Spring 2009 www.lawtechjournal.com Volume 13, Issue 1

UCLA Journal of Law & Technology

NO FREE LUNCH (OR WI-FI): MICHIGAN'S UNCONSTITUTIONAL COMPUTER CRIME STATUTE

Stacy Nowicki, Ph.D.

This article examines Michigan's computer crime statute in the context of unsecured wireless internet networks and argues that the statute is unconstitutionally void for vagueness. The statute violates the Due Process Clause of the Constitution because it uses terminology that does not afford citizens fair notice of illegal acts. The statute also fails to characterize prohibited conduct because it does not adequately define terms. This violates Due Process because it enables arbitrary and discriminatory enforcement by police officers and prosecutors. Part II gives a background of wireless internet technology, a legislative history of sections 752.791-752.797 of Michigan's statute, and an overview of the void for vagueness doctrine in constitutional law. Part III focuses on an analysis of sections 752.795 and 752.797(6) in relation to the void for vagueness doctrine. This Part demonstrates how these sections of the statute are unconstitutional because the phrase "valid authorization" does not provide fair notice to the public, and the lack of a definition of "authorization" encourages arbitrary and discriminatory implementation of the statute by law enforcement. Part IV offers solutions for these vagueness problems that would resolve the constitutionality issues, such as defining key terms and excising portions of the statute. Given that many contemporary computing platforms and devices such as Microsoft Windows XP and iPhones automatically detect and connect to unsecured wireless internet connections, Michigan's law criminalizes what has become a social norm. Michigan should make the use of unsecured Wi-Fi presumptively legal and take the best of other states' statutory definitions to create clear meanings for terms in its statute.

TABLE OF CONTENTS

I. Introduction.....1

II. Background.....5

a. Overview of Wireless Technology.....5

b. Michigan's Computer Crime Statute.....7

i. Public Act 53 (1979).....7

ii. 1996 Revision of the 1979 Act.....9

iii. Subsequent Revisions of the 1979 Act 12

c. The Void for Vagueness Doctrine.....13

III. Analysis.....17

a. Michigan's Computer Crime Statute Does Not Give Fair Notice.....17

i. The Phrase "Valid Authorization" is Unclear.....17

b. The Statute Does Not Provide Minimal Guidelines.....24

i. The Statute Allows Too Much Discretion for Law Enforcement.....24

ii. The Lack of Definition for "Authorization" Encourages Arbitrary Enforcement.....27

IV. Solutions.....33

a. Eliminate the Term "Valid".....33

b. Clearly define "Authorization" and "Exceeding Authorization" 33

c. Eliminate Section 752.797(6).....42

V. Conclusion.....42

NO FREE LUNCH (OR WI-FI): MICHIGAN'S UNCONSTITUTIONAL COMPUTER CRIME STATUTE

Stacy Nowicki, Ph.D.

I. INTRODUCTION

Sam Peterson checked his email during his lunch hour, just like other customers at the Re-Union Street Café.[1] But Peterson wasn't a customer—he checked his email from his car, parked outside.[2] Because Peterson pulled up and sat in his car without getting out, someone from a nearby barber shop suspected he was stalking a hairdresser and called the police.[3] Police Chief Andrew Milanowski talked with Peterson, but didn't charge him right away because he wasn't sure that Peterson was breaking the law.[4] However, after researching a Michigan statute on unauthorized computer access, Milanowski contacted Kent County prosecutors.[5] The café's wireless internet network did not require a password,[6] and according to some reports, the café

[1] *Internet Freeloader in Trouble*, GRAND RAPIDS PRESS (Mich.), May 22, 2007, at A1.

[2] *Id.*

[3] Sara Bonisteel, *Michigan Man Fined for Using Coffee Shop's Wi-Fi Network*, FOX NEWS, June 5, 2007, http://www.foxnews.com/story/0,2933,276720,00.html.

[4] *Internet Freeloader in Trouble*, *supra* note 1, at A1.

[5] *Internet Freeloader in Trouble*, *supra* note 1, at A1. Kent County prosecutors had not brought charges under this statute before and had been "hoping to dodge this bullet for a while." Patrick Center, *A Wireless Felony*, WOODTV.COM, June 18, 2007, http://www.woodtv.com/Global/story.asp?S=6546307 (on file with the Internet Archive Wayback Machine, http://web.archive.org/web/20080121104508/http://www.woodtv.com/Global/story.asp?S=6546307). The assistant prosecuting attorney for Kent County said that "it wasn't anything that we frankly particularly wanted to get involved in, but it basically fell in our lap and it was a little hard to just look the other way when somebody handed it to us." Bonisteel, *supra* note 3.

[6] Bonisteel, *supra* note 3.

charged patrons a fee to use the internet if they did not order anything.[7] Sitting outside, Peterson was using the unsecured wireless network for free.

Police arrested Peterson under Michigan's computer crime statute.[8] Michigan law prohibits accessing a computer network to use its services "intentionally and without authorization" or by "exceeding valid authorization."[9] This is a felony punishable by up to five years in prison and a $10,000 fine for citizens without prior convictions, regardless of the amount of loss.[10] Because he had no criminal record, Peterson will avoid charges if he pays $400 in fines and completes forty hours of community service.[11] Peterson's seemingly ridiculous predicament caught the attention of national news sources,[12] caused a firestorm of controversy on the blog circuit,[13] made international news,[14] and inspired a satirical exposé on

---

[7] News reports conflict as to whether the café charged non-paying customers a fee. *Compare Internet Freeloader in Trouble*, *supra* note 1, at A1 (stating that the café charged non-paying patrons a fee to use its wireless internet connection), *with* Bonisteel, *supra* note 3 (quoting café owner Donna May saying that Peterson "could have just come in the café, even if he didn't have any money, I would let him get on [the network]"), *and* Mark Gibbs, *Appalled by Things Legal*, NETWORK WORLD, June 7, 2007, at 34 (reporting that May said anyone was welcome to use her Wi-Fi but she preferred that they ask her first), *and The Colbert Report: Nailed 'Em–Cyberrorists* (Comedy Central television broadcast Oct. 2, 2007), *available at* http://www.colbertnation.com/the-colbert-report-videos/104580/october-02-2007/nailed--em---cyberrorists [hereinafter *Colbert Report*] (interviewing May, who states that Wi-Fi at her café is free).

[8] *Internet Freeloader in Trouble*, *supra* note 1, at A1.

[9] MICH. COMP. LAWS ANN. § 752.795 (West 2004).

[10] MICH. COMP. LAWS ANN. § 752.797(2)(a) (West 2004).

[11] *Internet Freeloader in Trouble*, *supra* note 1, at A1.

[12] Bonisteel, *supra* note 3; Lev Grossman, *Like a Thief in the Net*, TIME, June 23, 2008, at 118, *available at* http://www.time.com/time/magazine/article/0,9171,1813969,00.html (stating incorrectly that Peterson was fined under the Computer Fraud and Abuse Act (18 U.S.C. §1030 (2007 & Supp. 2008)) instead of the Michigan statute); John Agar, *Wi-Fi Use Nearly Lands Man in Jail*, NEW ORLEANS TIMES PICAYUNE, May 28, 2007, at 12.

