THINKPIECE

THE FOURTH AMENDMENT UNPLUGGED: ELECTRONIC EVIDENCE ISSUES & WIRELESS DEFENSES

BY TARA MCGRAW SWAMINATHA*

I. INTRODUCTION

It would be foolish to contend that the degree of privacy secured to citizens by the Fourth

---

Jointly reviewed and edited by YALE JOURNAL OF LAW & TECHNOLOGY and INTERNATIONAL JOURNAL OF COMMUNICATIONS LAW & POLICY.

* B.A. with high distinction, University of Virginia, M.T., University of Virginia, J.D. expected, Georgetown University Law Center. I would especially like to thank Scott Eltringham for his invaluable suggestions, which led to the creation of this piece, as well as his comments and insight throughout its development. I also wish to thank Kristy Bernard, Kelsi Brown Corkran, Robert A. Kaplan, Elizabeth Kennett, Jeffrey Shulman and Michael Songer for their suggestions and edits, all of which were important and very much appreciated.

> *Amendment has been entirely unaffected by the advance of technology.*[1]
>
> *The question . . . is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.* [2]

Well-established legal principles govern evidentiary issues arising from technology developments. [3] In the United States, the Supreme Court and Courts of Appeals in every circuit draw from non-computer and non-wireless Fourth Amendment doctrine to address nascent electronic evidence issues. I agree that legal analyses drawing from historical treatment can be effective, but will argue in this Article that Internet access raises difficult legal issues to which standard Fourth Amendment analysis cannot be easily applied. Furthermore, the analyses will become more difficult with the introduction of wireless Internet access.[4] As wireless Internet connectivity burgeons throughout the world, unsecure connections[5] will likely become a haven for illegal activity. Courts should consider and investigate the unique issues presented by wireless Internet access in depth to avoid setting unwanted precedents when they are, inevitably, presented with a defendant whose wireless connection was used to commit a crime.

---

1 Kyllo v. United States, 533 U.S. 27, 34 (2001) (citing California v. Ciraolo, 476 U.S. 207, 215 (1986)).

2 *Id.* (citing Florida v. Riley, 488 U.S. 445 (1989)).

3 *See, e.g.*, *id.* at 33-34.

4 "Wireless Internet access," Wireless Internet," "wireless access," "wireless network," and "wireless connection" are used interchangeably in this paper, although each has a slightly different meaning. All five terms are used herein to describe a network configuration where the owner has a single wireless access point connected to the Internet via an Internet Service Provider (ISP). The owner has a computer (either a desktop or laptop) with a wireless modem used to connect to the wireless access point. The wireless access point can be a hub, router, or any similar device. *See generally* Tracey Meyers, *802.11, What really is Wi-Fi?*, NET4NOWT (Aug. 21, 2003) , *at* http://www.net4nowt.com/isp_news/news_article.asp?News_ID=1219.

5 WorldWideWarDrive.org occasionally conducts informal surveys across the globe to determine how many wireless access points are detectable and unsecure. The most recent effort, "WWWD3," was conducted June 28, 2003, through July 5, 2003. WWWD3 revealed 88,122 access points. 67% did not have encryption enabled. WorldWideWarDrive.org *at* http://www.worldwidewardrive.org (Dec. 18, 2003).

A. NOVEL ELECTRONIC EVIDENCE ISSUES

In the first section of this paper, I will describe Fourth Amendment doctrine governing warrantless computer searches in the United States. This area of the law is unsettled. Although this paper treats only relevant United States law, the normative claims advanced are equally relevant to courts throughout the world. In countries experiencing rapid growth in the use of technology, such as China or countries that are part of the European Union, courts, government prosecutors, defendants and technology users will face the same evidentiary challenges as are discussed in this paper.

Enough cases with similar facts have percolated through United States courts that even though Fourth Amendment law governing technology is unsettled, meaningful distinctions can be drawn among opinions. I focus on courts' attempts to apply well-established warrantless search requirements to cases where electronic evidence is collected for use in a criminal prosecution. Courts loosely follow the Supreme Court's method for interpreting new search and seizure issues. Nevertheless, I discuss some courts' evaluations of search and seizure issues raised by technology to establish a basis for further discussion. In 2003, two courts addressed this issue and arguably expanded the boundaries of Fourth Amendment jurisprudence.[6] By using a set of hypothetical facts, I will examine the factors a court considers both (1) in determining whether a private searcher is considered a government agent for Fourth Amendment purposes, and (2) in determining the permissible scope of a government search following a private one.

In the second section of this paper, I examine a series of legal issues that I anticipate arising from offenses committed via unsecure wireless networks.[7] Once a government official has evidence gathered from a private, warrantless search like the

---

6 *See* United States v. Jarrett, 338 F.3d 339 (4th Cir. 2003) (finding no Fourth Amendment violation where FBI knew of and tacitly acknowledged warrantless search by hacker searching for electronic evidence); New York v. Emerson, 766 N.Y.S.2d 482 (Sup. Ct. 2003) (finding no Fourth Amendment violation where government viewed more files than the preceding warrantless private search because court found viewing more files not did not exceed scope of initial private search).

7 *See* Richard Shim, *Wi-Fi Arrest Highlights Security Dangers*, CNET NEWS.COM (Nov. 28, 2003), *at* http://news.com.com/2100-1039-5112000.html.

hypothetical one set forth in the first section, both the government and the defendant face additional challenges of proof if the defendant used a wireless network in the commission of the crime. Should the government be entitled to a presumption that the evidence on the computer belongs to the owner? How could the defendant prove it was not he who used his network connection to commit an offense? If the defendant ran an unsecure wireless hub, should courts consider him as having facilitated offenses committed by others? Should the defendant be liable to third-party victims of offenses committed by a person who hijacked his wireless Internet connection? Is a defendant negligent by not securing his wireless Internet connection? Courts will have to grapple with such evidentiary questions in the near future. Although the potential answers in this context are expected to run parallel to those from existing theories of liability and culpability, they do not. Because wireless Internet legal questions are new, they cannot yet be analyzed comprehensively. In this paper, I set out existing law, pose potential issues raised by wireless network use, and suggest how the law might be applied or how it may evolve.

B. HYPOTHETICAL FACTS

Fourth Amendment analyses are highly fact-specific. [8] Because of this, I will use a set of hypothetical facts to frame the electronic evidence search and seizure discussion throughout the paper. The hypothetical facts are as follows:

> While servicing a customer's computer, a computer repair technician ("the Technician") discovered files he believed were indicative of criminal conduct: receipt and possession of child pornography under 18 U.S.C. § 2252(a)(5)(B).[9]

8 United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1998) ("Having reached [a] conclusion, however, we are quick to note these results are predicated only upon the particular facts of this case, and a search of computer files based on different facts might produce a different result.").

9 18 U.S.C. § 2252(a)(5)(B). Section 2252(a)(5)(B) criminalizes "knowing[] possess[ion] [of] a computer disk "that contains *an image* of child pornography produced with materials shipped in interstate commerce." (Emphasis added). Electronic evidence raises suspicion of crimes other than child pornography. In *United States v. Carey*, a repairperson suspected electronic pictures indicated illegal drug enterprise activities. 172 F.3d at 1270. Similarly, electronic documents could raise suspicions of terrorism-related activities. Because evidence of crimes other than child pornography is

After alerting law enforcement authorities, the Technician searched the computer again and uncovered additional evidence. The government seeks to admit evidence obtained by the Technician at a later trial and search the rest of the computer.

The customer ("Defendant X") claims he never viewed, downloaded or otherwise accessed child pornography. Defendant X accesses a broadband Internet connection from his home using a wireless hub and modem. The hub, because it is used with default factory-configured settings, permits any computer with a wireless modem within 100 to 500 feet to access it automatically. Gaining access to Defendant X's hub provides access to the Internet via Defendant X's broadband Internet connection. Defendant X claims the actual perpetrator ("Perpetrator Y"), unbeknownst to Defendant X, accessed the Internet through Defendant X's wireless hub, gaining access to and viewing child pornography images. Perpetrator Y then used a simple file transfer application to store the images on Defendant X's computer for subsequent viewing. These images are the pictures the Technician later discovered on Defendant X's computer when he brought it in for servicing.

Perpetrator Y is probably liable for several civil and criminal offenses because of his conduct. Federal law explicitly prohibits intentional or attempted interception of electronic communication, *in transit*, by both government and private citizens under 18 U.S.C. § 2511. Federal law also prohibits unauthorized intentional access to *stored* electronic communications under § 2701 and unauthorized access to computers in general under § 1030. [10] Furthermore, Defendant X may be

more likely to raise First Amendment issues, they are not treated herein. This paper uses child pornography as its hypothetical crime because a layperson can more easily identify child pornography than most other genres of electronic evidence. *Cf.* United States v. Grimes, 244 F.3d 375, 378 (5th Cir. 2001); United States v. Hall, 142 F.3d 988, 995 (7th Cir. 1998).

