WIRELESS LIABILITY: LIABILITY CONCERNS FOR OPERATORS OF UNSECURED WIRELESS NETWORKS

*Casey G. Watkins**

INTRODUCTION

On February 11, 2011, a Department of Homeland Security Investigator discovered that a peer-to-peer network user, Doldrum, was in possession of and actively sharing image and video files depicting child pornography.[1] The agent identified Doldrum's IP

* J.D. Candidate, May 2013, Rutgers School of Law – Newark; Commentaries Editor, Rutgers Law Review; B.S. University of Idaho, 2008.

1. Wisniewski Affidavit ¶ 4, United States v. Luchetti, No. 1:11-cr-00143-RJA-HBS (W.D.N.Y. Mar. 15, 2011), ECF No. 1; Carolyn Thompson, *Unsecured Wi-Fi Can Lure Criminals, Cause Trouble for Internet Subscribers*, PENNLIVE.COM (Apr. 25, 2011, 12:21 PM), http://blog.pennlive.com/midstate_impact/print.html?entry=/2011/04/unprot

address using a software utility and shortly thereafter obtained the subscribers name and address from Time Warner Cable, his service provider.[2] Just before dawn on March 7, a team of seven U.S. Immigration and Customs Enforcement ("ICE") agents, armed with assault rifles and tactical gear, broke down the rear door of the suspect's house, seized a computer, two iPads, two cell phones, and detained the suspect.[3]

The suspect, a middle-aged businessman in Buffalo, New York, denied ever having downloaded child pornography. When confronted about the illicit file sharing he proclaimed his innocence, stating that "[s]omebody else could have [shared the files] but I didn't do anything like that."[4] After analyzing the contents of the seized electronics, federal agents found no evidence that anyone in the house had ever downloaded child pornography;[5] however, the businessman "maintained a wireless router at his residence that was not password protected, and could therefore be accessed by others in the vicinity of his residence."[6] A twenty-five-year-old neighbor who had repeatedly accessed the Internet through the businessman's unsecured wireless router was quickly identified as the actual culprit and charged with distribution of child pornography.[7]

Homeland Security officials issued an apology expressing regret "that the owner of the wireless system used in this case, who had nothing to do with the crime, was swept up into this investigation."[8] The businessman was not charged with a crime.[9] However, if a growing number of scholars and litigators have their way, people in his situation could face liability for the criminal and tortious activities committed by others over their unsecured wireless networks.

Criminal liability for the actions of third parties committed over unsecured wireless networks is largely theoretical for the moment;[10]

---

ected_wi-fi_can_lure_cri.html.

2. Wisniewski Affidavit , *supra* note 1, ¶ 5-6.

3. Thompson, *supra* note 1.

4. *Id.*

5. Dan Herbeck, *Child Porn Raid Wrong, but No Apology by Feds: W. Side Businessman Traumatized at Home Because of "Wi-Fi Theft,"* BUFFALO NEWS, Mar. 17, 2011, at A1.

6. Wisniewski Affidavit, *supra* note 1, ¶ 7.

7. Thompson, *supra* note 1. The neighbor was charged with violating 18 U.S.C. § 2252A(a)(2)—"knowing distribution of child pornography . . . transported in interstate . . . commerce by any means, including by computer." Criminal Complaint at 1, United States v. Luchetti, No. 1:11-cr-00143-RJA-HBS (W.D.N.Y. Mar. 15, 2011), ECF No. 1.

8. Dale Anderson, *Feds Apologize for Raid Violating West Side Home: Wrongful Invasion to Get Hochul Review*, BUFFALO NEWS, Mar. 18, 2011, at A1.

9. Thompson, *supra* note 1.

10. *See* Susan W. Brenner*, Toward A Criminal Law for Cyberspace: Product Liability and Other Issues,* 5 U. PITT. J. TECH. L. & POL'Y 2, 51-63 (2004) (advocating

however, civil liability is an increasingly real possibility facing wireless network operators. A growing number of plaintiffs' lawyers in digital copyright infringement cases are aggressively pursuing claims against even unlikely defendants. Most notably, in one case a seventy-year-old grandmother was accused of pirating pornography.[11] Furthermore, plaintiffs' lawyers state in settlement letters that "[t]he Internet Service Provider . . . account holder is responsible for securing [their] [wireless] connection and may be legally responsible for any infringement(s) that result from an unsecured wireless network/router," even if a "spouse, child, roommate, employee, or business associate" committed the infringement.[12] Some of these initial settlement letters even state that the affirmative defense of having an unsecured wireless network "has never been successfully argued, in multiple contexts, including child pornography and civil copyright infringements actions."[13]

Recently, negligent operation of a wireless network ("WLAN") has also begun to appear as a cause of action in digital copyright infringement cases.[14] One unnamed defendant ("Doe 4") even agreed

---

criminal liability for users who fail to take necessary precautions against becoming victims of cybercrime through a modified assumption of the risk or complicity theory); Susan W. Brenner, *Toward A Criminal Law for Cyberspace: A New Model of Law Enforcement?*, 30 RUTGERS COMPUTER & TECH. L.J. 1, 75-89 (2004) (arguing for criminal liability based on an assumption of the risk concept for "regular" adults).

11. James Temple, *Lawsuit Says Grandma Illegally Downloaded Porn*, SFGATE (July 15, 2011), http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/07/15/BUG51KA26R.DTL. The plaintiff dropped its claims against the women after the story garnered media attention, stating in a letter "the law firm found the actual person responsible for downloading the material in question." James Temple, *"Porn Granny" Update*, S.F. CHRONICLE, Aug. 31, 2011, at D1. A legally blind man, "physically incapable of watching any film," was also sued by another adult film producer, Imperial Enterprises, Inc., for alleged copyright infringement. Keegan Hamilton, *Porn, Piracy, & BitTorrent: The Film Industry Mounts A Sketchy Legal Strategy in Response to Illegal Downloads*, SEATTLE WKLY., Aug. 10, 2011, http://www.seattleweekly.com/content/printVersion/1395372.

12. *See, e.g.*, Letter from John L. Steele, Attorney, Steele Hansmeier, PLLC, to "M," Prospective Defendant in First Time Videos LLC v. Does 1-500, No. 1:10-cv-06254 (N.D. Ill. 2010) [hereinafter John L. Steele Letter], *available at* http://torrentfreak.com/the-anatomy-of-a-bittorrent-piracy-settlement-110606.

13. *Id.*

14. *See, e.g.*, Complaint ¶¶ 229-238, 808 Holdings, LLC v. Collective of Dec. 30, 2011 Sharing Hash E37917C8EEB4585E6421358FF32F29CD63 C23C91ON, No. 12CV0215 MMA-RBB, 2012 WL 381682 (S.D. Cal. Jan. 26, 2012); Complaint ¶¶ 110–117, Third World Media, LLC v. Ariz. Members of Swarm of July 15, 2011 through July 24, 2011, Sharing Hash File BD55F2868E09C08DADFC1032CCE43DE2BC1A2D17, No. 11CV01931, 2011 WL 4802886 (D. Ariz. Oct. 2, 2011); Complaint ¶¶ 373-80, Liberty Media Holdings, LLC v. Swarm of Nov. 16, 2010, Sharing Hash File A3E6F65F2E3D672400A5908F64ED55B66A0880B8, No. 11cv619 BTM BLM, 2011 WL 2491781 (S.D. Cal. Mar. 28, 2011) [hereinafter Swarm of Nov. 16, 2010 Complaint]; Complaint ¶¶ 274-80, Liberty Media Holdings, LLC, v. Does 1 through 62, No. 11cv0575 MMA NLS, 2011 WL 2491776 (S.D. Cal. Mar. 22, 2011).

to pay $10,000 as part of a settlement in which he "acknowledge[d] that a failure to secure [his] wireless internet router by password protection may invite infringing uses of copyrighted materials accessible to individuals through such a router."[15] Doe 4 also agreed to take steps to "secure his . . . router and to deny [the] use of his internet connection to anyone who would engage in infringing conduct."[16]

These attempts to establish liability for the operators of unsecured wireless routers pose a myriad of legal, moral, and policy questions. Not only are some of the claims made by plaintiffs' lawyers on shaky legal ground, the tactics being used in an attempt to extract settlements may cross ethical boundaries as well. These so-called "mass-BitTorrent" cases typically involve hundreds or thousands of defendants who have allegedly shared copyrighted content over peer-to-peer file sharing networks.[17] The largest cases to date involve the illegal sharing of feature films. Last year, Voltage Pictures, Inc., the production company that owns the copyright for *The Hurt Locker*, brought suit against 24,583 unnamed Does,[18] and the United States Copyright Group ("USCG") initiated an action on behalf of the studio that owns the rights to *The Expendables* against 23,322 Does.[19] Aside from these notable examples, however, the vast majority of these cases involve the illegal sharing of pornography and exploitation films.[20] The fact that pornography is involved has the potential to ratchet up the pressure on defendants to settle out of fear of public embarrassment or professional consequences, even if they did not infringe.[21] Critics of these suits claim that the studios are not seeking to deter piracy but use the legal system to create a revenue stream.[22] One class action complaint alleges they have used "fraudulent claims

15. Offer of Judgment Pursuant to Federal Rule of Civil Procedure 68 at pmbl., ¶ 4, *Swarm of Nov. 16, 2010*, No. 11cv619 BTM BLM.

16. *Id.* ¶ 6.

17. *See* David Kravets, *How Mass BitTorrent Lawsuits Turn Low-Budget Movies into Big Bucks*, WIRED.COM (Mar. 31, 2011, 2:36 PM), http://www.wired.com/threatlevel/2011/03/bittorrent.

18. Voltage Pictures, LLC v. Does 1–5,000, 818 F. Supp. 2d 28 (D.D.C. 2011). The suit originally targeted 5000 Does but Voltage subsequently filed an amended complaint adding 19,583 Does, identified by their respective IP addresses in a 397-page appendix. First Amended Complaint for Copyright Infringement ¶ 20, Voltage Pictures, LLC v. Vazquez, CA. 1:10-cv-00873-BAH (D.D.C. Apr. 22, 2011), ECF No. 172.