[13] Orin Kerr, *Crime to Use Coffee Shop Wi-Fi Without Entering the Coffee Shop?* THE VOLOKH CONSPIRACY, May 23, 2007, http://volokh.com/posts/1179938755.shtml; *Everything About You is Wrong*, CRIME & FEDERALISM, May 23, 2007, http://federalism.typepad.com/crime_federalism/2007/05/everything_abou.html; Baron Bodissey, *Assault with a Deadly Laptop*, GATES OF VIENNA, June 2, 2007, http://gatesofvienna.blogspot.com/2007/06/assault-with-deadly-laptop.html; Steven Musil, *Michigan Man Dodges Prison in Theft of Wi-Fi*, CNET.COM, May 22, 2007, http://news.cnet.com/8301-10784_3-9722006-7.html; Russell Shaw, *Michigan Man Busted for Stealing Wi-Fi Signal*, ZDNET.COM, May 22, 2007, http://blogs.zdnet.com/ip-telephony/?p=1640.

[14] John Leyden, *Drive-By Wi-Fi 'Thief' Heavily Fined*, THE REGISTER, May 23, 2007, http://www.theregister.co.uk/2007/05/23/michigan_wifi_conviction/.

Comedy Central's *The Colbert Report*.[15] A Maryland state representative even used Peterson's case to bolster his introduction of a bill that would criminalize intentional wireless internet use in Maryland without permission.[16]

Peterson's situation reflects the problematic relationship between Michigan's law and technology, especially the legality of accessing unprotected wireless networks. For instance, many contemporary computing platforms and devices, such as Microsoft Windows XP and iPhones, automatically detect and connect to unsecured wireless internet connections.[17] In Peterson's case, the Re-Union Street Café may have allowed paying customers to use their wireless internet network for free, but charged patrons a fee to use the internet if they did not order anything.[18] Regardless, the Café did not put security measures in place to prevent non-customers from accessing the network.[19] If piggybacking on an unsecured wireless network like the Café's is illegal, then Michiganders violate the statute daily through gadgets that connect to open wireless networks without their knowledge or intent.

---

[15] *Colbert Report*, *supra* note 7.

[16] Andrew Schotz, *Proposed Md. Bill Would Make Intentional Theft of Wireless Internet Access a Crime*, THE HERALD-MAIL, Mar. 19, 2008, http://www.herald-mail.com/?cmd=displaystory&story_id=188912&format=html (noting that Representative Myers introduced the bill after a neighbor used his wireless internet without permission). The Maryland public defender's office opposed the bill, arguing that it would be difficult to prove intent, and that securing wireless networks would be more effective. *Id.* The bill received an "unfavorable" report from the Maryland House Judiciary Committee. BILL INFO-2008 Regular Session-HB 1377, Maryland House of Representatives (Oct. 31, 2007), http://mlis.state.md.us/2008rs/billfile/hb1377.htm; Eric Bangeman, *Bill Criminalizing WiFi Leeching Shot Down, and Rightly So*, ARSTECHNICA, Mar. 23, 2008, http://arstechnica.com/news.ars/post/20080323-bill-criminalizing-wifi-leeching-shot-down-and-rightly-so.html. For the text of the bill, *see* H.B. 1377, 425th Leg., Reg. Sess. (Md. 2008), *available at* http://mlis.state.md.us/2008rs/bills/hb/hb1377f.pdf.

[17] Luc Small, *Theft in a Wireless World*, 9 ETHICS & INFO. TECH. 179, 180 (2007) (explaining the configuration of Windows XP to automatically select available wireless networks); Glenn Fleishman, *First Look: Finding Wi-Fi Hotspots with the iPhone*, MACWORLD, Jun. 28, 2007, http://www.macworld.com/article/58655/2007/06/iphone_wifi.html (explaining how to use the iPhone's W-Fi capabilities). The ability for gadgets to surf the airwaves for free wireless internet access has existed since at least 2003, when an application called WiFinder was released for the Palm Tungsten C that enabled it to find a public Wi-Fi connection. Ryan Kairer, *WiFinder, WiFi Scanner Released*, PALM INFOCENTER, May 29, 2003, http://www.palminfocenter.com/view_story.asp?ID=5424.

[18] *See* discussion, *supra* note 7.

[19] Bonisteel, *supra* note 3.

Michigan's present statute violates the Due Process Clause of the Constitution. It is void for vagueness because the phrase "valid authorization" does not afford citizens fair notice of illegal acts.[20] The statute also fails to characterize prohibited conduct because it does not adequately define the meaning of "authorization" or "exceeding valid authorization."[21] This violates Due Process because it enables arbitrary and discriminatory enforcement by police officers and prosecutors.[22]

This Comment examines sections 752.795 and 752.797(6) of Michigan's computer crime statute in the context of unsecured wireless internet networks and argues that the statute is unconstitutionally void for vagueness.[23] Part II gives a background of wireless internet technology, a legislative history of sections 752.791-752.797 of Michigan's statute, and an overview of the void for vagueness doctrine in constitutional law. Part III focuses on an analysis of sections 752.795 and 752.797(6) in relation to the void for vagueness doctrine. This Part demonstrates how these sections of the statute are unconstitutional because the phrase "valid authorization" does not provide fair notice to the public, and the lack of a definition of "authorization" encourages arbitrary and discriminatory implementation of the statute by law enforcement. Part IV offers solutions for these vagueness problems that would resolve the constitutionality issues, such as defining key terms and excising portions of the statute.

---

[20] The statute contains a mens rea requirement of "intentionally." MICH. COMP. LAWS ANN. § 752.795 (West 2004). A vagueness challenge is more viable if a criminal law has no mens rea requirement. *See* City of Chicago v. Morales, 527 U.S. 41, 55 (1999). But a statute is not automatically void for vagueness because it does not contain a mens rea requirement. *See* Rita J. Verga, *An Advocate's Toolkit: Using Criminal 'Theft of Service' Laws to Enforce Workers' Right to Be Paid*, 8 N.Y. CITY L. REV. 283, 297 n.59 (2005) (citing State v. Wilson, 848 A.2d 542, 544 (Conn. App. 2004)). Additionally, a mens rea requirement may mitigate a law's vagueness. Andrew E. Goldsmith, *The Void-for-Vagueness Doctrine in the Supreme Court, Revisited*, 30 AM. J. CRIM. L. 279, 301 (2003) (citing Vill. of Hoffman Estates v. Flipside, 455 U.S. 489, 499 (1982)). However, a law containing a mens rea requirement may still fail a vagueness challenge. John F. Decker, *Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws*, 80 DENV. U. L. REV. 241, 290 (2002).

[21] MICH. COMP. LAWS ANN. § 752.792 (West 2004).

[22] For an in-depth discussion of the void for vagueness doctrine, *see* Robert Batey, *Vagueness and the Construction of Criminal Statutes – Balancing Acts*, 5 VA. J. SOC. POL'Y & L. 1, 4 (1997).

[23] MICH. COMP. LAWS ANN. §§ 752.791-752.797 (West 2004 & Supp. 2008).