10 Many states have similar statutes. *See, e.g.*, HAW. REV. STAT. § 708-895.7 (2002); CONN. GEN. STAT. ANN. § 53a-251 (West 2003); N.H. REV. STAT. ANN. § 638:17 (2003); N.J. STAT. ANN. § 2A:38A-3 (West 2003).

entitled to civil damages from Perpetrator Y as provided in § 2520. Although not addressed in the scope of this paper, offenses committed under §§ 1030, 2511, 2520, and 2701 via wireless networks create challenges for both prosecution and defense.

In the context of the hypothetical scenario, I address the following evidentiary issues related to electronic evidence collection: (1) whether the evidence collected by the Technician in the initial search can be admitted; (2) whether the evidence collected by the Technician after contacting the government can be admitted; and (3) whether evidence collected by the government during a warrantless search of Defendant X's computer beyond those files the Technician accessed or viewed during his initial search can be admitted. Further, I set out problems facing Defendant X in defending himself against crimes he alleges Perpetrator Y committed; and potential civil claims against Defendant X by third parties. The issues analyzed under existing law highlight problems that arise by drawing analogies to existing theories of liability.

II. ELECTRONIC EVIDENCE AND PRIVATE SEARCHES

A. EVOLUTION OF FOURTH AMENDMENT JURISPRUDENCE

Legal principles, including those concerning Fourth Amendment jurisprudence, evolve with technological advances. When deciding novel Fourth Amendment issues, the Supreme Court first determines whether a certain government act violates the Fourth Amendment, the Court first determines whether the search and seizure would have been unlawful under the common law when the Fourth Amendment was written.[11] Only when this inquiry produces no answer does the Court turn to a "modern balancing test" [12] to evaluate the intrusion. The modern test balances the degree of intrusion on an individual's privacy with the need for the intrusion in order to promote legitimate governmental interests.[13] As Tracey Maclin notes,

11 Tracey Maclin, *Let Sleeping Dogs Lie: Why the Supreme Court Should Leave Fourth Amendment History Unabridged*, 82 B.U. L. REV. 895, 896 (2002) (quoting Wyoming v. Houghton, 526 U.S. 295, 299 (1999) (legal analysis of a Fourth Amendment challenge to a police intrusion)).

12 *Id.* (citing *Wyoming*, 526 U.S. at 299).

13 *Wyoming*, 526 U.S. at 299.

however, the Court considered historical common law in just one out of eleven Fourth Amendment cases in its 2000 and 2001 terms. [14] Maclin argues that lower courts are left with insufficient "guidance on when or why history makes a difference"[15] in Fourth Amendment interpretation. Lower courts quietly ignore the Supreme Court's suggested historical analysis.[16]

Courts of appeals have similarly neglected to consider common law principles. For example, in *United States v. Carey*, the Tenth Circuit examined the reasonableness of a police officer's search of a computer for child pornography.[17] Framing its Fourth Amendment inquiry, the court professed to follow the Supreme Court's guidance and began with a historical analysis.[18] The court shed no light on common law search and seizure concerns in the 1700s except noting that it must consider that a search could not "constitute[] general rummaging in 'flagrant disregard' for the terms of the warrant."[19] Having apparently fulfilled its duty to history, the court then, as most do, examined the current doctrine of warrantless police searches[20] without further historical discussion.

This method of examining 18th century Fourth Amendment jurisprudence is ineffective for determining 21st century Fourth Amendment electronic evidence issues. Professor Terrance Sandalow has stated that "[a]n understanding of the current meaning of . . . clauses limiting governmental power, depends far more on familiarity with the history of the twentieth century than of the latter years of the eighteenth."[21] Analyses of electronic evidence issues are difficult to parse, and their outcomes are difficult to predict for two reasons. First, Fourth

---

14 Maclin, *supra* note 11, at 896, 972. Maclin disputes the Court's claim that history is the departure point for every case it will decide. *Id.*

15 *Id.* at 899.

16 *Cf. id.* at 971-72.

17 *United States v. Carey*, 172 F.3d at 1270 (analyzing reasonableness "in light of what was reasonable at the time of the Fourth Amendment's adoption").

18 *Id.* at 1272 (analyzing reasonableness "in light of what was reasonable at the time of the Fourth Amendment's adoption").

19 *Id.* (quoting United States v. Foster, 100 F.3d 846, 849 (10th Cir. 1996)).

20 *Id.* at 1272.

21 Maclin, *supra* note 11, at 971 (quoting Terrance Sandalow, *Constitutional Interpretation*, 79 U. MICH. L. REV. 1033, 1050 (1981)).

Amendment analyses in particular are highly fact-specific. Second, where the common law sheds no light on the case at hand, the courts will determine an intrusion's legality under a modern balancing test that proceeds with little guidance.[22] The increasing pervasiveness of wireless networks will only exacerbate the difficulties in crafting workable, predictable balancing tests or defining appropriate presumptions. Perpetrators can gain access to wireless networks and use them to commit crimes while going undetected with surprising ease. The presumption that where electronic evidence is found on a computer, knowledge of the evidence's existence can be imputed to the owner of the computer should be challenged. Presumptions are discussed below.[23] Wireless network owners could be facilitating the commission of crimes unknowingly. The presumption that wireless network owners who fail to secure their networks should not be liable to third parties for offenses committed via their networks should also be challenged. Liability to third parties is discussed below.[24]

B. TECHNOLOGY'S IMPACT ON THE FOURTH AMENDMENT

In *Kyllo v. United States*, the Supreme Court commented on the impact technology has on Fourth Amendment jurisprudence, noting that technology has affected notions of privacy. [25] By way of example, the Court noted that "the technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private." [26] The Court is mindful of the curious tension brought about by the ability of technology to impact our notions of expected privacy.[27] As a new type of technology become inextricably linked with daily life, reasonable expectations of privacy are consequently redefined.

"Americans' love affair with technology is one of the defining characteristics of our culture."[28] Internet penetration

22 *See id.* at 896.
23 *See infra* Part III.B.1.
24 *See infra* Part III.B.2.
25 *See* 533 U.S. at 33-34.
26 *Id.* (citing California v. Ciraolo, 476 U.S. 207, 215 (1986)).
27 *Id.*
28 JOHN B. HORRIGAN, PEW INTERNET & AMERICAN LIFE PROJECT, CONSUMPTION OF INFORMATION GOODS AND SERVICES IN THE UNITED

in the United States reached sixty-three percent in April 2003.[29] Wireless Internet access is predicted to reach forty-eight percent of Internet users in the United States by 2005.[30] Even while 69 percent of the population is not technologically proficient,[31] the courts endeavor to keep pace with the 31 percent that is by establishing electronic evidence jurisprudence.[32] In criminal cases in particular, electronic evidence issues are increasingly important.[33]

C. WARRANTLESS SEARCHES

The hypothetical facts in this paper describe a warrantless search of Defendant X's computer by a technician. Courts consider two questions when determining if a government warrantless search of a computer violates the Fourth Amendment: (1) whether the search violates a reasonable expectation of privacy,[34] and if so, (2) whether the

---

STATES, i, (Nov. 23, 2003), *available at* http://www.pewinternet.org/reports/pdfs/ PIP_Info_Consumption.pdf.

29 HORRIGAN, *supra* note 28, at 4. Some facets of electronic evidence jurisprudence are unsettled or not fully realized. The Pew Report provides a frame of reference for understanding the growing number of individuals in the United States who may be effect by electronic evidence jurisprudence. The Pew Report identifies three tech-savvy segments of the American population: the "Young Tech Elites, the Wired GenXers, and the Older Wired Baby Boomers." *Id.* at 5. Comprising one-third of the population, these three tech-savvy segments crave information technology and engage in intense information exchanges. *Id.* They spend more money on technology goods and services than other, less tech-savvy segments of the population. *Id.* The less tech-savvy use less technology due to lack of time, experience, or levels of interest in information goods and services. *Id.*

30 *See* Press Release, Computer Industry Almanac, Inc., Internet Users Will Top 1 Billion in 2005 – Wireless Internet Users Will Reach 48% in 2005 (Mar. 21, 2001), *available at* http://www.c-i-a.com/pr032102.htm.

31 HORRIGAN, *supra* note 28, at 4.

32 Courts are no strangers to technology. Novel legal issues arise and are settled by applying existing principles as courts come up to speed with technology. *See, e.g.*, *Kyllo*, 533 U.S. 27 (applying Fourth Amendment to thermal imagery surveillance technology); Bartnicki v. Vopper, 532 U.S. 514 (2001) (applying Fourth Amendment to intercepted cellular telephone conversations); Katz v. United States, 389 U.S. 347 (1967) (applying Fourth Amendment to phone-booth conversation surveillance). This paper merely suggests two current novel issues courts will need to solidify.