19. Nu Image, Inc. v. Does 1-23,322, 799 F. Supp. 2d 34, 36 (D.D.C. 2011).

20. Kravets, *supra* note 17.

21. *See id.*; Hamilton, *supra* note 11 (discussing the impact of lawsuit on defendant who maintains his innocence but may still settle "to make [the lawsuit] go away"); Carol Lundberg, *Sharing, Swarms and Suing Over Porn*, MICH. LAW. WKLY., Jan. 13, 2012.

22. Kravets, *supra* note 17.

and coercive statements" to create a "lucrative trade in monetizing copyright infringement allegations . . . . [with] one overriding goal: to 'obtain settlement'—not judgments."[23]

The allegations of negligence and contributory liability combined with the early settlement offers that allow defendants to remain anonymous create a powerful incentive to settle. These allegations and attempts to hold unsecured wireless network operators liable deprive society of important public benefits provided by open Internet access and place a high burden on anyone who owns a wireless router. Are the defendants in these cases truly negligent for failing to password protect their wireless network? Or, are they simply unnamed Does facing the embarrassing and expensive prospect of being named as a defendant in a copyright infringement action?

There is division among the courts concerning whether the negligence cause of action can even survive a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6). The division appears to center around the sufficiency of the plaintiff's pleadings in most cases,[24] and as of this writing, no court has entered a judgment on the merits concerning the negligence cause of action. Nevertheless, if it continues to be a successful means for extracting settlements from defendants, the existence of a duty to secure wireless routers may become established by virtue of its ubiquity alone.

This Note will focus on the liability of the wireless network operator for the wrongful acts committed by others on their unsecured networks. The legality of using another's wireless network without permission is very much an open question in many jurisdictions,[25] but that discussion is beyond the scope of this Note. The premise of this Note is that the operator of an unsecured wireless router is not liable for the wrongful acts of third parties

23. Class Action Complaint and Jury Demand ¶¶ 2-4, Shirokov v. Dunlap, Grubb & Weaver PLLC, No. 1:10-12043 (D. Mass. Nov. 24, 2010), ECF No. 1.

24. *See* Liberty Media Holdings, LLC v. Swarm of Nov. 16, 2010, Sharing Hash File A3E6F65F2E3D672400A5908F64ED55B66A0880B8, No. 11cv619–BTM (BLM), 2011 WL 1597495, at *4 (S.D. Cal. Mar. 28, 2011) [hereinafter *Swarm of Nov. 16, 2010 Case*] (holding plaintiff adequately alleged the elements of negligence and that the "negligence cause of action could withstand a motion to dismiss"); Liberty Media Holdings, LLC v. Does 1-62, No. 11cv 575 MMA (NLS), 2011 WL 1869923, at *3 (S.D. Cal. May 12, 2011) (holding plaintiff failed to assert a "legal duty in connection with the negligence cause of action").

25. *See* Patrick S. Ryan, *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, 9 VA. J.L. & TECH. 7, 7 (2004); Ryan Singel, *Burning Question: Is Wi-Fi Squatting Illegal?*, WIRED, Apr. 2011, at 58, *available at* http://www.wired.com/magazine/2011/03/pr_burning_wifi_squatting; *see also* Stacy Nowicki, *No Free Lunch (or Wi-Fi)*: *Michigan's Unconstitutional Computer Crime Statute*, 2009 UCLA J. L. & TECH. 1, 3-4 (2009) (arguing Michigan's prosecution of defendant who used café's Wi-Fi from his car is unconstitutional).

committed over his open Internet connection.

First, I will discuss the complex landscape of organizations attempting to shape the law and the technologies that make cybercrime and cybertort possible over wireless connections. Second, I will discuss the potential liability for negligence facing individuals who operate unsecured wireless routers. I will discuss the theory's shortcomings concerning copyright infringement cases, primarily federal preemption, and the Digital Millennium Copyright Act's (DMCA)[26] safe harbor provision. I will also evaluate the theory's merits concerning common law torts and discuss how holding WLAN operators liable for the wrongful acts of a third party places an unnecessary burden on law-abiding citizens. Next, I will argue that the Communications Decency Act of 1996 (CDA)[27] shields unsecured WLAN administrators from civil liability. Finally, I will argue that the attempts to hold unsecured wireless network operators liable for the act of third parties will have negative consequences for our society, and that any actions taken to limit the use of open wireless networks should take a reasonable approach that does not hold innocent parties liable for the wrongs of others.

I. CYBERCRIME, CYBERTORTS, AND ENABLING TECHNOLOGIES

A. Competing Interests in the Development of Cyberlaw

The rise of mass-BitTorrent litigation has sparked a tremendous debate among various online communities focused on technology and piracy. The small number settlements in which WLAN operators have admitted liability for the actions of third parties in particular have sparked a lively debate among copyright attorneys within these communities.[28] The landscape of cybercrime and cybertort law is still unsettled, and creative plaintiffs' counsel have been attempting to expand and adapt traditional common law causes of action to cyberspace. With technological development outpacing the governing legislative framework,[29] trade organizations and interest groups have

26. Digital Millennium Copyright Act (DMCA) of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.).

27. Communications Decency Act (CDA) of 1996, 47 U.S.C. §§ 230, 560-61 (2006), *invalidated in part by* Reno v. ACLU, 521 U.S. 844 (1997).

28. *See* Marc Randazza, *Are You Guilty if Pirates Use Your Internet? Lawyer Says YES*, TORRENTFREAK (Aug. 6, 2011), http://torrentfreak.com/are-you-guilty-if-pirates-use-your-internet-lawyer-says-yes-110806; Nicholas Ranallo, *Are You Guilty if Pirates Use Your Internet? Lawyer Says NO*, TORRENTFREAK (Aug. 6, 2011), http://torrentfreak.com/are-you-guilty-if-pirates-use-your-internet-lawyer-says-no-110806; Corynne McSherry, *Open WiFi and Liability for Copyright Infringement: Setting the Record Straight*, ELEC. FRONTIER FOUND. (Aug. 18, 2011), https://www.eff.org/deeplinks/2011/08/open-wifi-and-copyright-liability-setting-record.

29. *See* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1555-57 (2005).

started taking action in an attempt to influence and shape the future of cyberlaw. Among the most prominent of these organizations are the Electronic Frontier Foundation ("EFF"), the Recording Industry Association of America ("RIAA"), and the Motion Picture Association of America ("MPAA").

The EFF is a nonprofit advocacy organization that "confront[s] cutting-edge issues[,] defend[s] free speech, privacy, innovation, and consumer rights."[30] The EFF prepares whitepapers on technology issues and frequently files amicus briefs with courts hearing cases concerning technology. The RIAA is a trade organization that seeks to "protect the intellectual property and First Amendment rights of artists and music labels."[31] It also plays an active role in the legislative process by "monitor[ing] and review[ing] state and federal laws, regulations[,] and policies."[32] The MPAA bills itself as the "voice and advocate of the American motion picture, home video and television industries" that "engag[es] in a variety of legislative, policy, . . . and law enforcement initiatives."[33] All three of these organizations have attempted to influence the development of cyberlaw as it matures.

B. Wi-Fi and Wireless Technology

"[T]he development of the Internet [has] wreak[ed] havoc and let[] loose the gods of war in the field of copyright law."[34] Wireless technology has only added to the problem, and the technology needed to commit wrongful acts over an unsecured wireless Internet connection is now commonplace. Any portable device with a wireless network adaptor—from mobile phones, digital audio players and tablets to laptops—can access an unsecured wireless connection and be utilized for illicit purposes.[35] In order to understand the potential for liability unsecured wireless network operators face it is necessary to have an understanding of the technologies involved.

---

30. The EFF is the most prominent of the organizations advocating against regulation and industry. *About EFF*, ELEC. FRONTIER FOUND., https://www.eff.org/about (last visited Mar. 18, 2013).

31. *About RIAA*, RECORDING INDUS. ASS'N OF AM., http://www.riaa.com/aboutus.php?content_selector=about-who-we-are-riaa (last visited Mar. 18, 2013).

32. *Id.*

33. *Frequently Asked Questions*, MOTION PICTURE ASS'N OF AM., http://www.mpaa.org/faq (last visited Mar. 18, 2013).

34. EDWARD F. O'CONNOR, INTELLECTUAL PROPERTY LAW AND LITIGATION: PRACTICAL AND IRREVERENT INSIGHTS 212 (2009).

35. *See* Paul Boutin, *How to Steal Wi-Fi: And How to Keep the Neighbors from Stealing Yours*, SLATE (Nov. 18, 2004, 5:16 PM), http://www.slate.com/articles/technology/webhead/2004/11/how_to_steal_wifi.html; Marguerite Reardon, *Mobile Phone Wi-Fi Usage on the Rise*, CNET (Feb. 12, 2009, 9:56 AM), http://news.cnet.com/8301-1035_3-10162711-94.html (noting the increasing use of wireless Internet on mobile phones).

Wireless local area networks ("WLAN") allow computers and devices to connect to the Internet and each other over short-range radio connections without the use of wires.[36] The radio signal is propagated from a wireless access point ("WAP"), typically a wireless router in a residential setting, and can be connected to by any device with Wi-Fi capabilities. The coverage area and connections speed of wireless routers have increased dramatically over the past few years with the implementation of new standards. For example, the new "wireless-n" standard expanded the effective coverage area of WAPs from the 300 feet possible with the previous "wireless-g" standard to nearly 200 meters.[37] The extended range makes it increasingly more likely that third parties in other buildings or residences will be able to detect and potentially connect to wireless networks without being seen or detected.

The term Wi-Fi has become widely synonymous with any WLAN but in fact, Wi-Fi is a certification mark registered by the Wi-Fi Alliance, and signifies that the product meets the Institute of Electrical and Electronic Engineers ("IEEE") 802.11 standards.[38] For the purpose of this Note, the term WLAN is used to discuss wireless network technology unless a Wi-Fi Alliance product or certification is being referenced.

