Will Not Be Prosecuted for Unlawful Searches Conducted to Assist Law Enforcement, Does This Give Rise to a Government Agency Relationship?*

What if the government assures that private actors will be held immune from criminal or civil liability for unlawful searches independently conducted to help law enforcement? Does this constitute enough governmental encouragement to give rise to a government agency relationship? The government can provide free license to conduct such surveillance through legislation, and also through the direct assurances of law enforcement officials. The few courts that have touched upon these areas have refused to apply Fourth Amendment protections here as well.

a. Legislative carte blanche

The government may provide free license to conduct private surveillance through legislation. For example, according to Title II of the ECPA, ISPs may voluntarily disclose customer communications to a governmental entity if, amongst other reasons, the provider, "in good faith, believe[s] that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[242] ISPs may also disclose information related to child exploitation.[243] ISPs may voluntarily disclose customer communications for the same circumstances, but only need to have a "reasonable belie[f]" in the danger.[244] Implicit in these provisions is that such voluntary disclosure may not be prosecuted, no matter how the ISP went about obtaining the information. No court has ruled on whether or

242. 18 U.S.C. § 2702(b)(8).
243. 18 U.S.C. § 2702(b)(6).
244. 18 U.S.C. § 2702(c)(4).

not this provision of the ECPA gives rise to a government agency relationship.

One district court, however, has held in a recent case that no such government agency relationship should be inferred from an anti-child pornography statute requiring mandatory disclosure by private parties. In *United States v. Peterson*, a defendant objected on Fourth Amendment grounds to the admission of evidence of child pornography obtained from his computer by his computer repairman.[245] The state statute absolutely requires such a disclosure when any film developer or computer technician views child pornography in their customers' possession.[246] The statute also states that "compliance does not give rise to any civil liability on the part of anyone making this report."[247] Nevertheless, the South Carolina district court held that people complying with this statute are not acting as government agents, because the statute does not "instruct [them] to [pro-actively] search or investigate" for such child pornography.[248] It merely requires them to report it if they "discover" such contraband.[249] Whether and how far other courts will follow this rather fine distinction remains to be seen.

b. Carte blanche offered directly by law enforcement officials

The government can also condone unlawful private searches by law enforcement officials providing assurances to private actors that they will not be prosecuted for their actions. Even this more specific offer of amnesty than the legislative carte blanche discussed above was insufficient to give rise to a government agency relationship in the eyes of two circuit courts, in cases brought about by the same vigilante child-porn fighter.

In *United States v. Steiger*, appellant moved to suppress evidence obtained and disclosed by a private vigilante who had obtained the evidence by hacking into appellant's home computer.[250] The vigilante had first left an image of child pornography on the World Wide Web as bait, and secretly attached a Trojan horse program to would-be viewers such as the appellant.[251] The individual then anonymously disclosed the evidence found in this manner to an FBI agent. After Steiger's conviction, the FBI agent thanked the vigilante, tried to arrange a meeting several times, and informed him that he would not be prosecuted for his unlaw-

245. 2003 WL 22883120, at *1 (D.S.C. 2003).
246. *Id.* at *6.
247. *Id.*
248. *Id.*
249. *Id.*
250. 318 F.3d at 1039.
251. *Id.* at 1044.

ful hacking activities.[252] Nevertheless, the Eleventh Circuit held that this was purely a private search, as the informant had disclosed the information obtained *before* making *any* contact with the FBI.[253]

In *United States v. Jarrett*, the same individual applied the same Trojan horse method to trap another appellant, this time disclosing the information obtained to a different FBI agent.[254] After the appellant in *Jarrett* was arrested based on the information disclosed, the *Jarrett* FBI agent exchanged e-mails with the vigilante, and engaged in what the Fourth Circuit referred to as the "proverbial 'wink and a nod:'"[255]

> I can not ask you to search out cases such as the ones you have sent to 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 to 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 e-mail you with the questions. But as long as you are not 'hacking' at our request, we can take the pictures and identify the men and take them to court.[256]