33 Amy Baron-Evans & Martin F. Murphy, *The Fourth Amendment in the Digital Age: Some Basics on Computer Searches*, 47 BOSTON B. J. 10, 13 (2003).

34 *See* Illinois v. Andreas, 463 U.S. 765, 771 (1983).

search can be considered reasonable because it falls within an exception to the warrant requirement.[35]

A search is constitutional if it does not violate a person's "reasonable" or "legitimate" expectation of privacy.[36] This inquiry embraces two discrete questions: first, whether the individual's conduct reflects "an actual (subjective) expectation of privacy," and second, whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'"[37] In most cases, the difficulty of contesting a defendant's subjective expectation of privacy focuses the analysis on the objective aspect of the test defined in *Katz v. United States*,[38] i.e., whether the individual's expectation of privacy was reasonable.

No bright line rule indicates whether an expectation of privacy is constitutionally reasonable.[39] For example, the Supreme Court has held that a person has a reasonable expectation of privacy in property located inside a person's home,[40] in "the relative heat of various rooms in the home" revealed through the use of a thermal imager,[41] in conversations taking place in an enclosed phone booth,[42] and in the contents of opaque containers.[43] In contrast, the Court has held that a person has no reasonable expectation of privacy in activities conducted in open fields,[44] in garbage deposited at the outskirts of real property,[45] or in a stranger's house that the person has entered without the owner's consent in order to commit a theft.[46]

The Fourth Amendment protects against unreasonable government – not private – searches. Therefore, it does not restrict the hypothetical Technician's initial search.[47] If the Technician also happens to be a confidential government informant, he could be found to be acting as a government agent

---

35 *See* Illinois v. Rodriguez, 497 U.S. 177, 185 (1990).
36 *Katz*, 389 U.S. at 362 (Harlan, J., concurring).
37 *Id.* at 361.
38 *See id.* at 347.
39 *See* O'Connor v. Ortega, 480 U.S. 709, 715 (1987).
40 *See* Payton v. New York, 445 U.S. 573, 589-90 (1980).
41 *See Kyllo*, 533 U.S. 27.
42 *See Katz*, 389 U.S. at 358.
43 *See* United States v. Ross, 456 U.S. 798, 822-23 (1982).
44 *See* Oliver v. United States, 466 U.S. 170, 177 (1984).
45 *See* California v. Greenwood, 486 U.S. 35, 40-41 (1988).
46 *See* Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978)
47 United States v. Jacobsen, 466 U.S. 109, 113 (1984).

and not a private citizen.[48] Whether a confidential informant is acting as a government agent is determined on a case-by-case basis by the district judge.[49] In a case analogous to the hypothetical scenario, a United States district court suppressed evidence of child pornography collected by a computer technician because the technician was a government informant and not a private citizen.[50]

The Fourth Amendment protects an individual's privacy from certain forms of government intrusion by prohibiting unreasonable searches and seizures by government actors.[51] The Fourth Amendment is "wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual."[52] If a court finds that the Technician acted as an instrument or agent of the government when conducting the search, however, the search is then subject to Fourth Amendment restrictions.[53]

Federal courts use a multi-part test in determining whether a private party has acted as a government agent. The test includes (1) whether the government knew of and acquiesced to the search; (2) whether the private party's purpose was to assist law enforcement or was independently motivated; and (3) whether the government requested the action or offered a reward.[54] The defendant, Defendant X, bears the burden of proving that the private party acted as an agent of the government.[55] Federal courts note that determining an agency relationship is a fact-intensive inquiry[56] not unlike general

48 United States v. McAllister, 18 F.3d 1412, 1417 (7th Cir. 1994).

49 *Id.*

50 United States v. Barth, 26 F. Supp. 2d 929, 933-935 (W.D. Tex. 1998).

51 Walter v. United States, 447 U.S. 649, 656 (1980); *Katz*, 389 U.S. at 350.

52 *Jacobsen*, 466 U.S. at 113 (internal citations omitted).

53 *McAllister*, 18 F.3d at 1417 (citing United States v. Coolidge, 403 U.S. 443, 487 (1971)).

54 *See, e.g.*, United States v. Crowley, 385 F.3d 553, 558 (7th Cir. 2002) (internal citations omitted).

55 *See, e.g.*, United States v. Feffer, 831 F.2d 734, 737 (7th Cir. 1987).

56 *See, e.g.*, United States v. Ellyson, 326 F.3d 522, 527 (citing United States v. Koenig, 856 F.2d 843, 847 n.1 (7th Cir. 1988)).

Fourth Amendment inquiries. Not all factors are weighted equally.[57]

1. TECHNICIAN'S AGENCY STATUS

Prior to contacting the government, the Technician unquestionably acted as a private citizen. Under traditional Fourth Amendment analysis, his *subsequent* searches could be considered private searches as well, under the government agent analysis. Thus, electronic evidence collected in the technician's initial search will probably be admitted.

In *United States v. Hall*, on facts closely analogous to the hypothetical facts, the Seventh Circuit conducted its government agent analysis where a computer technician searched a customer's computer and found evidence of child pornography prior to contacting the government.[58] The court concluded the technician acted as a private citizen because the search was conducted pursuant to the technician's work servicing the computer for the sole purpose of testing the computer, the government had no knowledge of the technician's search and the government did not instruct the technician to inspect the files.[59] The court also noted in its analysis that the technician did not contact the government until *after* the evidence was collected.[60]

The Fourth Circuit has held that even if the technician had attempted to aid the government, and the government both knew of the search and failed to proscribe further inspection, the search may still have been upheld.[61] In general, if a court finds that the hypothetical Technician did not act as a government agent, evidence collected in subsequent private searches by the Technician will not be suppressed *even* after contacting law enforcement authorities. Once a private searcher contacts the

57 *See Feffer*, 831 F.2d at 737 (7th Cir. 1987) (finding that a private searcher motivated to aid investigation after contacting government agents *not* acting as government agent where government did not request involvement and she had other motivations) (emphasis added).

58 United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998).

59 *Id.*

60 *Id.* (emphasis added).

61 *Cf.* United States v. Jarrett, 338 F.3d 339 (4th Cir. 2003). *See* discussion *infra* pp. 13-14.

government, at least one federal court explicitly regards the government agent analysis as a "difficult issue."[62]

In *United States v. Feffer*, a private searcher met with government agents to discuss her discovery of evidence that the defendant falsified his tax returns.[63] After this meeting, the private searcher searched the defendant's financial papers again.[64] The court noted several factors in its analysis of the application of the Fourth Amendment. First, although in this second search the searcher's motivation was in part to aid law enforcement, it was not her only goal.[65] More significantly, the government never requested documents from the private searcher nor expected to receive anything after their initial contact.[66] Last, the court noted that the government did not directly participate in collecting the evidence.[67] On these bases, the court did not suppress evidence collected from the search conducted after the private searcher contacted the government.[68]

The hypothetical case is analogous to *Feffer* in that the government did not request that the Technician further search the customer's computer nor did the government directly participate in collecting the evidence. Even if, *arguendo*, the Technician's motivation in the subsequent searches was to aid the government, without government inducement to continue searching, evidence collected should be admitted at trial.[69] As the Seventh Circuit said in *United States v. Shahid*,

> [a] private citizen might decide to aid in the control and prevention of criminal activity out of his or her own moral conviction . . . or even desire to incarcerate criminals, but even if such private purpose should happen to coincide with the purposes of the government, "this happy

62 *Feffer*, 831 F.2d at 737.
63 *Id.*
64 *Id.* at 739-40.
65 *Id.*
66 *Id.* at 739.
67 *Id.*
68 *Id.* at 739-40.
69 United States v. Shahid, 117 F.3d 322, 325 (7th Cir. 1997).

> coincidence does not make a private actor an arm of the government."[70]

A private search can be converted into a government search only where the government exercises power over the private searcher.[71] Based on Fourth Amendment jurisprudence governing non-computer searches, the evidence collected by the Technician in searches before and after contacting the government would be admitted.

In 2003, the Fourth Circuit, in *United States v. Jarrett*,[72] departed from traditional doctrine. The court significantly relaxed the government agent test for Fourth Amendment purposes.[73] The court held that prior email contact between the government and a private citizen and passive acceptance by the government of a private search by this citizen did not make the private citizen a government agent.[74] In *Jarrett*, the private citizen hacked into the defendant's computer in search of child pornography ("the Jarrett searches").[75] Finding child pornography, the private citizen hacker then copied the electronic files and turned them over to the FBI.[76]

The government was aware the private citizen had conducted a similar search a year before ("the first search"). [77] In the first search, the private citizen discovered electronic files by hacking into a computer and delivered them to the FBI, aiding the FBI in identifying a different defendant.[78] Between the first search and the Jarrett searches, the FBI had exchanged emails with the private citizen. [79] In these emails, the private citizen discussed his intent to continue hacking into child pornographers' computers and the government made "a vague offer of availability to receive more information in the future."[80]

---

70 *Id.* at 326 (quoting United States v. Koenig, 856 F.2d 847, 850-51 (7th Cir. 1998)).