In simplistic terms, wireless networks can be operated in two ways—unsecured or secured. Unsecured or "open" WLAN connections broadcast unencrypted data and allow "roaming users to access the Internet through [the] network[] without the operator's express prior consent, and . . . knowledge."[39] Secured WLANs utilize some type of cryptographic protocol that prevents devices from accessing the broadcasted data without the appropriate key or password.[40] Most wireless routers ship from the factory with security disabled, a default network name, and a default administrative user name and password.[41] These default settings are designed to make

36. *See The How and Why of Wi-Fi*, WI-FI ALLIANCE, http://www.wi-fi.org/knowledge-center/articles/how-and-why-wi-fi (last visited Mar. 18, 2013).

37. IEEE , IEEE STD 802.11N–2009 at 1 (2009); *FAQs: What Is the Range of a Wi-Fi Network?*, WI-FI ALLIANCE, http://www.wi-fi.org/knowledge-center/faq/what-range-wi-fi-network (last visited Mar. 18, 2013); *see also* WI-FI ALLIANCE, WI-FI CERTIFIED N: LONGER-RANGE, FASTER-THROUGHPUT, MULTIMEDIA-GRADE WI-FI NETWORKS 2 (2009) ("Today's Wi-Fi CERTIFIED n devices can deliver five times or more throughput and more robust connections at up to twice the range of legacy 802.11 technology.").

38. WI-FI, Registration No. 2525795; *The How and Why of Wi-Fi*, *supra* note 36.

39. Benjamin D. Kern, *Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 101, 104 (2004).

40. *See* MATTHEW S. GAST, 802.11 WIRELESS NETWORKS: THE DEFINITIVE GUIDE 114-17 (2d ed. 2005). For a brief history of the development of modern cryptography, see MARK STAMP, INFORMATION SECURITY: PRINCIPLES AND PRACTICE 37-40 (2d ed. 2011).

41. *Security*, WI-FI ALLIANCE, http://www.wi-fi.org/discover-and-learn/security

end user configuration as simple as possible and the Wi-Fi Alliance recommends that the settings be changed as part of the network setup,[42] but that does not always happen.

While seventy percent of American households now have a wireless router installed, eleven percent do not have a password protecting their wireless connection and an additional four percent of those surveyed did not know if their wireless router was secured.[43] The reasons wireless network operators have for leaving their connections unsecured vary wildly. Some open WLAN operators have an ideological commitment to providing others free access to the Internet,[44] while others may be unfamiliar with the technology and unable to configure their network with a password.[45] Others may appreciate the risks of maintaining an open connection but decide not to invest the time required to secure the router.[46] Some WLAN operators also maintain an unsecured or poorly secured connection for compatibility with older electronic devices.[47]

There are now over 96,000 open public WLAN locations in the United States, most provided by coffee shops, hotels, and fast food restaurants.[48] Over fifty-five percent of the public Wi-Fi is now offered free.[49] Many of the open access hotspots do not use any form of encryption or monitoring software—allowing potential cybercriminals and wrongdoers to use the connection for nefarious

---

(last visited Mar. 18, 2013).

42. *Id.*

43. NAT'L CYBER SEC. ALLIANCE, 2010 NCSA / NORTON BY SYMANTEC ONLINE SAFETY STUDY 9 (2010), *available at* http://www.staysafeonline.org/download/datasets/2064/FINAL+NCSA+Full+Online+Safety+Study+2010[1].pdf.

44. *See* Peter Eckersley, *Why We Need an Open Wireless Movement*, ELEC. FRONTIER FOUND. (Apr. 27, 2011), https://www.eff.org/deeplinks/2011/04/open-wireless-movement; Anonymous Letter to Judge Sarah Evens Barker at 1, Hard Drive Prods. v. Does 1-21, No. 11-59 (S.D. Ind. June 6, 2011), ECF No. 12 (stating that anonymous Doe operates an unsecured WLAN "out of a sense of community").

45. *See* Kern, *supra* note 39, at 104.

46. *Id.*

47. Some older handheld game systems and mobile personal assistant devices do not support secured connections or only support the easily cracked WEP protocol. *See, e.g.*, *WEP & WPA – Wireless Security*, NINTENDO, https://www.nintendo.com/consumer/wfc/en_na/wep-wpa.jsp (last visited Mar. 18, 2013) (noting that "Nintendo DS Game Cards . . . are not compatible with WPA security"). Occasionally, manufacturer firmware defects limit a devices' ability to connect to secured or adequately secured connections. For example, several Apple products released in 2008 with the 2.1.1 firmware were widely reported to be incompatible with the WPA protocol, requiring users to connect either to an unsecured or highly exploitable WEP connection. *See* Rene Ritchie, *2.1 Experiencing WiFi Problems*, IMORE.COM (Sept. 11, 2008, 9:49 PM), http://www.imore.com/21-already-experiencing-wifi-problems-211-shipping-on-touch.

48. JIWIRE, MOBILE AUDIENCE INSIGHTS REPORT Q2 2011, at 12 (2011), *available at* http://www.jiwire.com/sites/default/files/JiWire_MobileAudienceInsightsReport_Q2211_1.pdf.

49. *Id.*

purposes.[50] With such a large and ever increasing number of open connections available, the likelihood of third parties connecting is high and the issue of liability for the actions of those third parties is an important issue that must be resolved.

The percentage of people that have accessed or attempted to access another's unsecured wireless Internet connection has increased from eighteen percent in 2008 to thirty-two percent in 2011.[51] Some of this unauthorized access is accidental, with some operating systems designed to automatically attempt to connect with unsecured wireless connections.[52] While much of this roaming use is harmless joyriding, some users connect to open WLANs with nefarious purposes in mind. An entire tech subculture of "war-driving" and "whacking" has developed around open wireless networks.[53]

Wireless joyriding is the term used to describe "harmless or inoffensive use of the Internet, such as checking emails, reading the news, and shopping online, while utilizing another's unsecured wireless network without authorization."[54] War-driving is the rather ominous sounding term for driving around a specific area and mapping wireless networks.[55] War-driving is relatively harmless because the person mapping the networks does not actually connect to the networks.[56] The information collected by war-drivers can be used for wrongful purposes by cybercriminals or "whackers"—roaming users that commit independently illegal Internet crimes over an unsecured WLAN.[57]

---

50. Barry D. Bayer, *Wifi Basics and Protecting Your Hotspot Surfing with HotSpotVPN*, LAW OFF. TECH. REV. 2 (2004), *available at* 2004 WL 1063205.

51. Press Release, Wi-Fi Alliance, Make Security a Priority in 2011: Protect Your Personal Data on Wi-Fi Networks (Feb. 2, 2011), *available at* http://www.wi-fi.org/media/press-releases/make-security-priority-2011-protect-your-personal-data-wi-fi%C2%AE-networks.

52. *See* Randy Cohen, *The Way We Live Now: 2-8-04: The Ethicist; Wi-Fi Fairness*, N.Y. TIMES, Feb. 8, 2004, § 6 (Magazine), at 22, *available at* http://www.nytimes.com/2004/02/08/magazine/the-way-we-live-now-2-8-04-the-ethicist-wi-fi-fairness.html; Kern, *supra* note 39, at 105 (noting Windows XP's "zero configuration" feature). Windows Vista and 7 operating systems have replaced zero configuration with the similar "Native Wifi API." *Wireless Zero Configuration Reference*, MICROSOFT, http://msdn.microsoft.com/en-us/library/windows/desktop/ms706593(v=vs.85).aspx (last visited Mar. 18, 2013).

53. Kern, *supra* note 39, at 104.

54. Taylor E. White, *Criminal Consequences of Wi-Fi Joyriding: Whose Interests Should Arkansas Protect?*, 62 ARK. L. REV. 125, 125 (2009).

55. CHRIS HURLEY ET AL., WARDRIVING & WIRELESS PENETRATION TESTING 3 (2007).

56. *Id.* at 4.

57. Kern, *supra* note 39, at 105-06.

C. Internet Crimes

Simply put, cybertorts and cybercrimes are wrongful acts or omissions "involv[ing] a computer and a network, where a computer may or may not have played an instrumental part" in the wrongful conduct.[58] There is a significant overlap in conduct that may constitute criminal or tortious activity over an unsecured wireless Internet connection. This Note will focus largely on Internet crimes, defined as "any illegal activity involving one or more components of the Internet, such as websites, chat rooms, and/or email."[59] The closely associated civil wrongs are included in this definition for the purpose of this discussion.

The list of possible Internet crimes includes: hacking, currency counterfeiting, spamming, child pornography or exploitation, fraud, harassment, arms trafficking, copyright piracy, trademark counterfeiting, and theft of trade secrets.[60] Among the possibilities, copyright infringement,[61] child pornography and exploitation,[62] and hacking[63] are the most likely to occur over an unsecured wireless connection. Roaming whackers are able to use open connections to commit Internet crimes and often escape undetected, leaving the easily identifiable WAP operator vulnerable to investigation and civil action by those harmed by the actual wrongdoer.

D. BitTorrent

The most popular file sharing protocol used to commit online

---

58. ROBERT MOORE, CYBERCRIME: INVESTIGATING HIGH-TECHNOLOGY COMPUTER CRIME 4 (2d ed. 2010).

59. *Frequently Asked Questions*, THE INTERNET CRIME COMPLAINT CTR., http://www.ic3.gov/faq/default.aspx (last visited Mar. 18, 2013).

60. *Reporting Computer, Internet-Related, or Intellectual Property Crime*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/criminal/cybercrime/reporting.html (last visited Mar. 18, 2013).

61. *See* Chadwick Schnee, Note, *A "Sound" Policy? The RIAA and the Copyright Act*, 9 U. PITT. J. TECH. L. & POL'Y 1, 2 (2009); *see, e.g.*, Declaration of Francisco Zuleta, Atlantic Recording Corp. v. Zuleta, No. 1:06-cv-1221-RWS (N.D. Ga. June 15, 2006), ECF No. 3; Mark Ballard, *P2P Pinball Lawyers Say Ignorance Is No Defen[s]e*, REGISTER, Apr. 17, 2007, *available at* http://www.theregister.co.uk/2007/04/17/davenport_evidence.

62. *See, e.g.*, Dan Duffy, *Unsecured Wireless Network Opens Way for Child Pornography*, SUBURBAN J. (July 11, 2007, 12:00 AM), http://www.stltoday.com/suburban-journals/article_dea80d98-52b3-52f9-b4e2-531515f48eba.html; Herbeck, *supra* note 5.