II. BACKGROUND

a. Overview of Wireless Technology

Wireless internet, also known as "Wi-Fi," uses radio waves to communicate between a computer and a wireless router, which sends the computer's information to the internet.[24] Wireless internet networks use the 802.11 networking standard, a protocol established by the Institute of Electrical and Electronics Engineers (IEEE).[25] Various "flavors" of the IEEE 802.11 standard carry data at different speeds and use different parts of the radio spectrum.[26] Wi-Fi is distinct from cellular telephone technology, though both use radio signals. A Wi-Fi signal can carry more data than the ones used for cell phones, walkie-talkies, and televisions because it transmits at a higher frequency.[27] However, some newer phones can move seamlessly between a cell phone network and a Wi-Fi network.[28] These dual-network phones have become popular because entities like libraries and municipalities have made free Wi-Fi networks available to connect the public to the internet.[29] Termed "hotspots," public wireless internet access is also popular in airports, restaurants, hotels, RV parks, cafés, and other hangouts.[30] Even cars are now

---

[24] Marshall Brain & Tracy V. Wilson, *How WiFi Works*, Howstuffworks.com, http://computer.howstuffworks.com/wireless-network.htm (last visited Sept. 20, 2008); *see* EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS AND THE INTERNET 367 (2d ed. 2004).

[25] Brain & Wilson, *supra* note 24.

[26] *Id.* The different "flavors" of networking standards are 802.11a, 802.11b. 802.11g, and 802.11n. *Id.*

[27] *Id.*

[28] Matt Richtel, *The Wi-Fi in Your Handset,* N.Y. TIMES, July 29, 2006, at C2; What is Wi-Fi Cell Phone?: A Definition from Whatis.com (Mar. 7, 2008), http://searchunifiedcommunications.techtarget.com/sDefinition/0,,sid186_gci1170497,00.html.

[29] *See* Richtel, *supra* note 28, at C2. Unfortunately, some agreements between municipalities and internet providers are falling through as providers' profits decline and technology infrastructures become more costly. Ian Urbina, *Hopes for Wireless Cities Fade as Internet Providers Pull Out*, N.Y. TIMES, Mar. 22, 2008, at A10.

[30] *See* Wifinder.com, http://www.wifinder.com/ (last visited Oct. 5, 2008) (directing users to public Wi-Fi hotspots around the globe).

Wi-Fi hotspots; Chrysler recently announced a service called "UConnect" that combines cellular and Wi-Fi technologies to enable internet access in a car and within 100 feet around it.[31]

Though some individuals and organizations intentionally leave their Wi-Fi networks open for anyone to use, others run Wi-Fi networks that are inadvertently unsecured.[32] A 2006 Wi-Fi Alliance survey found that, though many Americans believe that securing their home Wi-Fi networks is just as important as locking their windows and doors, nearly thirty percent of home users using wireless networks do not have any security measures in place, leaving their wireless internet networks open for anyone to use.[33] Unfortunately, wireless networks using IEEE 802.11 technology are notoriously insecure.[34] Even with some data encryption in place, wireless networks are still vulnerable to hacking to intercept data or modify files.[35] Furthermore, the proliferation of public and unsecured Wi-Fi has initiated a movement called "war driving" where individuals drive around businesses and neighborhoods with laptops to find open Wi-Fi networks and even map them for others to use.[36]

---

[31] Marin Perez, *Chrysler's In-Car Wi-Fi Ready to Roll Aug. 25*, INFO. WEEK, Aug. 13, 2008, http://www.informationweek.com/news/mobility/wifiwimax/showArticle.jhtml?articleID=210003709.
[32] CASEY, *supra* note 24, at 368.
[33] Wi-Fi Alliance, Survey: Protecting Wireless Network an Essential Element of Home Security (Nov. 2, 2006), http://www.wi-fi.org/pressroom_overview.php?newsid=1.
[34] WEI-MENG LEE, WINDOWS XP UNWIRED: A GUIDE FOR HOME, OFFICE AND THE ROAD 53 (2003); Matthew Gast, *Seven Security Problems of 802.11 Wireless*, O'REILLY MEDIA, May 24, 2002, http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html; Alex Tsow, Markus Jakobsson, Liu Yang & Susanne Wetzel, *Warkitting: The Drive-by Subversion of Wireless Home Routers*, 1 J. DIGITAL FORENSIC PRAC. 179 (2006).
[35] 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, 113 (2004). "Hacking" is the subversion of security measures through computer code. NEIL BARRETT, THE BINARY REVOLUTION: THE DEVELOPMENT OF THE COMPUTER 236 (2006). In the largest hacking scheme to date, hackers stole over forty-one million credit and debit card numbers by identifying security holes in the wireless networks of retail stores. Brad Stone, *U.S. Charges 11 in Global Ring of ID Theft*, N.Y. TIMES, Aug. 6, 2008, at C1.
[36] CASEY, *supra* note 24, at 368; Kern, *supra* note 35, at 101; LEE, *supra* note 34, at 49-52.

Despite concerns about the insecurity of wireless networks, their popularity is high.[37] As of December 2006, one-third of internet users in the United States had used the web or checked email via wireless networks;[38] of those users, twenty percent had gone online via a wireless network at home, and twenty seven percent have used wireless networks outside of home or their place of employment.[39] These statistics demonstrate the pervasiveness of wireless internet use, which will likely continue to grow as more cell phone users discover mobile data services such as internet, text messaging, and email access.

b. Michigan's Computer Crime Statute

i. Public Act 53 (1979)

Michigan was among the first states to create a computer crime statute.[40] In 1979, the state legislature passed Public Act 53, which criminalized users accessing a computer or computer network for the purpose of obtaining money, property, or services by fraud.[41] Michigan recognized that traditional legal concepts were ill-equipped to deal with crimes perpetrated through technology.[42] Like many states, Michigan modeled its statute on the proposed Federal Computer Systems Protection Act of 1977.[43] Michigan's legislature aimed the

---

[37] *See* Robert V. Hale, *Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 543, 543-44 (2005).

[38] JOHN HORRIGAN, PEW INTERNET & AMERICAN LIFE PROJECT, WIRELESS INTERNET ACCESS 1 (2007),http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_Wireless.Use.pdf.pdf. This data includes users who utilize laptop computers, cell phones, and handheld personal digital assistants (PDAs) to access the internet. *Id.*

[39] *Id.* at 2.

[40] A. HUGH SCOTT & KATHLEEN BURDETTE SHIELDS, COMPUTER AND INTELLECTUAL PROPERTY CRIME: FEDERAL AND STATE LAW, at 28-4 n.6 (Supp. 2006). In 1978 Florida was the first state to pass computer crime legislation following an incident where employees printed fraudulent winning dog racing tickets with a computer. CASEY, *supra* note 24, at 25.

[41] MICH. COMP. LAWS ANN. §§ 752.791-752.797 (West 2004); 1979 Mich. Legis. Serv. 456 (West).

[42] HOUSE LEGISLATIVE ANALYSIS, H.B. 4112, at 1 (Mich. May 22, 1979). For a contemporaneous discussion of the need for computer crime statutes, *see generally* Cecelia E. Campbell-Klein, A Historical and Analytical Study of the Federal Computer Systems Protection Act of 1978 (1980) (unpublished M.A. thesis, University of California, Irvine) (on file with University of California Library, Irvine).