71 *Id.* at 325 (quoting *Koenig*, 856 F.2d at 849-50).

72 338 F.3d 339 (4th Cir. 2003) (finding no Fourth Amendment violation where FBI knew of and tacitly acknowledged warrantless search by hacker searching for electronic evidence), *discussed infra* p.7.

73 *See id.*

74 *Id.* at 341-42 (4th Cir. 2003).

75 *Id.* at 342.

76 *Id.*

77 *Id.* at 345-46.

78 *Id.*

79 *Id.*

80 *Id.*

Despite this contact, the court held that because the government was "under no special obligation to affirmatively discourage [the hacker] from hacking," the government's knowledge did not make the private citizen hacker a government agent.[81] Although the Fourth Circuit described the government's behavior as "discomforting," and noted that the government "operated close to the line" in its contact with the hacker, it upheld the search.[82]

Whether or not the result is preferable for policy reasons (which it may be), this court appears to be collapsing a multi-part test[83] into one factor: whether the government encouraged the additional searching. But for (a) the first search, that is, a previous case in which the hacker turned over evidence to the FBI, (b) the hacker's email indicating intent to do so again, and (c) the FBI's reply "vaguely" indicating willingness to receive more information, the court's holding would be in line with existing doctrine. These departures, however, are in conflict with other circuits' analyses.

The government in the hypothetical case did not encourage the Technician to search Defendant X's computer further. The Technician's continued searching was conducted of his own volition and even if his motivation was to aid law enforcement, his contact with the government does not give rise to an agency relationship. In light of this, courts will probably admit evidence collected after contacting the government.[84] The conduct does not approach that of the hacker in *Jarrett* who, despite concomitant "discomforting" government behavior, was still not considered a government agent.[85] In all circuits, the evidence collected during the Technician's searches after contacting the government will be admitted.

---

81 *Id.*

82 United States v. Jarrett, 338 F.3d 339, 347 (4th Cir. 2003).

83 Discussed, *supra* Part I.C.

84 *But see Barth*, 26 F. Supp. 2d at 936. In *Barth*, a technician discovered incriminating files, contacted the government and conducted a further search of the customer's computer. *Id.* The court held that once the technician contacted law enforcement officials, he became a government actor and suppressed evidence collected even though he did not continue searching at the government's request or with its tacit approval. *Id.*

85 *Jarrett*, 338 F.3d at 347.

2. SCOPE OF SUBSEQUENT GOVERNMENT SEARCHES

The government may conduct a search or seizure following the private search without a warrant if the scope of the search mirrors that of the private citizen's search.[86] In such an event, no warrant is required because the private, legal search has destroyed any legitimate expectation of privacy in the package's contents.[87] That is, the government may view all files viewed by the Technician without obtaining a warrant because Defendant X's expectation of privacy in those files is destroyed.[88]

The capacity to claim Fourth Amendment protection depends on whether a person had a reasonable expectation of privacy in the invaded place.[89] "If the files were closed and their contents not apparent from the exterior, the reasonable expectation of privacy continue[s] [only] so long as the files had not been searched *before* contact with the government occurred."[90] The government may re-open and view any computer files searched by the technician.[91] Further, courts may not suppress some files the government viewed beyond those viewed by the Technician. The boundaries establishing the scope of subsequent law enforcement searches of Defendant X's computer, where that search might include files not viewed by the technician, are as yet unsettled.[92]

The Tenth Circuit, in *United States v. Carey*, excluded electronic evidence of child pornography from an officer's search

---

86 *Jacobsen*, 466 U.S. at 115.

87 *Id.* at 118-22.

88 *See* New York v. Emerson, 766 N.Y.S.2d 482, 486 (Sup. Ct. 2003) (citing *Jacobsen*, 466 U.S. at 119).

89 U.S. v. McNeal, 77 F.3d 938, 945 (7th Cir. 1996) (citing *Rakas*, 439 U.S. at 143)).

90 United States v. Knoll, 16 F.3d 1313, 1320 (2d Cir. 1994) (emphasis added).

91 *See Emerson*, 766 N.Y.S.2d at 487.

92 The law regarding the acceptable scope of government searches of a computer pursuant to a warrant is also unsettled. *Cf. Carey*, 172 F.3d at 1272-75 (discussing acceptable scope of computer search pursuant to terms of a warrant); *United States v. Tamura*, 694 F.2d 591, 595-96 (9th Cir. 1982) (discussing acceptable scope of "intermingled documents" pursuant to terms of a warrant). Although technology exists that can indicate which files were viewed when, it is not reliable. The technology cannot always detect *who* viewed files when. Further a particularly savvy user can view files without leaving a trace.

pursuant to a valid warrant. [93] The warrant authorized the officer to search the defendant's computers for drug-related files, including "'names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances.'"[94] The detective and a computer technician conducted the search by viewing the directories (containing lists of file names) of the defendant's computers' hard drives.[95] The detective noticed "sexually suggestive titles and the label 'JPG.'"[96] In order to search the actual contents of the files, the detective used a government computer to search "text-based" files on disks copied from the defendant's computers for certain key words.[97] The detective then viewed the image files from the defendant's computers because he believed they "could contain evidence pertinent to a drug investigation such as pictures of 'a hydroponic growth system and how it's set up to operate.'"[98]

Although the search produced no text files "related to drugs," the detective opened files that contained child pornography.[99] It was not his discovery of evidence of other crimes that *per se* violated the warrant, rather the fact that the files had sexually suggestive titles which should have indicated their content.[100] The officer should have obtained a second warrant to continue searching for child pornography based on the probable cause he discovered while searching for the drug-related files.[101]

---

93 *See Carey*, 172 F.3d at 1276.

94 *Id.* at 1270 (quoting the warrant's text).

95 *See id.*

96 *Id.* at 1270-71. The file extension, ".jpg" typically indicates an image file.

97 The detective searched for "'names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances.'" *Id.* at 1271.

98 *Id.*, n.2. The detective testified later, however, that when he discovered the first JPG file, "he did not know what it was nor had he ever experienced an occasion in which the label 'JPG' was used by drug dealers to disguise text files." *Id.* Although it is unlikely that the detective was searching for drug-related files when he opened the image files because he knew their titles were sexually suggestive but *not* that they were, in fact, images, the detective's statement that image files could include drug-related files is valid.

99 *Id.* at 1270-71.

100 *Id.*

101 *Id.* at 1276-77.

The court in *Frasier v. Indiana*[102] faced a similar set of facts. An officer searching a computer pursuant to a warrant authorizing a search for drug-related files discovered evidence of child pornography.[103] The officer then obtained a second warrant to search for child pornography and the court did not suppress the evidence obtained pursuant to the second warrant.[104] The court distinguished itself from *Carey* by noting that the officer opened *ambiguously* labeled computer files only then to discover child pornography, whereas in *Carey* the files were undisputedly sexually suggestive.[105]

The court paid special attention to the fact that a file can be deliberately mislabeled in order to deceive and therefore held police should not be forced to rely on a defendant's own labeling of his computer files.[106] Drawing an analogy, the court noted that

> a computer image file is akin to a photograph sealed in an envelope or folder. And the name given to the file is like a label stuck onto the envelope or folder. Although such a label might say "Tax Records," the photograph inside could be of a nude child. Likewise, a computer image file containing child pornography could easily be named "tax_ records.xls," in an attempt to hide its actual contents. The approach suggested by [the defendant] would require the police to rely upon the name and file extension given to a file in order to determine its contents. . . . An officer searching for one type of record on a computer should not be forced to rely upon the name given to a file, which might very well hide its actual contents. In order to find out what is contained in the file, it must

---

102 794 N.E.2d 449 (Ind. App. 2003).

103 *Id.* at 453.

104 *Id.* at 455.

105 *Id.* at 465-66 (emphasis added). In order to satisfy particularity requirements, warrants for electronic evidence should describe either physical hardware to be seized (i.e., an entire computer), or the category of information to be searched for (e.g., "all records relating to an elaborate fraud scheme"). COMPUTER CRIME & INTELLECTUAL PROPERTY DIVISION, U.S. DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 88-89 (2002), *available at* http:// www.cybercrime.gov/s&smanual2002.htm (last visited Feb. 25, 2004).