63. Ideological hacking is now the fastest growing category of web hacking incidents. TRUSTWAVE SPIDERLABS, WEB HACKING INCIDENT DATABASE SEMIANNUAL REPORT: JULY TO DECEMBER 2010, at 4–5 (2011). Groups like Anonymous have now made website downtime and defacement the two most common web hacking outcomes. *Id.* at 5. Hacking for profit is the third most popular category and typically involves collecting sensitive customer data that is sold on the black market. *Id.*

copyright piracy is the BitTorrent protocol.[64] Peer-to-peer file sharing, including BitTorrent, now accounts for over fifty percent of the total bandwidth used worldwide while traditional HTTP web traffic accounts for just thirty-two percent of global bandwidth.[65] BitTorrent is not used exclusively for copyright piracy. The protocol has tremendous promise as a tool to share and distribute large data files for many purposes, including distribution of open source software, public domain or freely licensed books, films, and other media.[66] The protocol has, however, become popular among copyright pirates because it does not require a central server to store the pirated file; instead the torrent file containing information about the target file is hosted, and the target file is disbursed across many individual computers.[67]

The BitTorrent ecosystem consists of peers, trackers, and torrent-discovery sites.[68] An individual peer seeking to download a file can search a torrent-discovery site to locate .torrent files.[69] Among the most popular public torrent-discovery sites are the Pirate Bay, Mininova, and isoHunt.[70] Private torrent-discovery sites like Demonoid, BitNation, and cinematik are also popular because they offer faster download speeds by requiring registration and mandating a minimum download to upload ratio. These sites provide an "easy-to-use directory and search engine for . . . torrent files" but do not host the content; instead they host .torrent files that only contain an infohash identifier and metadata.[71] Users open .torrent files with a BitTorrent client, a program capable of utilizing the BitTorrent protocol, and the BitTorrent client communicates with a tracker to obtain a list of peers also sharing the desired content.[72] Trackers are web-accessible computers that keep track of all the peers associated with a .torrent file and put them in touch with each other.[73]

The BitTorrent protocol allows large files to be split into small pieces and shared among a large group of peers.[74] The whole

64. BAYTSP, ANNUAL REPORT ONLINE TRENDS & INSIGHT 2008, at 3 (2008).

65. HENDRIK SCHULZE & KLAUS MOCHALSKI, IPOQUE INTERNET STUDY 2008/2009, at 2-3 (2009); Karl Schrader et al., *Tracking Contraband Files Transmitted Using BitTorrent*, *in* ADVANCES IN DIGITAL FORENSICS V 159 (Gilbert Peterson & Sujeet Shenoi eds., 2009).

66. SUSANNAH GARDNER & KRIS KRUG, BITTORRENT FOR DUMMIES 14-15 (2006).

67. Clive Thompson, *The BitTorrent Effect*, WIRED, Jan. 2005, at 37, *available at* http://www.wired.com/wired/archive/13.01/bittorrent.html.

68. Chao Zhang et al., *Unraveling the BitTorrent Ecosystem*, 22 IEE TRANSACTIONS ON PARALLEL & DISTRIBUTED SYS. 1164, 1166 (2011).

69. *Id.*

70. *Id.*

71. *See FAQ*, MININOVA, http://www.mininova.org/faq (last visited Mar. 18, 2013).

72. Zhang et al., *supra* note 68, at 1166.

73. *See* GARDNER & KRUG, *supra* note 66, at 183.

74. *See Frequently Asked Questions*, BITTORRENT, http://www.bittorrent.com/help/

collection of peers sharing a file is referred to as a swarm.[75] Each individual peer in the swarm simultaneously downloads ("leeches") and uploads ("seeds") the file and the tracker acts as a traffic cop, allowing leechers to download the pieces of the file they are missing from seeders that have already obtained that particular piece.[76] As pieces of the file are downloaded, they are made available to other members of the swarm. This "allows individual users to distribute data am[ong] themselves by exchanging pieces of the file with each other to eventually obtain a whole copy of the file."[77]

Some copyright holders and trade organizations have begun filing complaints against entire BitTorrent swarms.[78] These mass-BitTorrent suits, discussed *infra*, target defendants that have most likely used BitTorrent to commit copyright piracy. They attempt to cast too broad a net, however, by arguing for what amounts to strict liability for WAP operators. The rest of this Note discusses the various legal theories advanced to hold open WLAN operators liable for the Internet crimes committed by roaming users.

II. LIABILITY FOR OPERATING AN UNSECURED ACCESS POINT

One troubling aspect of the attempts being made to hold WLAN operators liable for the actions of roaming users are the tactics being used, particularly in the mass-BitTorrent cases. The approach taken by many plaintiffs has been called "speculative invoicing" by some critics, and the practice has resulted in ethics sanctions for lawyers in the United Kingdom employing similar techniques.[79] The scheme seeks to elicit settlements from huge numbers of Doe defendants by offering to settle for amounts much lower than potential attorney's

faq/concepts (last visited Mar. 18, 2013); GARDNER & KRUG, *supra* note 66, at 11.

75. *See* BITTORRENT, *supra* note 74; GARDNER & KRUG, *supra* note 66, at 19.

76. *See* GARDNER & KRUG, *supra* note 66, at 13, 18-19.

77. MCGIP, LLC v. Does 1-30, No. C11-06380 HRL, 2011 WL 3501720, at *2 (N.D. Cal. Aug. 10, 2011) (internal citations omitted).

78. *See* Ernesto, *Movie Studio Sues BitTorrent Swarm in Civil Conspiracy Suit*, TORRENTFREAK (Mar. 30, 2011), https://torrentfreak.com/movie-studio-sues-bittorrent-swarm-in-civil-conspiracy-suit-110330; *see, e.g.*, *Swarm of Nov. 16, 2010 Case*, *supra* note 24; Third Degree Films v. Does 1-3577, No. C 11–02768 LB, 2011 WL 5374569 (N.D. Cal. Nov. 4, 2011); MCGIP, LLC v. Does 1-30, No. C11-6380 HRL, 2011 WL 3501720 (N.D. Cal. Aug. 10, 2011); Liberty Media Holdings, LLC v. Colo. Members of Swarm of Nov. 19, 2010 to Dec. 11, 2011, Civil Action No. 11–cv–01170–WJM–KMT, 2011 WL 1812554 (D. Colo. May 12, 2011).

79. The Solicitors Regulatory Authority has sanctioned several lawyers who represented clients in mass-BitTorrent cases because their tactics caused significant distress for the defendants, many of whom were innocent, and because they "acted in a way that was likely to diminish the trust of the public places in him or in the legal profession." *See In re* Andrew Jonathan Crossley, [2012] No. 10726-2011, [1.3] *available at* http://www.solicitorstribunal.org.uk/Content/documents/10726.2011%20-%20Crossley.pdf.

fees and by offering anonymity to those who settle.[80] The settlement letters also indicate that open WLAN administrators are liable for any illicit actions committed on their Internet connections.[81]

Over 250,000 individuals have now been sued for digital copyright infringement committed using a BitTorrent client and that number continues to grow rapidly as more copyright holders attempt to recover lost income.[82] Because public trackers are open, the copyright holders are often able to use forensic software, such as International IPTracker v1.2.1, to obtain a list of the Internet Protocol ("IP") addresses associated with the BitTorrent swarm.[83] An IP address is a unique number assigned to every host device connected to the Internet[84] and can be used to identify which Internet connection was used for the infringement.

After obtaining the list of IP addresses, the plaintiffs typically file a claim in federal court and motion for early discovery in order to obtain the identity of the subscribers associated with the offending IP addresses.[85] Courts have been fairly liberal in granting discovery and allowing plaintiffs to subpoena Internet service providers ("ISP"). After receiving the subpoena, the ISP usually notifies the subscriber that their information was subpoenaed, and an offer of early settlement from the plaintiff typically arrives shortly afterwards.[86]

Many defendants are shocked by and unsure how to respond to the notification from their ISP and the letters from plaintiff's counsel.[87] Plaintiffs take advantage of this fact by offering advice and including question and answer sections in the initial settlement demand.[88] These question and answer sections, perhaps unsurprisingly, claim that the ISP subscriber is liable for any copyright infringement no matter who actually committed the act.[89]

The settlement demand letters inform the recipient that "copyright owners may recover up to $150,000 in statutory

80. *See* Hamilton, *supra* note 11; Kravets, *supra* note 17.

81. *See, e.g.*, John L. Steele Letter, *supra* note 12.

82. *See* Ernesto, *Hurt Locker BitTorrent Lawsuit Dies, But Not Without Controversy*, TORRENTFREAK (Dec. 22, 2011), http://torrentfreak.com/hurt-locker-bittorrent-lawsuit-dies-but-not-without-controversy-111222.

83. Lundberg, *supra* note 21.

84. *See* TIMOTHY ROONEY, IP ADDRESS MANAGEMENT PRINCIPLES AND PRACTICE 3-4 (2011).

85. *See* Lundberg, *supra* note 21; Plaintiff's Emergency Ex-Parte Motion for Early Discovery at 1-2, Liberty Media Holdings, LLC v. Swarm Sharing Hash File AE340D0560129AFEE8D78CE07F2394C7B 5BC9C05, No. 11-10802 (D. Mass. May 9, 2011), ECF No. 6, *available at* http://www.citmedialaw.org/threats/liberty-media-holdings-v-john-does#description.

86. Lundberg, *supra* note 21.

87. *Id.*

88. *See, e.g.*, John L. Steele Letter, *supra* note 12, at 4-5.

89. *Id.*

damages . . . per infringing file plus attorney's fees."[90] Many of the letters also reference a case in which a defendant accused of illegally sharing a Liberty Media adult film through BitTorrent agreed to pay a $250,000 settlement.[91] The purpose of these statements is to scare defendants by threatening potential liability for hundreds of thousands of dollars. By comparison, the $1,000 to $3,000 settlement demanded in the letter seems reasonable. Indeed, many innocent defendants with open WLAN may choose to play it safe and settle to make the problem go away.