[43] Robin K. Kutz, *Computer Crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act*, 27 WM. & MARY L. REV. 783, 789 n.31 (1986) (listing twenty-three states with statutes

bill at "ingenious persons who can program a computer to defraud an organization or business and divert information or funds to themselves."[44] Section 752.795 of the Act established that "[a] person shall not intentionally and without authorization, gain access to, alter, damage, or destroy a computer, computer system, or computer network, or gain access to, alter, damage, or destroy a computer software program or data contained in a computer, computer system, or computernetwork."[45]

A violation of the Act was a misdemeanor if the crime caused damages of $100 or less. If damages exceeded $100, the violation was a felony punishable by up to ten years in prison or a fine up to $5,000 or both.[46] The bill passed overwhelmingly in the senate, with only two senators voting against it. Senator Fredericks explained his negative vote in a written protest, stating that "the bill makes it a felony for a person to 'gain access to' a computer. What does 'gain access to' mean? . . . The potential for abuse of a definition that loose is almost unbounded. The legislature must be vastly more specific before passing legislation of this nature."[47] Legislative analysis of the bill from the Michigan House of Representatives also suggested that the definition of "computer" in the bill might not be thorough enough to cover all computer processing.[48] Nonetheless, the house passed the bill unanimously.[49]

---

resembling the 1977 or 1979 proposed Federal Computer Systems Protection Act); *see* Joseph Audal, Quincy Lu & Peter Roman, *Computer Crimes Twenty-Third Annual Survey of White Collar Crime,* 45 AM. CRIM. L. REV. 233, 267-68 (2008); *Federal Computer Systems Protection Act: Hearings on S. 1766 Before the Subcomm. on Criminal Laws and Procedures of the S. Comm. on the Judiciary*, 95th Cong. 170-71 (1979).

[44] HOUSE LEGISLATIVE ANALYSIS, H.B. 4112, at 1 (Mich. 1979).

[45] PUBLIC & LOCAL ACTS 1979, *supra* note 41, at 142.

[46] *Id.* at 143.

[47] 2 MICH. J. OF THE SENATE 1211 (1979).

[48] HOUSE LEGISLATIVE ANALYSIS, H.B. 4112, at 1 (Mich. 1979).

[49] 2 MICH. J. OF THE HOUSE 1497-98 (1979). The amendments recommended and passed by the senate, and ultimately passed by the house, did not refer to the ambiguities pointed out by Senator Fredericks. *Id.*

Some definitional issues from the 1979 statute remain in Michigan's current statute. For instance, despite the concerns expressed by Senator Fredericks and the legislative analysis over definitions contained in the bill, the 1979 statute did not define what "without authorization" meant.[50] Additionally, though the statute focused on gaining access to a computer for fraudulent purposes, the Michigan Bankers Association expressed apprehension that the 1979 statute criminalized personal use of organizational computers.[51] It suggested that the legislature differentiate between major and minor unauthorized use.[52] The Association stated:

> In the computer industry, the unauthorized personal use of computers is an industry-wide operation. Practically every computer programmer or operator runs games, golf league statistics, and other personal projects without express authority of the computer owner. Although the use is forbidden[,] it is tolerated. The association believes that it is not a good idea to make such harmless use a felony with a potential ten-year prison term. A feasible alternative to this concern would be to distinguish between "petty" and "grand" use and provide that the unauthorized use of computer services having a value of less than a specified dollar amount would only be a misdemeanor.[53]

ii. 1996 Revision of the 1979 Act

By the mid-1990s, computer hacking was costing businesses millions of dollars,[54] federal lawmakers grew more concerned with the use of computers for child pornography,[55] and many states either enacted their first computer crime statutes or amended them to reflect the latest

---

[50] PUBLIC & LOCAL ACTS 1979, *supra* note 41, at 142.

[51] House Legislative Analysis, H.B. 4112, at 1 (Mich. 1979).

[52] *Id*.

[53] *Id.*

[54] Testimony of Richard G. Power, Editor, Computer Security Institute, Before the Permanent Subcommittee on Investigations, U.S. Senate Committee on Governmental Affairs (June 5, 1996), http://www.fas.org/irp/congress/1996_hr/s9606051.htm.

[55] The federal government enacted legislation in response, including the Communications Decency Act of 1996 and the Child Pornography Prevention Act of 1996. Audal, *supra* note 43, at 245-48.

crimes.[56] Though computer crime had clearly been a problem since the 1970s when states enacted their first computer crime statutes, the personal computer revolution in the 1980s and the advent of the World Wide Web in the 1990s created more fertile ground for computer crimes to flourish.[57] In 1996, the Michigan Legislature updated the computer crime statute to address technological advances, the rise of computer hackers, and the increasing number of individuals and businesses using computers.[58] Public Act 326 revised section 752.795 and inserted the problematic wording that persists in Michigan's current computer crime statute (revised wording in italics):

> A person shall not intentionally and without authorization *or by exceeding valid authorization do any of the following*:
>
> *(a) Access or cause access to be made to a computer program, computer, computer system, or computer network* to *acquire*, alter, damage, *delete*, or destroy *property or otherwise use the service of* a *computer program*, computer, computer system, or computer network.[59]

The addition of the phrase "exceeding valid authorization" increases the scope of the statute by applying it to authorized users who go beyond their permission to use the system.[60] As in the 1979 statute, the 1996 revision does not define "without authorization" or "exceeding valid authorization." Public Act 326 also inserted the "rebuttable presumption" wording in section 752.797(6):

> It is a rebuttable presumption in a prosecution for a violation of section 5 that the person did not have authorization from the owner, system operator, or other person who has authority from the owner or system operator to grant permission to access the computer program, computer, computer system, or computer network or has exceeded authorization unless 1 or more of the following

[56] A. HUGH SCOTT, COMPUTER AND INTELLECTUAL PROPERTY CRIME: FEDERAL AND STATE LAW 46 (2001 & Supp. 2006).

[57] *Id.* at 38-51.

[58] HOUSE LEGISLATIVE ANALYSIS, H.B. 5748-5755, at 1, 5 (Mich. 1996).

[59] 1996 Mich. Pub. Acts 1031.

[60] Patrick E. Corbett, *Cyberbullying and Other High-Tech Crimes Involving Teens*, 12 J. INTERNET L. 1, 14 (2008).

circumstances existed at the time of access:

> (a) Written or oral permission was granted by the owner, system operator, or other person who has authority from the owner or system operator to grant permission of the accessed computer program, computer, computer system, or computer network.
>
> (b) The accessed computer program, computer, computer system, or computer network had a pre-programmed access procedure that would display a bulletin, command, or other message before access was achieved that a reasonable person would believe identified the computer program, computer, computer system, or computer network as within the public domain.
>
> (c) Access was achieved without the use of a set of instructions, code, or computer program that bypasses, defrauds, or otherwise circumvents the pre-programmed access procedure for the computer program, computer, computer system, or computer network. [61]

The 1996 revision also created more severe penalties for violating the statute. Instead of requiring damage up to or beyond $100, the 1996 revision formed a complex scheme in section 752.797 that was further tiered and dependent on the amount of loss.[62] The legislature further developed the amount of loss to use an "aggregate amount" of direct or indirect loss, which included money, property, or services.[63]

Concerns over the 1996 revision centered on innocent users of the World Wide Web. Under the rebuttable presumption in section 752.797(6), innocent computer users could accidentally blunder into a closed system and "find themselves facing a criminal charge that presumed they were doing something illegally."[64] A Michigan House bill analysis recognized

---

[61] 1996 Mich. Pub. Acts 1032.