106 *Id.*

> necessarily be "opened" in some way to ascertain its contents.[107]

Regarding initial *private* searches, rather than initial searches pursuant to a warrant authorizing an officer to search for evidence of unrelated crimes, courts also disagree as to the permissible scope of a later government search. In *United States v. Runyan*,[108] a contested government search exceeded the scope of the initial private search because the government searched beyond computer disks examined initially by the defendant's wife. On the other hand, in *United States v. Grimes*,[109] the government seized only what the repair technician viewed during an initial search and therefore did not exceed the initial search scope.

In another possible expansion of the Fourth Amendment in 2003, a New York state court stretched the permissible scope of a warrantless government search following a private search in *New York v. Emerson*.[110] The government examined additional files but was held *not* to have exceeded the scope of the initial private search.[111] In *Emerson*, the court held that FBI agents could look at files the private citizen had not viewed during the private search without violating the Fourth Amendment.

Both *Emerson* and *Jarrett* will impact future warrantless searches. The courts were presented with fact patterns where the government acted beyond previously recognized boundaries of warrantless searches in two different areas. The government did not violate the Fourth Amendment in either case. *Emerson* and *Jarrett* do not change the requirement that the government must obtain a second warrant if it has possession of a computer and discovers probable cause to search for evidence of a second crime. Courts following *Jarrett*, however, might admit evidence obtained by non-government-agent hackers or other private searchers where the government knew of or acquiesced to but did not explicitly, affirmatively encourage the search. Courts not following *Jarrett* will continue to interpose a more obvious dividing line between agent and non-agent status by requiring that the government not know of the continued private search.

---

107 *Frasier*, 794 N.E.2d at 465-66.
108 275 F.3d 449 (5th Cir. 2001).
109 244 F.3d 375 (5th Cir. 2001).
110 766 N.Y.S.2d. 482 (Sup. Ct. 2003).
111 *Id.* at 494-95.

Courts following *Emerson* may admit electronic evidence collected by the government where the government did not obtain a warrant to search additional files on a defendant's computer after a private citizen examined only a few files. Courts will be forced to address the permissible Fourth Amendment scope. Courts could define the scope narrowly, restricting it to electronic files in the same sub-folder or folder as the files viewed by the private searcher. Courts could also define the scope more broadly, by admitting government-viewed files in the same drive partition or computer as files viewed by the private searcher. Courts may constrict the permissible scope and treat each individual file separately, as a piece of evidence that must have been viewed by the private searcher before the government can view it without a warrant. Courts may expand the scope and treat each computer separately, enabling the government to view every file without a warrant. Courts might also find middle ground by differentiating among folders or sub-folders; under this theory, the private searcher, by viewing one file in a folder would enable the government to view all of the other files in just that folder.

Returning to the hypothetical case, in order to search other areas of Defendant X's computer, most courts will require the government to obtain a valid search warrant. The government may use evidence obtained by the Technician to establish probable cause requisite to obtain a search warrant.[112] In order to establish probable cause to search, the affidavits must include a "'fair probability that contraband or evidence of a crime' will be found in the location identified in the search warrant."[113]

Most cases regarding evidence collected during computer technicians' searches involve discovery of files indicating possible criminal child pornography possession.[114] Also, in most cases, electronic pictures discovered by a technician contain evidence of child pornography sufficient to establish probable cause for a search warrant.[115] In the hypothetical case, the files discovered by the technician must indicate a fair probability

112 *Hall*, 142 F.3d at 995.

113 *Id.* at 995 (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

114 *See, e.g.*, *Grimes*, 244 F.3d at 378; *Hall*, 142 F.3d at 995.

115 *See, e.g.*, *Id.* at 378; *Hall*, 142 F.3d at 995. *But see* United States v. Harned, 182 F.3d 928, 1999 WL 362397, at **2 (9th Cir. June 2, 1999) (finding files computer technician believed to be child pornography insufficient to establish probable cause for a search warrant).

that evidence of the alleged crime will be found on Defendant X's computer.[116] If this condition is met, the government can use evidence collected by the technician's initial search — prior to contacting the government — as probable cause for a search warrant. [117] The government could then access or view other files on Defendant X's computer according to the terms of a valid warrant.[118]

If the files discovered during the Technician's search are not sufficient to establish probable cause, the government can neither obtain a warrant based solely on electronic files viewed by the Technician, nor conduct a further search of the computer for evidence to bolster a finding of probable cause. The files viewed in the Technician's search may, however, be used in conjunction with other information legitimately obtained through government investigation to establish probable cause. Only after obtaining a valid search warrant based on other evidence could the government then search the rest of the customer's computer.

D. CONCLUSIONS ON ELECTRONIC EVIDENCE AND PRIVATE SEARCHES

In brief, evidence obtained during the hypothetical Technician's initial search, albeit warrantless, is admissible. The government may use evidence collected by the Technician to establish probable cause for a search warrant to search other areas of the computer for additional evidence. Evidence collected by the government in a warrantless search mirroring the Technician's is admissible. The government can view any files viewed by the Technician without a warrant and possibly other files located within the same folder as those viewed by the Technician depending on the jurisdiction and possibly turning on the actual file names. Without a warrant, the government may examine this limited set of files, probably those in the same folder as the files viewed by the Technician even if not accessed or viewed by him. Before searching other areas of Defendant X's computer, the government must obtain a search warrant.

Certain fact patterns test the limits of existing legal doctrine in ways that warrant careful consideration. Adding to

116 *Hall*, 142 F.3d at 995.
117 *Grimes*, 244 F.3d at 378; *Hall*, 142 F.3d at 995.
118 *Grimes*, 244 F.3d at 378; *Hall*, 142 F.3d at 995.

the facts in the hypothetical case, I now assume the evidence was collected without violating Defendant X's constitutional rights. The fact that Defendant X used a wireless network and claims that Perpetrator Y, in fact, downloaded the child pornography, presents additional issues to which I now turn.

III. ELECTRONIC EVIDENCE AND WIRELESS INTERNET ACCESS

"Unfortunately, some people abuse public anonymity systems by engaging in criminal actions such as large-scale intellectual property theft, financial crimes, copyright infringement, cyberstalking threats, child pornography, and even terrorist instructions."[119]

A. WIRELESS (IN)SECURITY ENABLES OFFENSES

"The modern world relies on computer security and increasingly finds that it cannot be taken for granted."[120] Wireless Internet users like Defendant X usually do not grasp the extent to which their computers and Internet connections are vulnerable.[121] The *San Diego Union Tribune*, to curb this growing problem, created public service announcements to alert people that hackers can access everything on a computer with an improperly secured (or unsecure) wireless access point.[122] A computer user with basic computer skills can *unintentionally* access Defendant X's electronic communications sent over his wireless network.[123] Every time Defendant X logs into his email account, his username and password are sent over the wireless network unencrypted, that is, readable by a person without

---

119 *See* Jonathan I. Edelstein, *Note, Anonymity and International Law Enforcement in Cyberspace*, 7 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 231, 250-51(1996). *But see* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 26 (1999) ("[University] networks [should be open] for anonymous use because . . . 'people should have the right to communicate at the university anonymously, because the First Amendment to the Constitution guarantees the same right vis-à-vis governments.'" (quoting Geoffrey Stone, Provost of the University of Chicago)).

120 Ethan Preston & John Lofton, *Computer Security Publications: Information Economics, Shifting Liability and the First Amendment*, 24 WHITTIER L. REV. 71, 76 (2002).

121 Lisa Weinreb, *Personal Technology: Five Questions*, SAN DIEGO UNION-TRIBUNE, Nov. 17, 2003, at C1.

122 *Id.*

123 Erik Sherman, *Why Wi-Fi Worries?*, NEWSWEEK, Dec. 2003, 41.

computer-aided translation.[124] Wireless Internet appliances are inherently unsecure if installed with default, out-of-the-box configurations.

In wired networks, hackers and attackers cannot steal electronic communications or access computers unless they are in close physical proximity to the network.[125] The attacker must be close enough to use "listening equipment [physically connected to the network] to intercept waves emitted as data flows through the network."[126] In wireless networks the same attacker could accomplish the same nefarious goals simply by sitting in her car parked on the street in front of Defendant X's house. "Wardriving,"[127] the practice of driving around in search of accessible wireless home or business networks is well known in major cities.[128] Wardrivers survey and record accessible wireless access points, often posting them on Web sites.[129] Would-be perpetrators can even enter a zip code in various databases on Web sites[130] and locate the nearest wireless access point.

---

124 *Id.* Unencrypted text is readable by humans. Encrypted text is scrambled so that it is only decryptable (and then readable) by a software application using an algorithm and secret key. *See* DEBORAH RUSSELL & G.T. GANGEMI SR., COMPUTER SECURITY BASICS 169-71 (1991); SIMSON GARFINKEL & GENE SPAFFORD, PRACTICAL UNIX AND INTERNET SECURITY 142-46 (1996).