The typical settlement agreement also includes language stating that "[i]n some cases the settlement offered by us is significantly lower than the costs associated with hiring an attorney."[92] The letters also state that settlement is the best option compared with the cost of attorney's fees.[93] The letters, particularly in cases involving pornography, also stress that a quick settlement will allow the ISP account holder to remain anonymous.[94]

The initial settlement offer is very effective at reaching settlements with the unnamed Does, even among Does who appear likely to win at trial. For example, Imperial Enterprises sued 3545 Does, among them was Doe 2057, a legally blind man who was incapable of viewing the adult film he was accused of pirating.[95] Doe 2057's wife set up the family's wireless router without a password, and the couple assumed that because they "lived in a very upscale building . . . [with] no riffraff . . . . [they] didn't have anything to worry about."[96] Their children, who are four and six years old, were obviously not likely suspects. Only in hindsight did Doe 2507 realize that his neighbors downloading movies over his unsecured connection probably caused the slow Internet connection he complained about to Comcast.[97] Even though Doe 2507 remains adamant that he did not pirate the film, he stated in an interview that he was concerned about what the accusation would do to his career and that "[a]t the end of the day, [he will] probably settle and pay the fee to make [the lawsuit] go away."[98]

In very few of these mass-BitTorrent cases have individual defendants been held liable for anything approaching the intimidating figures laid out in the settlement letters. The often referenced $250,000 settlement figure has come under scrutiny

90. *Id.* at 2.
91. *Id.*
92. *Id.* at 5.
93. *Id.*
94. *Id.* at 4.
95. Hamilton, *supra* note 11.
96. *Id.*
97. *Id.*
98. *Id.*

recently, with some commentators speculating that the actual amount paid by the defendant was significantly less.[99] Even default judgments have not approached the maximum statutory damages. In fact, a recent default judgment was entered against two defendants for only $750 plus interest.[100]

The lawsuits are not intended to lead to trials. Instead, they are intended to collect small settlements from hundreds or thousands of defendants. Prenda Law, a firm that specializes in mass-BitTorrent cases, stated in a declaration to the court that out of 118 mass-BitTorrent cases it previously filed, it has not actually served process on a single defendant.[101] Conducting depositions and electronic forensic discovery of thousands of defendants and their computer hard drives would be incredibly expensive, and many of these firms appear to lack the resources needed to take the cases beyond the filing and motion for emergency discovery. The plaintiffs simply dismiss the claim once it becomes clear that the defendant is in the litigation for the long run, sometimes after media attention highlights the plight of an implausible defendant.[102]

Some firms do serve defendants, however, and they have been actively seeking to establish precedent under several theories holding open WLAN administrators liable for all Internet traffic that takes

---

99. The settlement agreement included a "good behavior" clause that allowed the defendant to reduce the amount owed by "mak[ing] regular payments toward the judgment on a schedule which will be agreed upon between the parties in a separate settlement agreement." Enigmax, *Biggest Ever BitTorrent Piracy Settlement Is Intriguing*, TORRENTFREAK (Jan. 7, 2011), http://torrentfreak.com/biggest-ever-bittorrent-piracy-settlement-is-intriguing-110107. The settlement agreement was signed just four days after service of process and appears to have been structured in such a way that allowed for a huge figure to be publicized without going through the expense of a trial. *See id.*

Liberty Media then publicized the settlement as the largest ever BitTorrent settlement and announced that it would soon launch a large round of lawsuits. Rhett Pardon, *Corbin Fisher Offers $1K Amnesty to BitTorrent Users*, XBIZ NEWSWIRE (Jan. 25, 2011 6:00 PM), http://newswire.xbiz.com/view.php?id=129918. Liberty also implemented a surprisingly successful amnesty program, offering anyone who had previously pirated its products amnesty and a year's subscription to the company's web content in exchange for a $1,000 payment. *Id.* At least ten people took advantage of the program. Enigmax, *File-Sharers Start Handing Over $1,000 Each in Bizare Amnesty Program*, TORRENTFREAK (Feb. 17, 2011), http://torrentfreak.com/file-sharers-start-handing-over-1000-each-in-bizarre-amnesty-program-110217.

100. Default Judgment at 1-2, K-Beech, Inc. v. Hernandez, No. CV 11-01604-PHX-NVW (D. Ariz. Feb. 10, 2012), ECF No. 46. The defendants were also ordered to destroy any copies of the motion picture obtained illegally and were enjoined from committing further direct, contributory, or indirect copyright infringement. *Id.*

101. Brief for Electronic Frontier Foundation, et al. as Amici Curiae Supporting Defendants, AF Holdings, LLC v. Does 1-1058, Case No. 1:12-cv-00048 (BAH), at 2 (D.D.C. Mar. 13, 2012), *available at* https://www.eff.org/sites/default/files/filenode/12cv00048BAH.Amici_.Brief_.pdf.

102. Lundberg, *supra* note 21.

place under the owner's registered IP address.

A. Liability Under a Theory of Negligence for Copyright Infringement

The lawyers seeking to hold wireless network operators liable under a theory of negligence often analogize failing to password protect a wireless router with "leav[ing] a loaded gun within reach of a 3-year old,"[103] or with leaving keys in an unlocked car where a thief could easily steal it.[104] These analogies serve a rhetorical purpose but their value as legal precedent applicable to open WLAN operator liability is doubtful.

While leaving a loaded firearm accessible to a child creates a prima facie case for negligence in many states,[105] liability is based on the "failure to exercise the required degree of care in regard to a dangerous instrumentality."[106] It hardly seems reasonable to claim that a wireless network is a dangerous instrumentality akin to a loaded firearm. Even proponents of liability for unsecured wireless network operators have characterized this analogy as "overly melodramatic and hysterical."[107] The comparison with leaving keys in an automobile is more intriguing, but not wholly applicable or supportive of liability.

Only a minority of states hold a vehicle owner who leaves the key in the ignition liable for damage caused by a third party who steals the car.[108] There is also a consensus among most jurisdictions that a vehicle owner is not liable for intentional torts committed by the third-party thief.[109] While the classification may not be a perfect fit, direct copyright infringement has been classified as an "intentional tort."[110]

Most jurisdictions find no liability either because the vehicle

---

103. Temple, *supra* note 11.

104. Randazza, *supra* note 28.

105. The case law is inconsistent even within jurisdictions but a majority of states appear to find negligence in this type of situation. *See* L.S. Rogers, Annotation, *Liability of Person Permitting Child to Have Gun, or Leaving Gun Accessible to Child, for Injury Inflicted by the Latter*, 68 A.L.R. 2D 782 (1959).

106. *Id.*; *see also* RESTATEMENT (SECOND) OF TORTS § 308 (1965) ("It is negligence to permit a third person to use a thing . . . which is under the control of the actor, if the actor knows or should know that such person . . . is likely to use the thing . . . in such a manner as to create an unreasonable risk of harm to others.").

107. Randazza, *supra* note 28.

108. David L. Reed, Annotation, *Liability of Motorist Who Left Keys in Vehicle for Injury Caused by Thief Operating Stolen Vehicle*, 13 AM. JUR. PROOF OF FACTS 3D 405, § 1 (2012).

109. *Id.* § 1 n.8; *see, e.g.*, Burns v. Gleason Plant Sec., Inc., 523 A.2d 940, 943 (Conn. App. Ct. 1987) (holding plaintiff leaving keys in ignition was not the proximate cause of assault committed during an armed robbery in which the stolen car was used).

110. Bucklew v. Hawkins, Ash, Baptie & Co., 329 F.3d 923, 931 (7th Cir. 2003).

owner owes no duty to the injured party,[111] or because the action of leaving the keys in the car is not the proximate cause of the subsequent harm. In the few cases that have found the vehicle owner liable, factors like the car being parked in a "high-crime" area,[112] or the inherent danger in operating a motor vehicle have been cited.[113] The traditional notion of a high-crime area is not applicable to wirelessly committed Internet crimes. Areas with higher rates of violence or drug-related crimes are not likely to correlate with the areas with the highest concentration of Internet crimes. Moreover, like the loaded firearm analogy, the likelihood of physical injury resulting from the misuse of a wireless network is virtually nonexistent.

The operation of an unsecured wireless router is not easily analogized to any pre-existing area of the law. Like any new revolutionary technology, previous law may help to establish the legal framework, but a thorough analysis of the issue will be required to reach any meaningful conclusion.

B. Federal Preemption of Negligence Under Copyright Law

The argument made in support of negligence as a theory of liability for indirect copyright infringement is that "[r]easonable Internet users take steps to secure their Internet access accounts to prevent the use of such accounts for nefarious and illegal purposes."[114] Therefore, operating an unsecured wireless router "constitutes a breach of the ordinary care that reasonable persons exercise in using an Internet access account."[115]

On its face, this theory of liability sounds plausible and is likely intimidating to defendants accused of negligence. A prominent copyright settlement "portal"—a website used by plaintiffs to collect settlements—states in its FAQ section that even if defendants are unfamiliar with the copyrighted content they are accused of pirating, as the "account holder [they are]/or may be legally responsible for infringement(s) and settlement(s) [fees]."[116] This is so even if the

111. Reed, *supra* note 108, § 11.

112. State Farm Mut. Auto. Ins. Co. v. Grain Belt Breweries, Inc., 245 N.W.2d 186, 189-90 (Minn. 1976) (holding that jury could find proximate causation when employee left beer truck in area with high crime rate).

113. Hergenrether v. East, 393 P.2d 164, 167 (Cal. 1964) ("[T]he vehicle was a partially loaded two-ton truck . . . which was capable of inflicting more serious injury and damage than an ordinary vehicle . . . .").

114. Swarm of Nov. 16, 2010 Complaint, *supra* note 14, ¶ 376; Complaint ¶ 319, 808 Holdings, LLC v. Collective of Dec. 29, 2011, Sharing Hash E37917C8EEB4585E6421358FF32F29CD63 C23C91, No. 12CV0186 MMA RBB, 2012 WL 314117 (S.D. Cal. Jan. 23, 2012).