[62] *Id.* at 1031. Up to a $200 loss was a 93-day misdemeanor subject to a $500 to $600 fine, a $200 to $1,000 loss was a one-year misdemeanor subject to a $2,000 to $3,000 fine, a $1,000 to $20,000 loss was a five-year felony subject to a $10,000 to $60,000 fine; and a $20,000 plus loss was a ten-year felony subject to a $60,000 fine or more. *Id.*

[63] *Id.* at 1030-31. The definition of "services" includes computer time, data processing, storage functions, computer memory, or the unauthorized use of a computer. *Id.* at 1030.

[64] HOUSE LEGISLATIVE ANALYSIS, H.B. 5184-5187, S.B. 893 and 894, at 5 (Mich. 2000), *available at* http://www.legislature.mi.gov/documents/1999-2000/billanalysis/House/pdf/1999-HLA-5184-C.pdf.

that it could be difficult and costly for the network user to rebut the presumption that he or she had acted unlawfully.[65]

iii. Subsequent Revisions of the 1979 Act

In September 2000, Michigan's attorney general used section 752.795 for the first time, charging two teenagers with hacking.[66] The Michigan Legislature had just revised the statute through Public Act 180,[67] this time criminalizing unauthorized access to computers without regard to the amount lost.[68] Since the 2000 revision changed the law to no longer require $1,000 in damage for the crime to be a felony, one of the teens accused of hacking faced felony charges.[69]

The 2000 revision also narrowed the rebuttable presumption of section 752.797(6) added in 1996 to apply to section 752.795 of the statute only.[70] However, these revisions did not address the issue raised in 1996 regarding the rebuttable presumption for the innocent user.[71]

---

[65] *Id.* Sam Peterson's case exemplifies this situation. Bonisteel, *supra* note 3 (quoting Peterson as saying, "A lot of people tell me I should fight this, but they're not the ones looking at the felony charges on their record if it happens to go bad."). Furthermore, section 752.797(6) may be unconstitutional because it may violate the constitutional presumption of innocence. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1624 n.110 (2003). A similar debate is occurring in Illinois. Theodore A. Gottfried & Peter G. Baroni, *Presumptions, Inferences and Strict Liability in Illinois Criminal Law: Preempting the Presumption of Innocence?*, 41 J. MARSHALL L. REV. 715 (2008).

[66] 39 GONGWER NEWS SERVICE, MICHIGAN REPORT NO. 179, at 11 (2000). Assistant Attorney General Terry Berg said that no one had been charged under the law until 2000 because businesses did not want to publicize a security lapse, technological complexities made hacking cases difficult to investigate, and few people had access to the Internet when the law was passed. Dennis Niemiec, *High-Tech Prankster Finds Trouble Under Michigan Hacker Law*, DETROIT FREE PRESS, Oct. 2, 2000, at 1B.

[67] 2000 Mich. Pub. Acts 512.

[68] Patrick Corbett, *Michigan's Arsenal for Fighting Cybercrime: An Overview of State Laws Relating to Computer Crimes*, 79 MICH.B.J. 656, 657 (2000); *see also* Patrick Corbett, *State and Federal Criminal Cyberlaw and Legislation Survey*, 18 T.M. COOLEY L. REV. 7 (2001).

[69] Niemiec, *supra* note 66, at 1B. Teen Jesse Salens was charged even though he claimed no password was required to alter the website. *Id.*

[70] 2000 Mich. Pub. Acts 512.

[71] HOUSE LEGISLATIVE ANALYSIS, H.B. 5184-5187, S.B. 893 and 894, at 5 (Mich. 2000), *available at* http://www.legislature.mi.gov/documents/1999-2000/billanalysis/House/pdf/1999-HLA-5184-C.pdf.

The Michigan legislature introduced two bills in 2007 that further expand the statute. Michigan Senate Bill 144 adds section 752.795(b) and states that a person shall not:

> (a) Intentionally and without authorization install or attempt to install spyware into a computer, computer program, computer system, or computer network belonging to another person.
> (b) Intentionally and without authorization use or attempt to use spyware that has been installed into a computer, computer program, computer system, or computer network belonging to another person.
> (c) Manufacture, sell, or possess spyware with the intent that it be used to violate this act . . . .[72]

This bill prescribes the same penalties as a violation of section 752.795. It also defines "authorized user" as "the owner of a computer, computer program, computer system, or computer network or a person authorized by the owner or the lessee to use the computer, computer program, computer system, or computer network."[73] However, the bill does not define what "authorized" means.

At the same time, the legislature introduced Michigan Senate Bill 145, the Spyware Control Act. This bill defines "authorized user" as "the owner of the computer or a person who is authorized by the owner or lessee of the computer to use the computer."[74] However, this bill also does not define what the term "authorized" means.

c. The Void for Vagueness Doctrine

The void for vagueness doctrine challenges the language of a law as unconstitutional.[75] It originates in the Due Process Clauses of the Fifth and Fourteenth Amendments, which assert that neither federal nor state governments shall deprive any person of "life, liberty, or property,

---

[72] S. 144, 94th Leg., Reg. Sess. (Mich. 2007), *available at* http://www.legislature.mi.gov/documents/2007-2008/billintroduced/Senate/pdf/2007-SIB-0144.pdf.

[73] *Id.*

[74] S. 145, 94th Leg., Reg. Sess. (Mich. 2007), *available at* http://www.legislature.mi.gov/documents/2007-2008/billintroduced/Senate/pdf/2007-SIB-0145.pdf.

[75] *See* Michael C. Steel, *Constitutional Law – The Vagueness Doctrine: Two-Part Test, or Two Conflicting Tests?* City of Chicago v. Morales, *119 S. Ct. 1849 (1999)*, 35 LAND & WATER L. Rev. 255, 257 (2000).

without due process of law."[76] A statute that does not clearly define forbidden behavior violates due process because it does not give the public notice of what activities are prohibited, and law enforcement can enforce the law in an arbitrary and discriminatory way.[77] The void for vagueness doctrine requires that statutes contain clear, precise language so they "give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly."[78]

The vagueness doctrine is often confused with the overbreadth doctrine,[79] and the two are related in that they both deal with laws containing imprecise language. However, the overbreadth doctrine differs from the vagueness doctrine because it prevents criminal laws from infringing upon constitutionally protected activity.[80] The Supreme Court most often applies the overbreadth doctrine to First Amendment cases, but the Court has applied the doctrine to other constitutional rights as well, such as the freedom of movement and right to vote.[81] In contrast, whether a statute prohibits activities that are constitutionally protected is irrelevant to the vagueness doctrine. The central principle of the vagueness doctrine is whether "men of common intelligence must necessarily guess at [a law's] meaning and differ as to its application."[82]

---

[76] Vanessa Wheeler, Comment, *Discrimination Lurking on the Books: Examining the Constitutionality of the Minneapolis Lurking Ordinance*, 26 LAW & INEQ. 467, 473 n.41 (2008) (citing U.S. CONST. amend. V, cl. 4 and U.S. CONST. amend. XIV, § 1, cl. 3).

[77] Batey, *supra* note 22, at 4 (citing Coates v. City of Cincinnati, 402 U.S. 611 (1971) and Papachristou v. City of Jacksonville, 405 U.S. 156, 168-71 (1972)).

[78] Goldsmith, *supra* note 20, at 284 (citing Grayned v. City of Rockford, 408 U.S. 104, 108 (1972)).

[79] John F. Decker, *Overbreadth Outside the First Amendment*, 34 N.M. L. REV. 53, 60 (2004).