125 TARA M. SWAMINATHA & CHARLES R. ELDEN, WIRELESS SECURITY AND PRIVACY: BEST PRACTICES AND DESIGN TECHNIQUES 45 (2002). The goal of wireless security is to approach that of wired networks. *Id.*

126 *Id.*

127 "War driving" gets its name from a practice popular in the 1980s called "war dialing." War dialers called phone numbers at random searching for unprotected modems through which they gained access to networks. *Id.* at 188.

128 Leigh Dyer, *Security Key For Wireless Networks*, CHARLOTTE OBSERVER, Nov. 15, 2003, at 1A.

129 According to the World Wide War Drive, wardriving is not the practice of attempting unauthorized access to unsecure networks. Its aim is to "generate awareness of the need by individual users and companies to secure their access [by] occasionally conduct[ing] informal surveys across the globe to determine how many wireless access points are detectable and unsecured." *At* http://www.worldwidewardrive.org/faq.html (Dec. 18, 2003). The website includes a page on ethics, encouraging users to abide by laws and not access networks, merely note their existence. http://www.worldwidewardrive.org/ethics.html.

130 *See, e.g.*, NetStumbler's database, *at* http://maps.netstumbler.com or its nationwide map *at* http://www.netstumbler.com/nation.php.

Warchalking is another method of finding access points and making their locations known to others. Warchalkers make symbols using chalk on building walls or pavement to indicate a spot where one could access a wireless network. The symbols are universal in the United States and abroad[131] and they could alert would-be perpetrators to Defendant X's (or even Corporation Z's) free Internet connection. Businesses who do not secure wireless Internet connections arguably open themselves to even more serious threats than home users.[132] Warchalking is not as pervasive as once predicted. [133] Searching online Wardriving databases is still more efficient for would-be perpetrators attempting to locate unwitting users' wireless Internet access.

The goal of wireless security is to approach the security of wired networks.[134] Although inherently unsecure, wireless access points can be configured so that they are more secure than their default configurations. The easiest ways to bolster security on a wireless access point are to enable wireless encryption, allow access only to IDs of specified wireless network cards,[135] and by not broadcasting the access point's ID.[136] While not failsafe, using encryption[137] protects against inadvertent, unintentional access to Defendant X's wireless Internet connection.[138] Enabling encryption also protects against significantly more intentional attempts.

---

131 *See* Warchalking.org's symbol pocket guide, *at* http://www.blackbeltjones.com/warchalking/warchalking0_9.pdf.

132 Connecting to a business's wireless access point gives the hacker access to the company's corporate network *behind* the company's firewall affording access to sensitive internal data as well as facilitating general Internet access.

133 *See* Nick Langley, *The Demise Of Warchalkers*, COMPUTER WEEKLY, June 25, 2003, at 36.

134 SWAMINATHA & ELDEN, *supra* note 125, at 45.

135 MAC address filtering.

136 Its SSID.

137 The most prevalent wireless standards in the United States are versions of 802.11 (e.g., 802.11b). Wireless encryption deployed with virtually all 802.11 wireless access points is called Wired Equivalent Privacy (WEP). SWAMINATHA & ELDEN, *supra* note 125, at 45. Early versions of WEP were broken in the Spring of 2001. *Id.* at 47. The current state of WEP, while not unbreakable, affords protection against unintentional or passive access and all but the most diligent and skilled hackers. *See id.* at 48.

138 Tyler Hamilton, *Beware Roving Hackers, Wireless Networkers Are Warned; Recent Arrest Underlines Systems' Vulnerability,*

The concern at hand is not whether this intentional access is an offense. Recall that people like the alleged Perpetrator Y who intentionally use another's wireless Internet connection are violating several federal laws.[139] Is the potential for wireless crimes merely hype? Prior to November 2003, the concerns about individuals like Perpetrator Y committing crimes by usurping wireless connections were only theoretical, albeit highly possible; no wireless crimes had been identified or charged. In the last two months of 2003, wireless crimes were charged. In North Carolina, a man pled guilty to two felony counts and one misdemeanor for accessing confidential patient records via a hospital's wireless network.[140] In Detroit, three 20-year-olds faced federal criminal charges for attempting to misappropriate credit cards by hacking a store's wireless network, which caused damages in excess of $2.5 Million dollars according to the government; two pled guilty in May 2004.[141]

While there are endless concerns regarding unsecure wireless networks,[142] the concern at hand is that without

---

Owners Could Find Themselves Accused Of Crimes, TORONTO STAR, Nov. 24, 2003, at D03.

139 Intentional access to Defendant X's wireless network violated, *inter alia*, 18 U.S.C. §§ 1030, 2511, 2520, and 2701. *See supra* pp. 4-5.

140 *See* Gary Villani, *Landmark Conviction Handed Down In Cyber Case*, HOLLY SPRINGS SUN, Nov. 19, 2003, *available at* http://www.hollyspringssun.com/news/2003111900438.html (last accessed Dec. 2, 2003). The man was sentenced to 18 months in prison and ordered to pay $10,000 restitution to the victim. *Id.*

141 *See* Dyer, *supra* note 128. The three were indicted on charges of conspiracy, wire fraud, computer fraud, unauthorized computer access, intentional transmission of computer code, and attempted possession of unauthorized access devices for accessing the store's wireless network more than ten times in three weeks. *Three Indicted For Alleged Hacking*, GRAND RAPIDS PRESS, Nov. 21, 2003, at A2. The first two to plead guilty will face shorter sentences in consideration for cooperation with law enforcement by disclosing details about the intrusions. The third has been arraigned but no further information is available yet regarding his plea or conviction. *See* Roberts, Paul, *Michigan Man Pleads Guilty to Wireless Hack Into Stores,* COMPUTERWORLD (Jun. 7, 2004), available at http://www.computerworld.com/securitytopics/security/holes/story/0,10801,93708,00.html (last visited October 14, 2004).

142 Files that should be protected could be stolen. Medical records in hospitals, legal documents in law firms or government documents in government agency unsecure wireless networks could all be misappropriated easily.

encryption or other security mechanisms,[143] anyone near Defendant X's house can access his network and use his Internet connection to commit offenses.[144] In November 2003, Toronto police reported the first offense committed via an unsecure wireless network. The facts are comparable to the hypothetical case set forth in this paper. In Toronto, police pulled over a car headed the wrong way on a one-way street.[145] The driver ("the Toronto driver") was watching a pornographic video on a laptop computer on his front seat.[146] The Toronto Driver apparently hijacked a residential wireless Internet connection and was using it to view the pornographic video.[147] He was charged with possession of child pornography,[148] the first such charge committed via a wireless network in Canada.[149] While the Toronto Driver committed the first crime using an innocent person's wireless Internet connection, the differences between this case and Perpetrator Y's are significant.

First and foremost, the police caught the Toronto Driver in the act. His unknowing Internet access provider, the wireless connection owner whose connection he used to view the child pornography, will not have difficulty proving her innocence. Defendant X, on the other hand, has no proof that Perpetrator Y is the true offender.[150] As George DuPont has observed, "[d]ue to advances in technology and the emergence of cyberspace, personal identities and physical locations are far more easily

---

143 Security products called Virtual Private Networks (VPNs) can also bolster security. *See, e.g.*, SWAMINATHA & ELDEN, *supra* note 125, at 135-150; Sherman, *supra* note 123, at 41.

144 *See* Hamilton, *supra* note 138, at D03.

145 *Id.*; *Half-Naked Man Stole Wireless Web Access, Was Looking At Child Porn*, CANADIAN PRESS, Nov. 22, 2003.

146 Hamilton, *supra* note 138.

147 *Id.*

148 The article cites a Toronto Police press release. The press release was unavailable on the Toronto Police website, http://www.torontopolice.on.ca/. Emails to the contact for press release inquiries returned undelivered.

149 Hamilton, *supra* note 138.

150 There are network monitoring tools Defendant X could have used to allow him to gather some information and/or records about Perpetrator Y's access and activity. It is highly unlikely Defendant X would *not* secure his wireless access point but *would* be able to install, configure and understand network monitoring tools. *See, e.g.*, STANFORD LINEAR ACCELERATION CENTER, NETWORK MONITORING TOOLS, *at* http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html (last accessed Feb. 25, 2004).

cloaked in anonymity and pseudo-anonymity than ever before."[151]

B. DEFENDANT X'S CRIMINAL AND CIVIL LIABILITY

Wireless Internet access issues parallel existing theories of liability and culpability in other legal disciplines but present new challenges. Courts now must grapple with these challenges. Prosecuting Perpetrator Y for unauthorized access to Defendant X's home computer via his wireless network or for unauthorized use of Defendant X's wireless Internet connection is the tip of the iceberg.