115. Swarm of Nov. 16, 2010 Complaint, *supra* note 14, ¶ 376.

116. *Peer-to-Peer Infringement FAQ*, COPYRIGHT SETTLEMENTS, http://www.copyrightsettlements.com/faq.html (follow "Peer to Peer Unauthorized Use" hyperlink)

infringement "[was] . . . [committed by] a spouse, child, roommate, employee, . . . business associate," or an unknown party over an "unsecured wireless network."[117]

Negligence, however, is not a viable theory of liability in copyright infringement cases because of the federal preemption doctrine.[118] Federal preemption can occur in three situations.[119] Preemption occurs when Congress explicitly preempts state law, and when a federal scheme of regulation occupies the field, preempting state law in that field.[120] Preemption may also occur "when compliance with both state and federal [laws] is a physical impossibility or when state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[121] Both the Digital Millennium Copyright Act ("DMCA")[122] and the Communications Decency Act ("CDA")[123] limit the extent to which state common law theories of liability can apply to the operators of an unsecured wireless network.[124]

1. Preemption Under the Copyright Act of 1976 and the Digital Millennium Copyright Act

Negligence, as a state law tort claim, is preempted by the DMCA.[125] Congress passed and presented the DMCA to President Clinton on October 21, 1998,[126] with the intention of adjusting the Copyright Act of 1976[127] for "the new realities of Internet technology and commerce by providing for technological protection measures, electronic rights management and safe harbors for online service providers."[128] Congress and the international community—through

(last visited Mar. 18, 2013).

117. *Id.*

118. *See* Elizabeth Helmer, Comment, *The Ever-Expanding Complete Preemption Doctrine and the Copyright Act: Is This What Congress Really Wanted?*, 7 N.C. J.L. & TECH 205, 217 (2005).

119. G.S. Rasmussen & Assocs., Inc. v. Kalitta Flying Serv., Inc., 958 F.2d 896, 903 (9th Cir. 1992).

120. *Id.*

121. Online Policy Grp. v. Diebold, Inc., 337 F. Supp. 2d 1195, 1205 (N.D. Cal. 2004) (quoting Hillsborough Cnty. v. Automated Med. Labs., Inc., 471 U.S. 707, 713 (1985)).

122. Digital Millennium Copyright Act (DMCA) of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (codified in scattered sections of 17 U.S.C.).

123. Communications Decency Act (CDA) of 1996, 47 U.S.C. §§ 230, 560-61 (2006), *invalidated in part by* Reno v. ACLU, 521 U.S. 844 (1997).

124. *See* McSherry, *supra* note 28.

125. *See Online Policy Grp.*, 337 F. Supp. 2d at 1205 (holding state claim for tortious interference preempted by DMCA).

126. 144 CONG. REC. 27,409 (1998).

127. 17 U.S.C. §§ 101-805, 1101 (2006).

128. PAUL GOLDSTEIN & R. ANTHONY REESE, COPYRIGHT, PATENT, TRADEMARK AND RELATED STATE DOCTRINES: CASES AND MATERIALS ON THE LAW OF INTELLECTUAL

the implementation of the World Intellectual Property Organization Copyright Treaty ("WIPO")[129]—recognized in the mid-1990s that the technological innovations associated with the Internet held tremendous promise for commerce and "distribution of copyright[able] works," but also had the potential to facilitate piracy.[130] Seeking a balance between the interests of the copyright industry, users, and service providers, Congress enacted the DMCA "both to preserve copyright enforcement . . . and to provide immunity to service providers from copyright infringement liability for passive, automatic actions in which a service provider's system engages through a technological process initiated by another without the knowledge of the service provider."[131]

The 1976 Copyright Act makes it clear that:

> "[A]ll legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright . . . and come within the subject matter of copyright . . . whether created before or after that date, and whether unpublished, are governed exclusively by this title . . . . [N]o person is entitled to any such right or equivalent right in any work under the common law or statutes of any state."[132]

A state common law claim is preempted by the federal copyright law if "(1) the work at issue comes within the subject matter of copyright; and (2) the state law rights are 'equivalent to rights within the general scope of copyright.'"[133] This standard of copyright preemption is broad.[134] In the case of unsecured WLAN operators accused of negligence resulting in copyright infringement, there is little doubt that the motion pictures at issue (or any other digital media) fall squarely within the general scope of copyright protection.[135] This conclusion is bolstered by the inclusion of other, more traditional

---

PROPERTY 680 (7th ed. 2012).

129. WIPO Copyright Treaty, Dec. 20, 1996, S. TREATY DOC. No. 105-17 (1997), 36 I.L.M. 65 (1997).

130. Presidential Statement on Signing the Digital Millennium Copyright Act, 2 PUB. PAPERS 1902 (Oct. 28, 1998).

131. Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1086 (C.D. Cal. 2004) (internal quotation marks omitted), *aff'd in part, rev'd in part*, 481 F.3d 751 (9th Cir. 2007).

132. Dielsi v. Falk, 916 F. Supp. 985, 990 (C.D. Cal. 1996) (quoting 17 U.S.C. § 301(a) (2006)).

133. *Id.* at 991 (quoting Del Madera Properties v. Rhodes & Gardner, Inc., 820 F.2d 973, 977 (9th Cir. 1987).

134. *Id.* at 990.

135. Section 102 of the Copyright Act of 1976 delineates the scope of copyright protection. 17 U.S.C. § 102 (2006). Section 102 provides a nonexclusive list of works that are considered works of authorship. This list includes in relevant part: literary works, musical works, pictorial and graphic works, "motion pictures and other audiovisual works," and sound recordings—all of which could potentially be subjects of digital copyright piracy. *Id.* § 102(a)(1), (2), (5)-(7).

copyright infringement claims in the complaints.[136]

Under the second prong of the test, a state law claim is preempted if "the rights protected by state law are equivalent to those protected by the Copyright Act."[137] Although some courts considering the issue have stated that if a state law claim has an extra element it is not preempted, a consensus seems to have formed around the view that "a fact-specific inquiry into the actual allegations" is required, not just a "laundry list" comparison between claims.[138] The true test is whether the state law claim seeks to protect a right that is "more or less equivalent to those exclusively protected by copyright."[139]

State civil claims for unauthorized copying of computer programs are preempted.[140] Claims for civil conspiracy to commit copyright infringement have also been held to be preempted in many jurisdictions.[141] In cases where negligent administration of a wireless network is alleged, the negligence claim is seeking to vindicate the underlying copyright infringement claim and is therefore preempted.

Although no court has addressed the issue of negligence concerning wireless technology and digital media specifically, several courts have analyzed negligence claims in traditional copyright infringement disputes. For example, in *Dielsi v. Falk*, the court held that the defendant screenwriter's claim of negligence was "merely [a] recharacterizat[ion of] a copyright infringement claim as one for negligence," and was preempted by federal law.[142]

"Copyright preemption is both explicit and broad . . . ."[143] When federal law "so thoroughly occupies a legislative field," it can be reasonable to assume by inference that Congress intended to

---

136. *See, e.g.*, *Perfect 10, Inc.*, 340 F. Supp. 2d at 1085 (bringing claims against defendants under DMCA and federal copyright infringement); *see also* cases cited *supra* note 14 (same).

137. Idema v. Dreamworks, Inc., 162 F. Supp. 2d 1129, 1190 (C.D. Cal. 2001), *aff'd in part*, *dismissed in part*, 90 F. App'x. 496 (9th Cir. 2003) (internal quotation marks omitted).

138. *Id.* at 1190; Entous v. Viacom Int'l, Inc., 151 F. Supp. 2d 1150, 1159-60 (C.D. Cal. 2001); Groubert v. Spyglass Entm't Grp., LP, No. CV 02-01803-SVM (JTLx), 2002 WL 2031271, at *2 (C.D. Cal. July 22, 2002).

139. *Idema*, 162 F. Supp. 2d at 1190 (internal quotation marks omitted).

140. *See* Madison River Mgmt. Co. v. Bus. Mgmt. Software Corp., 351 F. Supp. 2d 436, 445 (M.D.N.C. 2005).

141. Joseph P. Bauer, *Addressing the Incoherency of the Preemption Provision of the Copyright Act of 1976*, 10 VAND. J. ENT. & TECH. L. 1, 87-88 (2007) (citing *e.g.*, Irwin v. ZDF Enters. GMBH, No. 04 CIV. 8027 (RWS), 2006 WL 374960, at *4 (S.D.N.Y. Feb. 16, 2006); Brown v. McCormick, 23 F. Supp. 2d 594, 608 (D. Md. 1998)).

142. Dielsi v. Falk, 916 F. Supp. 985, 992-93 (C.D. Cal. 1996).

143. G.S. Rasmussen & Assocs., Inc. v. Kalitta Flying Serv., Inc., 958 F.2d 896, 904 (9th Cir. 1992).

preempt state law claims.[144] If a plaintiff is seeking to hold the owner of an open network liable for third-party infringement, it must do so within the existing recognized framework of federal copyright law. Plaintiffs should not be permitted to use a state law claim of negligence as an end run around federal preemption.

2. Potential Liability Under Existing Copyright Doctrine

As the law currently stands, there are only three potential types of third-party liability for copyright infringement.[145] The Copyright Act does not expressly provide for indirect liability in copyright infringement cases; however, the Supreme Court has recognized contributory, vicarious, and intentional inducement as viable theories of liability.[146] These three doctrines emerged from deeply rooted common law copyright principles and remain the exclusive means of holding indirect infringers liable. As the EFF has noted, "there is no negligence theory of copyright liability."[147] It should also be noted that to date, no mass-BitTorrent plaintiff has alleged any of the established theories of third-party liability against a WLAN operator.

Contributory infringement requires that the noninfringing party (1) must know or have reason to know of the direct infringement, and (2) must (a) materially contribute to or (b) actively induce the direct infringer's conduct.[148] The level of knowledge and the level of direct assistance required to trigger contributory liability has been subject to some debate over time but a clear consensus has developed among most jurisdictions requiring a "relatively specific [level of] knowledge and direct assistance."[149]

It is clear that something more than the mere chance that infringing conduct may occur must be known to the noninfringing party. In *Sony Corp. of America v. Universal City Studios, Inc.*, the Supreme Court ruled that mere constructive knowledge by a manufacturer that its videotape recorders could be used to commit

144. *See* Orson, Inc. v. Miramax Film Corp., 189 F.3d 377, 381 (3d Cir. 1999) (quoting Ciapollone v. Ligget Grp., Inc., 505 U.S. 504, 516 (1992)).

145. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 929-41 (2005) (discussing contributory, vicarious, and intentional inducement theories of liability).

146. Contributory infringement and vicarious infringement have long been recognized and were explicitly recognized by the Supreme Court in 1984. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 434-35 (1984). Intentional inducement is a more recent theory of liability and was recognized by the Court in 2005. *See Grokster*, 545 U.S. at 936.

147. McSherry, *supra* note 28.

148. *Grokster*, 545 U.S. at 930; Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 795 (9th Cir. 2007).

149. Alfred C. Yen, *Third-Party Copyright Liability After* Grokster, 91 MINN. L. REV. 184, 195 (2006) (citing *Sony Corp.*, 464 U.S. at 439).

copyright infringement was not enough to satisfy the knowledge prong.[150] Because Sony's videotape recorders could be used for substantial noninfringing use, the Court refused to construe Sony's knowledge as adequate to establish liability.[151] Similarly, credit card processors and financial institutions providing financial services to infringing websites were found not to have sufficient knowledge of infringement to be held liable.[152] In the online context, only when the service provider has received express notice of infringement taking place on its system and failed to take action to remedy the situation has actual knowledge been imputed.[153] The Ninth Circuit embraced this interpretation in *Perfect 10, Inc. v. Amazon.com, Inc.*, stating that "a computer system operator can be held contributorily liable if it 'has *actual* knowledge that *specific* infringing material is available using its system,' . . . and can 'take simple measures to prevent further damage' to copyrighted works, . . . yet continues to provide access to infringing works."[154]

The proprietor of an unsecured wireless network has no knowledge of a roaming user's infringing behavior. Just as in *Sony* and *A & M Records, Inc. v. Napster, Inc.*, the technology used in a wireless network could conceivably be used to commit copyright infringement but is also capable of substantial noninfringing use. Even if an open WLAN operator knew that a roaming user could use its network for infringing purposes, it would be very difficult to establish the level of knowledge required for liability. Even when symptoms like dramatically slower connection speeds appear—like in the case of Doe 2057 discussed *supra*—a culpable level of knowledge is not established. Doe 2057 complained to his ISP about the slow speeds, indicating that he did not know infringing conduct was occurring.[155]

The inducement subpart of the second prong is also not satisfied by the operation of an unsecured WLAN, and to date, no plaintiff has even alleged that it does. Absent some extenuating circumstance—e.g., the network's SSID name is something like "copyright pirates welcome"—the act of simply maintaining an unsecured network does not actively induce roaming users to infringe copyrights. The standard for evaluating material contribution, however, is incoherent.[156] Jurisdictions vary from case to case on how to

150. *Sony Corp.*, 464 U.S. at 439.

151. *Id.* at 442.

152. Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, No. C 04-00371 JW, 2004 WL 3217732, at *3-4 (N.D. Cal. Dec. 3, 2004), *aff'd*, 494 F.3d 788 (9th Cir. 2007).

153. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1021-22 (9th Cir. 2001).

154. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1172 (9th Cir. 2007).

155. *See supra* Part II.

156. *See* Mark Bartholomew & Patrick F. McArdle, *Causing Infringement*, 64 VAND. L. REV. 675, 689-90 (2011).

approach the analysis and often reach contradictory results.[157]

There are currently two competing approaches in use across the United States.[158] Some courts focus on "the relationship between [the] defendant and [the] direct infringer" while others focus on" the relationship between [the] defendant and the act of infringement."[159] The relationship between the parties approach requires that the noninfringer exercise some level of control over the direct infringer.[160] The second approach requires that the infringing act is not too attenuated from the noninfringer's actions.[161] The murkiness in this area of the law makes it exceedingly difficult to predict what the outcome of this analysis would be and any attempt to do so would be beyond the scope of this Note.[162] It is, however, possible to conclude that pursuing a claim of contributory infringement against a WLAN operator would be very difficult, and most likely futile, because of the DMCA's safe harbor provisions discussed below.[163]

The second form of indirect liability under copyright law is vicarious liability.[164] Vicarious infringement liability is found "[w]hen the right and ability to supervise [the direct infringer] coalesce with an obvious and direct financial interest in the exploitation of copyrighted materials."[165] Although the doctrine does not require an employment relationship, it is derived from the concept of respondeat superior and requires a significant level of control by the noninfringer. Unsecured WLAN administrators do not have the ability to control roaming users' conduct, and have no financial interest in any of the online activities of roaming users, let alone direct copyright infringement.

The third possibility, inducement, extends liability based on a

---

157. *See id* at 690 (noting that the Ninth Circuit reasoned that facilitating access was enough to satisfy the material contribution element in *Perfect 10, Inc. v. Amazon.com*, 508 F.3d 1146 (9th Cir. 2007) but ruled two weeks later in *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n*, 494 F.3d 788 (9th Cir. 2007) that it was not); *see also* Matthew Bender & Co. v. West Publ'g Co., 158 F.3d 693, 706-07 (2d Cir. 1998).

158. Bartholomew & McArdle, *supra* note 156, at 687.

159. *Id.* at 691.

160. *Id.* (citing Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 437 (1984)).

161. *Id.* at 691-92.

162. For a detailed analysis of the state of the material contribution element and suggestions on how to clarify and rescue the doctrine of contributory liability, see *id. See also* Lital Helman, *Pull Too Hard and the Rope May Break: On the Secondary Liability of Technology Providers for Copyright Infringement,* 19 TEX. INTELL. PROP. L.J. 111, 131-32 (2010) (discussing the open-ended and unpredictable nature of the secondary liability standard because congressional acts were disharmonious with case law).

163. *See infra* Part II.B.iii.

164. Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 929-41 (2005).

165. Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963).

purposeful, culpable expression and conduct intended to commit copyright infringement.[166] The intentional inducement theory was used by the Supreme Court in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.* to hold the maker and distributor of peer-to-peer file sharing software liable for the infringing acts of the software's users even though Grokster had no control of the users or the content.[167] The Court stated that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[168]

As noted above, there is no reason to believe that a court would hold that operating an unsecured wireless network actively induces roaming users to commit copyright infringement. Unlike *Grokster*, wireless technology is not promoted as a way to infringe copyrights.

3. The Digital Millennium Copyright Act's Safe Harbor Provisions

Title II of the DMCA incorporates the Online Copyright Infringement Liability Limitation Act ("OCILLA") and provides immunity from secondary liability for qualifying ISPs and Online Service Providers ("OSP"). The DMCA's four safe harbor provisions protect qualifying ISPs from liability "when those ISPs act merely as passive networks or provide unknowing assistance to copyright infringers."[169] The first safe harbor provision, § 512(a), is applicable to operators of unsecured wireless networks and states that:

> A service provider shall not be liable for monetary relief, . . . injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of . . . providing connections . . . .[170]

No liability attaches to the service provider as long as: (1) the transmission was not initiated by the service provider; "(2) the transmission, routing, provision of connections, or storage [was] carried out . . . automatic[ally] . . . without selection of the material by the service provider; (3) the service provider does not select the recipients of the material"; (4) a copy of the material is not stored on the system; and "(5) the material is transmitted through the system

166. *Grokster*, 545 U.S. at 929-38.

167. *Id.* at 936-41.

168. *Id.* at 936-37.

169. Lori E. Lesser, *Current Copyright Internet Litigation Issues*, 932 PLI/PAT 349, 359 (2008).

170. Online Copyright Infringement Liability Limitation Act, 17 U.S.C. § 512(a) (2006).

or network without modification of its content."[171]

A service provider is "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[172] America Online ("AOL") was found to be immune against a claim of vicarious copyright infringement under § 512(a) in *Ellison v. Robertson*, a California case in which a science fiction author sued AOL because it offered access to the USENET group used to host the infringing content.[173] The Ninth Circuit agreed with the district court's determination that "AOL functioned as a conduit service provider" and was eligible for protection under the OCILLA safe harbor provisions.[174] Similarly in *Interscope Records v. Does 1-7*, the court held that the College of William and Mary fell within § 512(a)'s safe harbor provision because "the College simply acted as a conduit by providing the Doe defendants with access to the [I]nternet."[175]

An unsecured wireless network acts as a conduit, allowing anyone with a wireless device to access the Internet.[176] Any infringing material downloaded or uploaded over the connection by a roaming user is done without the knowledge or intervention of the WLAN's operator. There is no reason that the courts should not extend the safe harbor's protection to these defendants when they are essentially acting as micro telecommunication companies by offering Internet access to roaming users. The operator of an unsecured wireless router is an Internet service provider as defined under the DMCA and is therefore shielded from liability.

C. Liability Under General Tort Theory of Negligence for Common Law Torts

Even though the common law negligence cause of action is not available in copyright infringement suits, there are hosts of cybertorts that are actionable under state law that should be discussed. Cybertorts are typically divided into two categories, torts against personal interests–such as defamation or intentional infliction of emotional distress—and torts committed against a personal property interest—such as trespass to chattels, conversion, and misappropriation of trade secrets.[177] The cybertorts committed

171. *Id.* § 512(a)(1)-(5).
172. *Id.* § 512(k)(1)(A).
173. Ellison v. Robertson, 357 F.3d 1072, 1074, 1080-81 (9th Cir. 2004).
174. *Id.*
175. Interscope Records v. Does 1-7, 494 F. Supp. 2d 388, 390 (E.D. Va. 2007).
176. *See supra* Part I.B.
177. MOORE, *supra* note 58, at 6.

against personal property have largely been recognized as actionable by most jurisdictions.[178]

Assuming that negligence is available as a cause of action against the administrator of an open WLAN connection based on the acts of a third party, the existence of a duty is the most contentious part of the theory of liability. As of this writing no court has ever ruled that a duty to secure wireless networks exists.