[80] M. Katherine Boychuk, *Are Stalking Laws Unconstitutionally Vague or Overbroad?*, 88 NW. U. L. REV. 769, 773 (1994).

[81] *Id*. at 773 n.22.

[82] Connally v. Gen. Constr. Co., 269 U.S. 385, 391 (1926).

The void for vagueness doctrine focuses on two fundamentals: fair notice for citizens and minimal guidelines for law enforcement.[83] A statute need not fail both in order to be unconstitutionally vague; a failure of one or the other will suffice.[84] The fair notice element exists so that citizens can act in conformity to the law.[85] Citizens have a better chance of acting in conformity with the law if they are aware of what conduct is prohibited; otherwise, "the public is more likely to violate the law unwittingly, thereby expanding the pool of potential suspects."[86] Though easy to understand, the fair notice element can be difficult to apply.[87] For example, "fair notice" does not imply "actual notice."[88] Publication of a statute without further instruction for the public is always adequate notice, regardless of how difficult the statute is to find.[89] Rather, courts have defined "fair notice" in this context to mean "defin[ing] the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited."[90] Furthermore, finding a standard to apply is problematic. Awareness of a statute, knowledge of the law, and life experience vary from person to person.[91] Even reliance on the "ordinary person" standard is difficult because the "ordinary person" neither reads statute books nor studies

---

[83] Steel, *supra* note 75, at 258 (citing City of Chicago v. Morales, 527 U.S. 41, 56 (1999)). Steel contends that the two elements of the void for vagueness doctrine have really developed into two separate tests which, if applied independently, produce conflicting results. *Id.*

[84] *Id*. For example, in *Morales*, the Supreme Court found a Chicago city ordinance forbidding loitering to be unconstitutional on the minimal guidelines element alone. Goldsmith, *supra* note 20, at 289 (citing City of Chicago v. Morales, 527 U.S. 41 (1999)). Some commentators, and even the Court, refer to these two ideas as "elements" or "prongs," but both terms are misleading since both need not be shown. *See* Smith v. Goguen, 415 U.S. 566, 574 (1974) (referring to minimal guidelines as "the other principal element of the doctrine"); Goldsmith, *supra* note 20 (using the term "prong"); Wheeler, *supra* note 76 (using the term "prong").

[85] *Morales*, 527 U.S. at 58.

[86] Kim Forde-Mazrui, *Ruling Out the Rule of Law*, 60 VAND. L. REV. 1497, 1517 (2007).

[87] Batey, *supra* note 22, at 4.

[88] John Calvin Jeffries, Jr., *Legality, Vagueness, and the Construction of Penal Statutes*, 71 VA. L. REV. 189, 207 (1985).

[89] *Id.*

[90] Wheeler, *supra* note 76, at 473 (citing Kolender v. Lawson, 461 U.S. 352, 357 (1983)).

[91] *See* Batey, *supra* note 22, at 4.

cases interpreting criminal statutes.[92] Though ignorance of the law is not an excuse,[93] courts do not focus on a particular defendant, but rather ask whether "a person familiar with the statute and its official interpretation would have fair notice."[94]

Even more important to the vagueness doctrine than the fair notice element is the minimal guidelines element.[95] The purpose of the minimal guidelines element is to prevent law enforcement from arbitrarily enforcing statutes and "pursu[ing] their personal predilections."[96] Too much discretion on the part of police and prosecutors can lead to irreparable harm to the wrongly accused.[97] Therefore, a statute must "provide explicit standards for those who apply them."[98] How does a legislature know when a law meets the "minimal guidelines" standard? The best guidance the Court provides is that statutes are to include "ascertainable standards of guilt" that are measureable by objective norms.[99]

Furthermore, legislatures must also balance these "minimal guidelines" with factors that necessitate vague language in a statute.[100] For example, law enforcement officers must be able to use their judgment to determine how and if to take action in any particular situation,[101] and the language of a law must be flexible enough to respond to societal changes, technological advances, and multiple criminal situations.

---

[92] *Id.* at 5.

[93] People v. Turmon, 340 N.W.2d 620, 657 (1983) (paraphrasing WILLIAM BLACKSTONE, 4 COMMENTARIES ON THE LAWS OF ENGLAND 27 (11th ed. 1791)).

[94] Batey, *supra* note 22, at 5.

[95] Decker, *supra* note 79, at 61 (citing Smith v. Goguen, 415 U.S. 566, 574 (1974)).
[96] Kolender v. Lawson, 461 U.S. 352, 358 (1983) (quoting *Goguen,* 415 U.S. at 575).
[97] Batey, *supra* note 22, at 6.
[98] Grayned v. City of Rockford, 408 U.S. 104, 108 (1972).

[99] *See* John F. Decker, *Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws*, 80 DENV. U. L. REV. 241, 253 (2002) (quoting Palmer v. City of Euclid, 402 U.S. 544, 545 (1971); Keyishian v. Bd. of Regents, 385 U.S. 589, 604 (1967); NAACP v. Button, 371 U.S. 415, 466 (1963)).
[100] *See generally* Batey, *supra* note 22, at 10.

[101] *See* Debra Livingston, *Police Discretion and the Quality of Life in Public Places: Courts, Communities, and the New Policing*, 97 COLUM. L. REV. 551, 658 (1997).

III. ANALYSIS

Sections 752.795 and 752.797(6) of Michigan's computer crime statute are void for vagueness. The statute fails to communicate which behaviors are permissible and which are prohibited, and it permits the police too much discretion. For example, the phrase "valid authorization" is vague and does not offer the public fair notice, and the term "authorization" is undefined, which encourages arbitrary and discriminatory enforcement.

a. Michigan's Computer Crime Statute Does Not Give Fair Notice

i. The Phrase "Valid Authorization" is Unclear

The rebuttable presumption in section 752.797(6) uses the phrase "exceeded authorization." Section 752.795, on the other hand, uses the phrase "exceeding *valid* authorization." The addition of the phrase "exceeding valid authorization" in section 752.795 suggests that the Michigan Legislature revised the statute to apply to both "outsiders" (unauthorized users who intentionally access a system) as well as "insiders" (authorized users who go beyond their permission to use the system).[102] However, legislative history does not reveal why the legislature chose to include the term "valid" in section 752.795, but not section 752.797(6),[103] since the legislature revised both sections of the statute at the same time.[104]

This phrase "valid authorization" is vague because there is more than one definition of the word "valid."[105] "Valid" could mean "able to effect or accomplish what is designed or

---

[102] Corbett, *supra* note 60, at 14; Kerr, *supra* note 65, at 1630-31.
[103] Though legislative history is one method by which meaning of a term can be construed, the history of this statute is not illuminating. *See generally* Goldsmith, *supra* note 20, at 296-98.
[104] 1996 Mich. Pub. Acts 1031.
[105] Some commentators argue that a double meaning is actually an ambiguity rather than vagueness (where a word is not understood). Paul G. Morrissey, *Do the Adult Crime, Do the Adult Time: Due Process and Cruel and Unusual Implications for a 13-Year-Old Sex Offender Sentenced to Life Imprisonment in* State v. Green, 44 VILL. L. REV. 707, 734 n.158 (1999); Jeremy Waldron, *Vagueness in Law and Language: Some Philosophical Issues*, 82 CAL. L. REV. 509, 512 (1994). Earlier editions of Black's Law Dictionary defined "ambiguous" as "doubleness of meaning." Morrissey, *Do the Adult Crime,* 734 n.158 (citing BLACK'S LAW DICTIONARY 79, 1549 (6th ed. 1990)). However, the current edition defines "ambiguity" as "an uncertainty of meaning or

intended" (as in "valid methods").[106] In this sense, "valid authorization" could mean that a password is correct and effective because it is accepted by the system and produces a desired result: the user gains access to a network.[107] However, "valid" could also mean "sanctioned," "justifiable," or "having legal strength or force" (as in a "valid contract").[108] Interpreted this way, "valid authorization" could mean that the authorization was given by someone who has the authority to do so.[109]