Still in infant stages, wireless Internet legal issues cannot yet be comprehensively analyzed. Defendant X faces several problems in defending himself against crimes he alleges Perpetrator Y committed and potential civil claims against him by third parties. As stated earlier, the issues analyzed under existing law highlight problems that arise by drawing analogies to existing theories of liability.

1. BURDENS OF PROOF AND DEFENDANT X'S DEFENSES

Ethan Preston and John Lofton believe that "[t]he fundamental problem recognized by legal commentary is that perpetrators of computer crime are not only difficult to identify; they are difficult to apprehend and prosecute or sue."[152] The government must prove each element of a crime beyond a reasonable doubt.[153] Criminal possession statutes in general usually require "knowingly receiving an item" or "retention after awareness of control over it."[154]

---

151 George F. du Pont, *The Time Has Come for Limited Liability for Operators of True Anonymity Remailers in Cyberspace: An Examination of the Possibilities and Perils*, 6 J. TECH. L. & POL'Y 3 (proposing limited liability for remailer operators).

152 Ethan Preston & John Lofton, *Computer Security Publications: Information Economics, Shifting Liability and the First Amendment*, 24 WHITTIER L. REV. 71, 80 (2002).

153 1 WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW §§ 1.8(a), (b) (2d ed. 2003).

154 *Id.* at § 6.1(e) (internal citations omitted).

Possession of child pornography, the federal crime with which Defendant X is charged, allegedly committed by Perpetrator Y, includes an element of scienter.[155] Courts cannot impose criminal responsibility in obscenity crimes without requiring proof of some level of knowledge on the part of the defendant.[156] Defendant X will not be found guilty unless the prosecution proves beyond a reasonable doubt that Defendant X "knowingly" possessed child pornography.[157] In existing case law where a defendant contests the prosecution's argument that the defendant knowingly possessed child pornography images, the defendant typically argues that he did not know the persons depicted in the images were minors.[158] Few, if any, child pornography cases involve a defendant who argues he did not know he actually possessed the images. The scienter element regarding a possession offense concerns the physical object, however, and not its properties.[159] If the government cannot prove beyond a reasonable doubt that Defendant X knew he physically possessed the images on his computer, a court cannot find him guilty.

Defendant X has still more significant hurdles to clear, however. Courts and legislatures create rebuttable presumptions when a defendant is found in possession of evidence.[160] One rebuttable presumption, "the presumption from recent exclusive unexplained possession of stolen property, [is that] the possessor stole it."[161] Criminal statutes sometimes make proof of a *physical* fact presumptive or prima facie evidence of a separate *mental* element required in order to convict a defendant.[162] This presumption gives the government a necessary advantage yet can be rebutted by a defendant.

In jurisdictions where the prosecution has the benefit of this presumption, Defendant X will have a difficult — almost impossible — time rebutting the presumption. Courts should

---

155 *See* 18 U.S.C. § 2252(A)(5)(b).

156 New York v. Ferber, 458 U.S. 747, 765 (1982) (citing Smith v. California, 361 U.S. 147 (1959); Hamling v. United States, 418 U.S. 87 (1974)).

157 *Id.*

158 *See e.g.*, *Ferber*, 458 U.S. at 765-66; Ashcroft v. Free Speech Coalition, 535 U.S. 234, 255 (2002).

159 LAFAVE, *supra* note 153 at § 6.1(e).

160 LAFAVE, *supra* note 153 at § 1.8(f) ("courts have created rebuttable presumptions in favor of the prosecution in some cases.").

161 *Id.*

162 *Id.*

take into account the fact that wireless networks are inherently unsecure when determining whether to grant the prosecution a rebuttable presumption that the evidence on a defendant's computer (a) belongs to the defendant or (b) can be used to prove a scienter element. Wired networks are not altogether secure, but are more secure than wireless networks. As a result, there may be legitimate reasons for treating one differently from the other. Although this is not unlike other non-electronic evidence (*e.g.*, that a defendant might argue drugs in his home were not his), the level of expertise required to adequately secure wired and non-wired networks should persuade courts to remove the presumption, relieving a defendant of the burden of proving electronic evidence found on his computer is not in fact his. This situation would be appealing to Defendant X because the hypothetical facts indicate that he may be an innocent, unknowing and an unwitting intermediary in Perpetrator Y's crime. If such defendants have no method by which they can introduce evidence to rebut the presumption, the presumption should not be granted.

Because both the average computer owner and Defendant X probably lack the expertise and resources required to show that someone else used their wireless networks and put files on their computers, the presumption is dangerous. One solution might be for courts to allow affirmative defenses that effectively rebut presumptions. In order to avail himself of the affirmative defense, Defendant X could cooperate with the government, allowing government technology experts to examine his computer to attempt to determine what user placed evidence on the computer. This scenario does not solve all problems, but it might help cooperative innocent defendants while still identifying guilty defendants. The success of this solution depends on the government technology experts' capabilities in examining computers for evidence. If the government cannot determine the identity of the perpetrator after examining the computer, the affirmative defense and burden-shifting does not solve any of the previous problems.

Because these cases are highly fact-specific, courts will not be able to create bright line rules without difficulty. If the courts altogether remove the rebuttable presumption regarding electronic evidence in general or electronic evidence on a wireless Internet user's computer, other problems arise. Removing the presumption would create an easy escape route for actual perpetrators. They could claim their networks were

usurped or their computers hacked. The government would then face an almost insurmountable task of proving a defendant was, in fact, the person who downloaded child pornography or committed another crime via the unsecure wireless connection.

In the hypothetical case in this paper, Defendant X may be able to avail himself of an established affirmative defense. The defendant has the burden of introducing evidence in support of an affirmative defense.[163] The federal statute under which Defendant X is charged provides two affirmative defenses. First, the defendant can escape prosecution by proving the individuals in the images were, in fact, all legal adults engaged in sexual activity who consented to having their images taken.[164] Second, a defendant is not responsible for possession if the defendant possesses less than three proscribed images, prevents anyone but law enforcement officials from accessing the images, reports the matter to law enforcement and promptly destroys such images.[165] Defendant X would undoubtedly be willing to contact law enforcement, prevent access (even simply by unplugging his wireless access point), and destroy the images. If there are three images or fewer on Defendant X's computer, he will not have to worry about the possibility of a rebuttable presumption that he knew the images existed because they were found on his computer.

If there are more than three images of child pornography on Defendant X's computer, the second affirmative defense will not be available. Defendant X will want to introduce evidence indicating that Perpetrator Y used Defendant X's Internet connection to commit the offense. Records from Defendant X's Internet Service Provider (ISP) might be of some assistance, albeit minimal. The records would not indicate that a user other than Defendant X accessed and downloaded child pornography unless the events occurred at a time Defendant can prove he was not at home. ISPs typically do not retain records indefinitely. Relevant records of activity on Defendant X's account will probably be purged from the ISP's records storage by the time Defendant X requests them or the ISP attempts to retrieve them.[166]

---

163 *See id.*

164 *Ashcroft*, 535 U.S. at 261 (citing 18 USC § 2252(A)(4)).

165 *Id.* (citing 18 USC § 2252(A)(5)).

166 ISPs typically store documents for 30-90 days.

This problem will arise in civil offenses as well. The suits that the Recording Industry Association of American (RIAA) is filing against individual users who download music in violation of copyright laws provide a current example. In one such case that received considerable press, the RIAA falsely accused a woman of copyright violations arising from the illegal downloading of thousands of songs.[167] The woman, a 66-year old sculptor, was able to convince the RIAA to drop its copyright suit against her because she owned a Macintosh computer (on which the file-downloading software could not run at the time), she had no file downloading software on her computer and claimed she was a "computer neophyte."[168] The RIAA claimed it was certain the IP address[169] associated with the woman's computer had been the recipient and transmitter of thousands of copyrighted songs.[170]

Either the woman's ISP matched the wrong customer with the IP address, or the RIAA made a mistake in identifying the IP address initially.[171] If the woman had a wireless Internet connection, the copyright-infringing downloading and uploading might have appeared to have originated from her IP address but actually have been the work of another party (such as Perpetrator Y). The fact that a defendant uses a wireless network increases the likelihood that network activity conducted via the defendant's Internet account was, in fact committed by someone usurping the defendant's network.

Imposing some liability on wireless users creates an incentive to secure their wireless networks. The notion of using criminal law to implement this incentive is troubling. Although the hassle of being accused of a crime might be sufficient, it is

---

167 *See* William Glanz, *Music Industry Plans Second Round Of Suits*, THE WASHINGTON TIMES, Oct. 18, 2003, at A01

168 Chris Gaither, *Recording Industry Withdraws Suit: Mistaken Identity Raises Questions on Legal Strategy*, BOSTON GLOBE, Sept. 24, 2003, *at* http://www.boston.com/business/articles/2003/09/24/recording_industry_withdraws_suit/.