Following the lead of the *Steiger* FBI agent, the *Jarrett* FBI agent also gave assurances that "[w]e also have no desire to charge you with hacking."[257] The agent continued: "You are not a U.S. citizen and are not bound by our laws."[258] Nevertheless, the Fourth Circuit in *Jarrett*, much like the *Steiger* court, reversed the district court, holding that the vigilante was not acting as a government agent because this e-mail was sent *after* the vigilante had already hacked into appellant's computer and disclosed the pornographic images to the FBI.[259] Significantly, however, the *Jarrett* court noted in dicta that had this e-mail exchange taken place *before* the vigilante had hacked into appellant's computer and disclosed the evidence to the FBI, the evidence would have been excluded, as the e-mail "probably does constitute the sort of active Government participation sufficient to create an agency relationship going forward."[260]

It is unclear, however, why the *Jarrett* court did not deem the communications sent from the *Steiger* FBI agent to the vigilante in the time between *Steiger* and *Jarrett* to be already sufficient to give rise to a gov-

252. *Jarrett*, 338 F.3d at 341.
253. *Steiger*, 318 F.3d at 1045.
254. 338 F.3d at 340.
255. *Id.* at 343.
256. *Id.*
257. *Id.*
258. *Id.* The vigilante had previously disclosed to the FBI Agents that he resided in Turkey.
259. *Id.* at 346.
260. *Id.*

ernment agency relationship in the informant's subsequent actions leading to *Jarrett*. This is clearly the same type of situation as in *Walther*, in that even though the FBI in *Jarrett* had no prior knowledge that this particular search would be conducted . . . it had "certainly encouraged [the vigilante] to engage in this type of search."[261] Furthermore, the individual also had the requisite intent to hack into private computers in order to assist the government.

The *Jarrett* court should have found that the informant was acting as a government agent for purposes of the Fourth Amendment, and the evidence so obtained should have been excluded. If other circuits follow the Fourth Circuit's flawed analysis, then the Fourth Amendment offers little to no protection against random monitoring by private individuals, or even more troubling by ISPs, of e-mails for the purpose of aiding law enforcement officials.

V. CONCLUSION: TO PROTECT THE PUBLIC AGAINST RANDOM ISP MONITORING FOR THE PURPOSE OF ASSISTING LAW ENFORCEMENT, CONGRESS MUST FURTHER AMEND THE *WIRETAP ACT*

The *Wiretap Act*, as amended by the ECPA, fails to protect the public against ISP random monitoring of e-mails for the purpose of assisting law enforcement, as ISPs remain effectively immune from criminal and civil sanctions for such behavior. Furthermore, the *Wiretap Act* does not make available the remedy of the exclusionary rule for such violations. The Fourth Amendment does not provide much protection either, as the courts are reluctant to recognize a government agency relationship unless law enforcement officials make a direct request of a particular private actor to conduct a particular search. Barring a complete turnaround by the courts, it will be up to Congress to pass new legislation further amending the *Wiretap Act* to protect against the unprecedented threat ISPs currently pose to our privacy.

As ISPs today pose a much greater threat to our privacy than telephone companies ever have, Congress should at the very least proscribe ISP surveillance of stored e-mails on its systems to the same degree that it prohibited the interception of phone calls under the *Wiretap Act*.[262] Random ISP monitoring, whether conducted by the government or private ISPs, should be prohibited, unless done exclusively for mechanical or service quality control checks. ISPs should face the threat of criminal prosecutions for violations of the Act, and also should bear the threat of civil liability for any searches they conduct absent a subjective and objective good faith belief of the lawfulness of their actions. Most importantly,

261. *Walther*, 652 F.2d at 793. For full discussion, *see supra*, pt. IV.C.3.

262. *See supra*, pt. III.A.

the exclusionary rule should be made available as a remedy against evidence obtained from unlawful surveillance by ISPs, much like it is for that conducted by telephone companies.[263] This is especially the case when such ISP surveillance is carried out, in part, as a response to the calls of the government for vigilance and assistance.

263. *See supra*, pt. III.A.3.