These definitions give different results under the statute. Using the first definition, if "valid authorization" refers to an effective password, then perhaps it does not matter that a password was stolen or used without permission—the mere fact that the password allows access to the system would make it "valid authorization."[110] Two federal court cases interpreting the Digital Millennium Copyright Act of 1998 (DMCA)[111] support this reading. In *Egilman v. Keller*,[112] the defendant used "an unauthorized but valid password" to access a computer and website without permission from the plaintiff.[113] In deciding whether this was a "circumvention of technological measures" (hacking), the court concluded that "using a username/password

---

intention" and explains that "double meaning" is the "ordinary language" interpretation, whereas in "judicial usage" an ambiguity is "any kind of doubtful meaning of words." BLACK'S LAW DICTIONARY 88 (8th ed. 1990) (quoting RUPERT CROSS, STATUTORY INTERPRETATION 76-77 (1976)).

[106] WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY OF THE ENGLISH LANGUAGE UNABRIDGED 2530 (3d ed. 1961) [hereinafter WEBSTER'S THIRD].

[107] Kerr, *supra* note 65, at 1619-20 (stating that "a user who enters a valid username and password has accessed the computer, but a user who inputs an incorrect name or password has been denied access.").

[108] WEBSTER'S THIRD, *supra* note 107, at 2529.

[109] *See* discussion *infra* pp. 21-22.

[110] Egilman v. Keller & Heckman, LLP, 401 F. Supp. 2d 105, 113 (D.D.C. 2005) (citing I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys, Inc., 307 F. Supp. 2d 521 (S.D.N.Y. 2004) and observing that "[i]t was irrelevant who provided the username/password combination to the defendant, or, given that the combination itself was legitimate, how it was obtained.").

[111] 17 U.S.C. § 1201 (2007 & Supp. 2008).

[112] 401 F. Supp. 2d. 105 (D.D.C. 2005).

[113] *Id*. at 112.

combination as intended—by entering a valid username and password, albeit without authorization—does not constitute circumvention under the DMCA."[114] The court in *I.M.S. v. Berkshire*[115] also distinguished between "circumvention" under the DMCA and using a username and password without permission.[116] In both of these cases, the defendant's actions are analogous to stealing a key to open a door rather than picking a lock.[117] Therefore, the meaning of the term "valid" in these cases refers to the effectiveness of the username and password in obtaining access to a computer or network.[118]

A user could also exceed valid authorization under this first definition. For example, one person could log on to a network with a password (stolen or not) and allow a second person to access the network. If the network was unsecured, as in Sam Peterson's case, then "valid authorization" could mean that anyone could access the network without logging in because the Re-Union Street Café's act of broadcasting an open Wi-Fi signal into the street implied that all access was "valid."[119] In the case of an unsecured network, a user might exceed valid authorization if she used the network too frequently or for too long.

Applying the second definition of "valid," "valid authorization" could refer to permission given by someone who has the power to do so. The issue here is who has the right to authorize permission. For example, if a mid-level manager instructs a data entry technician to access part of a computer network without authority from the company's CEO, has the data entry technician

[114] *Id*. at 112-13.

[115] 307 F. Supp. 2d 521 (S.D.N.Y. 2004).

[116] *Id*. at 532.

[117] *See* Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 497 F.Supp.2d 627, 645 (E.D.Pa. 2007).

[118] *But cf.* Commonwealth v. Farley, No. 95934, 1996 WL 1186936, at *2 (Mass. Super. Oct. 18, 1996) (interpreting the use of stolen passwords as "unauthorized" under the Massachusetts statute). The Massachusetts statute states that "[t]he requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users," but it does not use the term "valid." MASS. GEN. LAWS ch. 266 § 120F (2008).

[119] *See* Small, *supra* note 17, at 181.

has exceeded valid authorization? In another scenario, a company's computer use policy could forbid personal email use on the company's computers, but a manager allows his staff to do so. It is impossible for the company's staff to know whether they have valid authorization to use the computers for personal email—who has more authority, the manager or the written policy? Internet service provider (ISP) contracts routinely state that the subscriber may be liable if third parties access a subscriber's wireless internet network.[120] If a café allows customers to use their Wi-Fi, have they given valid authorization to their patrons even though it may violate their ISP contract? Patrick Corbett suggests that determining when a user is "unauthorized" or when an authorized user exceeds "valid authorization" is the duty of a jury.[121] However, this does not help network users because they cannot rely on a jury to determine which everyday computer uses comprise valid authorization. Therefore, Michigan's statute may or may not be violated depending on the meaning each third party gives to "valid authorization" and depending on which third party defines "valid authorization."

Assuming that a network user can determine who has the right to give "valid authorization", the phrase is still subjective. In *United States. v. Williams*, the Court elaborated on the kind of language it found objectionable:

> What renders a statute vague is not the possibility that it will sometimes be difficult to determine whether the incriminating fact it establishes has been proved; but rather the indeterminacy of precisely what that fact is. Thus, we have struck down statutes that tied criminal culpability to whether the defendant's conduct was "annoying" or "indecent"—wholly subjective judgments without statutory definitions, narrowing context, or settled legal meanings.[122]

---

[120] *See* S. Gregory Herrman, Comment, *One or More Wireless Networks Are Available: Can ISPs Recover for Unauthorized Wi-Fi Use Under Cable Television Piracy Laws?,* 55 CATH. U. L. REV. 1095, 1127 n.219 (2006); Hale*, supra* note 37, at 555-56.

[121] Corbett, *supra* note 60, at 14.

[122] 128 S. Ct. 1830, 1846 (2008).

As in *Williams*, the phrase "valid authorization" is subjective because a third party, such as the Re-Union Street Café, must clarify what the phrase means.[123] Since each third party will have a different standard of "valid authorization," a user may not know what facts create validity or invalidity. For example, each café offering Wi-Fi may have a different policy that determines under what circumstances non-paying patrons are allowed internet access; none of which may be clear to the person who just wants to check his email.

Some contend that words and phrases cannot be defined with absolute certainty.[124] Vagueness "does not invalidate every statute which a reviewing court believes could have been drafted with greater precision."[125] The Supreme Court concedes that "[m]any statutes will have some inherent vagueness, since '(i)n most English words and phrases there lurk uncertainties.'"[126] Furthermore, police must retain the ability make split-second decisions on duty, and prosecutors must maintain their ability to use discretion in order to function effectively.[127] However, the Due Process clause only requires that laws give fair warning so citizens can avoid prohibited conduct.[128] It is not reasonable to expect the ordinary person to know what behavior is forbidden under sections 752.795 and 752.797(6) because the various

---

[123] Kern suggests that Michigan's law allows the use of an unsecured wireless internet network if the network's owner has not put security measures in place, but he does not consider whether a user's authorization is valid. Kern, *supra* note 35, at 144-45.