169 An Internet Protocol (IP) Address is a unique identifier for any computer on the Internet. IP Addresses are not necessarily assigned to a computer indefinitely, however, and can be dynamically allocated by an ISP. When an ISP dynamically allocates IP Addresses, it assigns IP Addresses arbitrarily to users for certain periods of time. One user can have used hundreds of IP Addresses over the course of a month, making identification of a user by her IP Address difficult.

170 Gaither, *supra* note 168.

171 *Id.*

not a viable solution. Liability to third parties, both for wireless network owners and wireless equipment manufacturers, might provide a workable alternative.

2. DEFENDANT X'S CIVIL LIABILITY TO THIRD PARTIES

Defendant X may face civil liability to third parties for failing to secure his wireless network. These claims will not necessarily be successful but they present Defendant X with challenges. Perpetrator Y might have hacked into Corporation Z's private network via Defendant X's unsecure wireless network connection. Corporation Z might bring suit against Defendant X for damage caused, including financial loss due to stolen proprietary information and damage caused to internal computer or network systems.

Congress's Internet Caucus Wireless Task Force (ICWTF) has been considering the range of wireless technologies' technical and personal implications on public and private users.[172] In November 2003, the ICWTF convened a panel to informally discuss drafting legislation concerning liability and security.[173] Panelists agreed that the "liability implications of wireless data communications, including Wi-Fi, are unclear, and users need to know that they are dealing with some uncharted territory as to who can be held liable for misuse of their networks."[174] The panel believes that although "drive-by" downloaders or perpetrators can take advantage of unsecure access points, liability should not extend to the private owners for unauthorized use of their network.[175]

Stephen Henderson and Matthew Yarbrough argue otherwise.[176] Henderson and Yarbrough contend that applying traditional negligence liability will encourage better security on an inherently unsecure Internet.[177] Although ignorant parties

---

172 Mark Rockwell, *Panel Examines Wi-Fi Liability Issues*, WIRELESSWEEK.COM, (Nov. 4, 2003) *at* http://wirelessweek.com/index.asp?layout=documentPrint&doc_id=128175 (last accessed Nov. 4, 2003).

173 *Id.*

174 *Id.*

175 *See id.*

176 *See* Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Unsecure?: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11 (2002).

177 *Id.* at 11.

such as Defendant X lack criminal intent, if they could be considered knowingly unsecure with respect to a certain well-known threat or vulnerability, third-party victims might be able to recover damages in a tort suit.[178] Common law negligence doctrine is relatively unexplored in the modern Internet era.[179] Two negligence factors, causation and damages, will not be treated significantly different here than in non-computing cases.[180] Legal duty and an innocent access point owner's failure to conform to reasonable standards of care, however, are probable hotbeds for future litigation.[181] Generally, a person is subject to liability for negligent actions where the actions cause physical, personal or property injury to another. To illustrate their argument, Henderson and Yarbrough give an example of an attack on a third-party network via the innocent party's unsecure network. The third party network could sustain property damage, but this alone will not give rise to liability without the innocent person owing a duty to the third party.[182] Courts, or the legislature, (possibly prompted by the ICWTF to promulgate regulations), must decide whether Defendant X has a duty of care to a third party victim and if so, the duty's scope.

If a duty exists, courts still must define the standard of care required to fulfill that duty.[183] Computer owners and operators who are aware of potential vulnerabilities can take steps to fix them.[184] Their potential for liability would then decrease. By the same token, if such owners and operators fail to take action when they know of a vulnerability and how to fix it, they might be subject to increased liability. Imputing knowledge of a vulnerability, however, is elusive at best. Standards of care are derived from industry custom, notions of reasonable care and occasionally from relevant legislation.[185] No existing legislation mandates general Internet security on the part of all who access it. Federal and state legislation requires standards of care regarding technical security in certain industries including the healthcare industry and financial industry.[186] These

178 *Id.* at 14.
179 *Id.*
180 *Id.* at 14-15.
181 *See id.* at 15.
182 *Id.* at 16.
183 *Id.* at 17.
184 Preston & Lofton, *supra* note 152, at 83.
185 *Id.* at 18.
186 *See id.* at 19, 20 (citing Pub. L. No. 104-191, Pub. L. No. 106-102.)

standards aim to protect the confidentiality of stored information, not specifically to prevent unsecure networks from being exploited to perpetrate attacks and offenses.[187] Nevertheless, they may guide courts' analyses.[188] Courts cannot define standards of care outside the context of actual cases, so unless and until legislatures introduce standards of care, [189] negligence lawsuits, particularly against wireless Internet users who fail to reasonably secure their access points, may arise and increase in number.

I suggest a few potential solutions, none of which fully resolve the problems faced by Defendant X, the government or third party victims. First, the insurance industry might assist. As they do for other potential liabilities, insurance companies could define appropriate algorithms and companion actuarial tables. Under this scheme, individuals could purchase insurance against liability to third parties resulting from their failure to maintain secure wired or wireless networks. This might reduce courts' reluctance to assign civil liability, especially where defendants use unsecure *corporate* wireless networks. Furthermore, it might meet an important policy goal of encouraging corporate wireless network administrators to continually update their wireless network security schemes. Second, the government could use its purchasing power to require wireless network equipment manufacturers to produce secure products. If government procurement processes were designed to enforce regulations to that end, secure products would be increasingly produced. By sheer volume required by the government, industry will be able to produce secure products at lower costs. The products will be more readily available to the average user. There are possible complications resulting from this solution. Wireless users who purchase the cheaper, non-compliant (unsecure) wireless network equipment might be liable to any third parties for offenses conducted via their wireless networks for having chosen an unsecure option. If industry manufacturers risk liability for selling supposedly-secure products that turn out to be unsecure, this might drive up prices of the secure devices to compensate for damage awards paid by the manufacturers. These and other theories will certainly be raised in courts and in legislative proposals.

187 *See id.*
188 *See id.*
189 *Id.* at 25.

Courts could apply attractive nuisance theories. If courts took judicial notice of the fact that enough of the population is aware of the fact that wireless networks are inherently unsecure, and if unsecure wireless networks become hotbeds of illicit activity, courts might consider unsecure wireless networks an attractive nuisance and assign liability to wireless network owners on this basis. If most wireless networks were secure, running unsecure networks would attract criminals attempting to evade detection. Courts could also consider more technically savvy users more likely responsible for having secure wireless networks. While this policy mimics the higher standards of care required for certain specialized doctors, for example, it seems the worst suggestion of all because it creates a disincentive for the average person to become educated on wireless security. If the average user is deterred from learning about how to secure her wireless network, the potential for crimes to be committed via unknowing users' wireless networks will greatly increase.

Courts should craft careful solutions, bearing in mind how best to assign burdens; legislatures should create incentives that encourage an educated and more secure public. As soon as crimes committed via unsecure wireless networks become more prevalent, courts and legislatures will have to consider the variety of options presented herein. Several competing interests will define the resulting legal doctrine including: innocent defendants' need to offer exculpatory evidence; government's need to convict actual offenders; third parties' needs to seek remedies from wireless offenses committed against them; and the public policy goal of cultivating educated wireless Internet users and secure wireless networks.

IV. CONCLUSION

Electronic evidence presents many difficult but interesting and increasingly common issues for courts. Fourth Amendment doctrine on warrantless searches will continue to evolve in the face of advances in technology and changes in legal thinking. If the courts are overly protective of defendants' rights in this arena, the government will face difficulty in prosecuting cases involving electronic evidence collected from a private search. Once a critical mass of cases have percolated through the courts, government investigators and prosecutors will be able to better understand (1) what conduct will give rise to an agency relationship with a private searcher, rendering evidence

inadmissible and (2) the permissible scope of a warrantless search following a private one.

The legal doctrine governing warrantless searches for electronic evidence, though unsettled, is better established than legal doctrine regarding wireless Internet access. Even where electronic evidence is properly collected, criminal possession cases involving wireless networks present difficult problems for all parties involved. Investigators face challenges in identifying perpetrators. Prosecutors face challenges in alleging and proving scienter elements of offenses committed via wireless networks. Defendants are met with obstacles in obtaining exculpatory evidence where rebuttable presumptions are afforded to the prosecution. The removal of rebuttable presumptions protects actual perpetrators from conviction.

Defendants whose only defense to charges based on their possession of electronic evidence is that they are "computer neophytes" face difficulties. Courts should consider burden-shifting defenses, whether to assign rebuttable presumptions, what set of facts presents a question of fact for a jury, and what jury instructions would be proper in these wireless Internet, highly fact-specific inquires.