The plaintiff's lawyer in *Liberty Media Holdings, LLC v. Swarm of Nov. 16, 2010* argues that *The T.J. Hooper*[179] makes the case for the existence of a duty to password protect a wireless router.[180] The proposition from *The T.J. Hooper*—that new technology that would be used by the reasonable person should be used by all[181]—has been used to argue for the existence of a duty. Alternatively, the existence of a duty to secure a wireless router is couched in the Hand formula analysis.[182] It could be argued that because the burden of securing the router is very low compared to the potential harm (digital piracy, child pornography, identity theft, harassment), the reasonable person would secure his or her wireless router.

The reasonable person, however, would not necessarily secure his or her router. There are many reasons to leave a router unsecured.[183] These reasons range from convenience to ideological beliefs about freedom of information. It has long been held that "[w]hile mere inconvenience or cost are often insufficient in themselves to justify proceeding in the face of danger, they will justify taking some risks which are not too extreme."[184] The risk of a third party discovering and then using the unsecured connection for nefarious purposes is not extreme and is sufficiently remote.

1. Preemption of Common Law Torts Under the Communications Decency Act

Assuming, arguendo, that a cause of action for negligence could be established against the operator of an unsecured wireless network, the CDA[185] would still shield the operator from liability

178. *Id.*

179. The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932).

180. Randazza, *supra* note 28.

181. *The T.J. Hooper*, 60 F.2d at 740 ("Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.").

182. United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

183. *See supra* Part I.B.

184. W. PAGE KEETON ET AL., PROSSER AND KEETON ON TORTS § 31, at 172 (5th ed. 1984).

185. Communications Decency Act (CDA) of 1996, 47 U.S.C. § 230 (2006), *invalidated in part by* Reno v. ACLU, 521 U.S. 844 (1997).

against common law tort claims.[186] The CDA "offers broad immunity from tort claims (including negligence) to providers of 'interactive computer services' for claims arising from the activities of their users."[187]

Congress enacted the CDA in 1996 with the principal goal of limiting the exposure of minors to indecent materials.[188] Parts of the CDA designed to further this goal have been cut back and struck down by the Supreme Court as unconstitutional limits on free speech.[189] Congress, however, had a secondary policy goal in mind when it enacted the CDA—"to promote the continued development of the Internet and other interactive computer services and other interactive media,"[190] and "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."[191]

To implement these policy goals, Congress provided that "[n]o provider . . . of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[192] The CDA does not provide immunity for criminal liability or any laws pertaining to intellectual property.[193] The CDA also makes clear that state law claims cannot be used to circumvent the immunity provided for under § 230.[194] "Courts have construed the ISP . . . immunity broadly, in the spirit of the CDA's stated purpose of promoting rather than impeding technology and Internet use."[195] It is my contention that the definitions provided under the CDA, the nature of cybertort, and subsequent judicial construction combine to broaden the exception's scope enough to shield unsecured WLAN operators from liability for the acts of roaming users.

In order to determine whether immunity under the CDA applies,

---

186. *See* McSherry, *supra* note 28.

187. *Id.*

188. Batzel v. Smith, 333 F.3d 1018, 1026 (9th Cir. 2003) (citing H.R. REP. NO. 104-458, at 81-91 (1996); S. REP. NO. 104-230, at 187-193 (1996); S. REP. NO. 104-23, at 9 (1995)).

189. *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 867-68 (1997) (invalidating § 223); United States v. Playboy Entm't Grp., Inc., 529 U.S. 803, 827 (2000) (invalidating § 505).

190. 47 U.S.C. § 230(b)(1) (2006).

191. *Id.* § 230(b)(2).

192. *Id.* § 230(c)(1).

193. *Id.* § 230(e)(1)-(2).

194. *Id.* § 230(e)(3).

195. Smith v. Intercosmos Media Grp., Inc., No. 02-1964, 2002 WL 31844907, at *3 (E.D. La. Dec. 17, 2002) (quoting Sewali K. Patel, *Immunizing Internet Service Providers from Third Party Internet Defamation Claims: How Far Should Courts Go?*, 55 VAND. L. REV. 647, 661 (2002)).

courts undertake a three part inquiry.[196] First, the court must determine whether the defendant meets the definition of an interactive computer service.[197] Next, the court must decide if the case involves information provided by an information content provider.[198] Finally, the court must determine if the plaintiff's claims "seek to treat Defendant as a publisher or speaker of third party content."[199]

Under the CDA, an interactive computer service is "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet."[200] Entities that provide access to the Internet have been routinely held to fall within the definition of interactive computer service. For example, AOL was held to be an interactive computer service provider that provides access to the Internet.[201] Likewise, an ISP who also provided website hosting,[202] and corporate employers providing access to the Internet have been deemed to be interactive computer service providers.[203] There seems to be little doubt that the administrator of an unsecured WLAN is enabling access by multiple users to a computer server—specifically the Internet. Roaming users take advantage of the open connection, use the equipment provided by the WAP owner, and connect to the Internet through the WAP owner's Internet connection.

An information content provider is "any person . . . responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[204] The nature of Internet crime is important for the application of this definition to § 230's grant of immunity. Almost without exception the Internet crimes committed by a malicious roaming user involve the "creation or development of information" that is then transmitted (provided) through the Internet. In *Green v. America Online (AOL)*, for example, the Third Circuit ruled that a

196. Gibson v. Craigslist, Inc., No. 08 Civ. 7735 (RMB), 2009 WL 1704355, at *3 (S.D.N.Y. June 15, 2009) (internal citations omitted).

197. *Id.*

198. *Id.*

199. Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 564 F. Supp. 2d 544, 548 (E.D. Va. 2008) (citing Schneider v. Amazon.com, 31 P.3d 37, 40 (Wash. Ct. App. 2001)), *aff'd*, 591 F.3d 250 (4th Cir. 2009).

200. 47 U.S.C. § 230(f)(2) (2006).

201. Noah v. AOL Time Warner, Inc., 261 F. Supp. 2d 532, 538 (E.D. Va. 2003), *aff'd sub nom*. Noah v. AOL-Time Warner, Inc., No. 03-1770, 2004 WL 602711 (4th Cir. Mar. 24, 2004).

202. Smith v. Intercosmos Media Grp., Inc., No. Civ.A. 02-1964, 2002 WL 31844907, at *3 (E.D. La. Dec. 17, 2002).

203. Delfino v. Agilent Tech., Inc., 52 Cal. Rptr. 3d 376, 389-90 (Cal. Ct. App. 2006).

204. 47 U.S.C. § 230(f)(3) (2006).

computer virus constituted "information" when sent from one user to another and granted AOL (the ISP) immunity from tort liability under a theory of negligence.[205]

Courts have broadly interpreted the term "publisher or speaker" used in § 230(c)'s grant of immunity to shield interactive computer service providers from liability in a hugely varied number of situations—particularly in situations where service providers have been accused of negligence. Craigslist was found to be immune from an allegation of negligence by a gunshot victim for negligently failing to police advertisements because the allegation improperly attempted hold it liable as the publisher of third party content.[206] Similarly, a claim against a social networking site for negligent failure to implement safety measures to protect underage users from sexual assault was found to be an attempt to hold the defendant liable as a publisher.[207]

Attempting to hold unsecured WLAN operators liable for negligent failure to secure their networks is barred by the CDA.[208] Any information provided by a roaming user, rather used to defame, steal an identity, harass, spam, or spread computer viruses, is not published by the WLAN operator. The actual tortfeasor is publishing the information through the WLAN operators computer service. Although no court has addressed the issue of open WLAN operator liability for information provided by a roaming user, the case law makes it clear that no liability should attach to the WLAN operator in his capacity as an interactive computer service provider.

III. CONCLUSION

There are two critical public policy question underlying the possibility of liability for unsecured WLAN network operators. The first, do we want to encourage open access to Wi-Fi or do we want closed networks to be the norm? The second, and arguably much more important for the future of our legal system is whether tort liability should be extended to encompass the situations created by wireless technology?

Regarding the first question, other nations have answered the question in several ways. Germany has taken a reasonable middle road and made it mandatory for WLAN operators to password protect their networks.[209] The German high court held that "[p]rivate users

205. 318 F.3d 465, 470-71 (3d Cir. 2003).

206. Gibson v. Craigslist, Inc., No. 08 Civ. 7735(RMB), 2009 WL 1704355, at *3-4 (S.D.N.Y. June 15, 2009).

207. Doe v. MySpace, Inc., 528 F.3d 413, 420-21 (5th Cir. 2008).

208. *Id.*

209. Bundesgerichtshof [BGH] [Federal Court of Justice] May 12, 2010, I ZR 121/08 ¶ 17 (Ger.).

are obligated to check whether their wireless connection is adequately secured to the danger of unauthorized third parties abusing it to commit copyright violation[s]."[210] Network operators who fail to secure their connection are subject to a €100 ($132) fine if the connection is used by a third party to illegally download or share copyrighted material, but are not liable for any damages resulting from the wrongful acts of roaming users.[211]

Open wireless networks have the potential to greatly benefit society by expanding the number and types of connections available to the Internet.[212] Holding unsecured WLAN operators liable for the Internet crimes committed by roaming users may act to discourage copyright infringement and other Internet crimes, but it will also chill lawful access and activity over wireless networks. Many members of the public who enjoy the use of wireless Internet access may be discouraged from enjoying its benefits if they fear being held liable for the actions of others.

Copyright infringement and other Internet crimes do pose a real threat to our society and should be actively discouraged. Holding WLAN administrators liable for the actions of malicious roaming users, however, is not the proper way to curb the undesired behavior. Internet crimes will continue to occur regardless of whether wrongdoers are able to use an unsecured connection. If securing wireless networks is to become a national policy goal it should be accomplished by following the German model that encourages WLAN administrators to take steps necessary to secure their connections while still holding the direct wrongdoer liable for the damage caused by their conduct.

---

210. Translated quotation from the Associated Press. Kirsten Grieshaber, *German Court Orders Wireless Passwords for All*, ASSOCIATED PRESS, May 12, 2010, *available at* http://www.billboard.com/biz/articles/news/1206894/german-court-orders-wireless-passwords-for-all.

211. Bundesgerichtshof [BGH] [Federal Court of Justice] May 12, 2010, BGH, I ZR 121/08 (¶¶ 17, 22-24) (Ger.).

212. *See* Kern, *supra* note 39, at 106.