[124] Waldron, *supra* note 106, at 522-26 (discussing philosophical models of meaning).

[125] Rose v. Locke, 423 U.S. 48, 49(1975).

[126] *Id.*at 49-50 (quoting Robinson v. United States, 324 U.S. 282, 286 (1945)).

[127] Markus Dirk Dubber, *Policing Possession: The War on Crime and the End of Criminal Law*, 91 J. CRIM. L. & CRIMINOLOGY 829, 839-40 (2001); Sa'id Wekili & Hyacinth E. Leus, *Police Brutality: Problems of Excessive Force Litigation*, 25 PAC. L.J. 171, 178 (1994); *see generally* John M. Allen, *Expanding Law Enforcement Discretion: How the Supreme Court's Post-September 11th Decisions Reflect Necessary Prudence*, 41 SUFFOLK U. L. REV. 587 (2008).

[128] *Rose*, 423 U.S. at 50 (finding that the phrase "crimes against nature" was not overly vague in a Tennessee statute).

ways "valid authorization" can be construed creates confusion and does not enable the members of the public to conform their behaviors to the law.

Sam Peterson, who accessed unsecured wireless internet from his car outside the Re-Union Street Café, probably did not violate the statute. Regardless of whether the café charged non-paying customers a fee,[129] Peterson accessed the café's wireless internet connection without hacking into it, and the network did not have security features enabled, such as a password.[130] Consequently, a user who accesses an open Wi-Fi network without circumventing security measures could reasonably think he or she has authorization to utilize the network.[131] According to section 752.797(6)(c), Peterson is free from the rebuttable presumption that he used the network with authorization because the network was not protected.[132]

Assuming that the Re-Union Street Café did charge non-customers a fee,[133] one could argue that Peterson had authorization but exceeded it by using the network without purchasing something from the café or paying the non-customer fee. However, he only broke the law if the café did not consider his authorization valid.[134] If network operators have a responsibility to secure their networks as Kern suggests,[135] and if ISPs place liability on the subscriber,[136] then the café is the party responsible for determining the validity of authorization to use the network. However, Sam Peterson would have had no way of knowing whether the Re-Union Street Café

---

[129] *See* discussion *supra* note 7.

[130] *See* Bonisteel, *supra* note 3.

[131] Kern, *supra* note 35, at 144-45. *See generally* Egilman v. Keller & Heckman, LLP, 401 F. Supp. 2d 105, 113 (D.D.C. 2005); I.M.S. Inquiry Mgmt. Sys. v. Berkshire Info. Sys., 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004).

[132] MICH. COMP. LAWS ANN. § 752.797(6)(c) (West 2004).

[133] *See* discussion *supra* note 7.

[134] *See* discussion *supra* pp. 21-23.

[135] Kern, *supra* note 35, at 144-45.

[136] Hale, *supra* note 37, at 555-56.

or its ISP considered his authorization valid. The Supreme Court in *City of Chicago v. Morales*, described an analogous situation in terms of Chicago's loitering law:

> The Illinois Supreme Court recognized that the term "loiter" may have a common and accepted meaning, . . . but the definition of that term in this ordinance —"to remain in any one place with no apparent purpose"—does not. It is difficult to imagine how any citizen of the city of Chicago standing in a public place with a group of people would know if he or she had an "apparent purpose." . . . [T]he vagueness that dooms this ordinance is not the product of uncertainty about the normal meaning of "loitering," but rather about what loitering is covered by the ordinance and what is not.[137]

Because of the statute's vague and subjective terms, Sam Peterson did not have fair notice that his behavior was unlawful. The fact that the police, the café owner, Peterson's lawyers, and Peterson were all unaware that Peterson's activities could be prosecuted under Michigan law is further evidence that the law does not provide fair notice of prohibited conduct.[138]

One could argue that the "person of ordinary intelligence"[139] would know what "valid authorization" means because word "valid" is in widespread use. However, the phrase "valid authorization" is not common, and ordinary people would not have a shared understanding of its meaning. [140] Additionally, the ordinary person cannot know whether she is or is not presumed to have exceeded authorization under section 752.797(6) since only one section of the statute refers to her authorization as being "valid." Even if the ordinary person could determine whether the term "valid" applied to 752.797(6), the word "valid" itself is undefined, making it difficult for the ordinary person to know which meaning to apply to the term. Furthermore, the phrase "valid

---

[137] 527 U.S. 41, 56-57 (1999)

[138] Bonisteel, *supra* note 3 (stating that Peterson consulted two lawyers, both of whom were unaware of the law, and quoting Peterson as saying "I do not understand how this is illegal."); Center, *supra* note 5 (quoting the café owner saying that she "didn't know it was really illegal, either"); *Internet Freeloader in Trouble*, *supra* note 1, at A1 (noting that the Police Chief "didn't accuse Peterson immediately because he wasn't certain Peterson was breaking the law" and Peterson himself "was floored").

[139] *See* Grayned v. City of Rockford, 408 U.S. 104, 108 (1972).

[140] Goldsmith, *supra* note 20, at 299-300 (stating that the Supreme Court has upheld some criminal statutes because they contain "commonly understood" terms).

authorization" is not given meaning through context because a computer can be accessed in or out of a workplace, and through a secured or unsecured network.[141]

Michigan's statute is void for vagueness because the phrase "valid authorization" has two distinct interpretations, is undefined in the statute, has no legal meaning, and is not given any context by the statute. What facts create "valid authorization" are uncertain, and the statute provides no standard to objectively determine validity. Under the statute, a person walking in downtown Lansing, Michigan, whose Wi-Fi cell phone hops from one unsecured wireless internet network to another, may be "exceeding valid authorization" because, though she did not hack into a network, her authorization might not be "valid" to a third party. It is also difficult for computer users to know which third party has the right to establish "valid authorization." As with the term "authorization," Michigan's computer crime statute does not provide examples of criminal conduct or reasonably define how one exceeds "valid authorization."[142] The term "valid" is subjective because a third party such as the Re-Union Street Café must determine what "valid" means. Therefore, citizens do not have fair notice and cannot modify their actions to comply with the law.

b. The Statute Does Not Provide Minimal Guidelines

i. The Statute Allows Too Much Discretion for Law Enforcement

Regardless of the fair notice element, section 752.795 of Michigan's computer crime statute is void for vagueness because it does not establish minimal guidelines for police and

[141] *See* Goldsmith, *supra* note 20, at 300 (suggesting that context can provide meaning in limited situations). Goldsmith also suggests that prosecutors can give meaning to words in a statute depending on how they enforce it. *Id.* at 300-01. However, law enforcement invokes Michigan's computer crime statute too rarely to be of help. SCOTT & SHIELDS, *supra* note 40, at 51-2 (stating that there have been few reported prosecutions under this statute); Center, *supra* note 5 (stating that Kent County prosecutors had not charged anyone for piggybacking on Wi-Fi before Sam Peterson in 2007).

[142] *See also* Wheeler, *supra* note 76, at 485-86 (discussing this issue in relation to a Minneapolis, Minnesota city ordinance).

prosecutors. The minimal guidelines element exists to prevent arbitrary and discriminatory enforcement.[143] According to *Morales*, a statute may be vague if it "fails to establish standards for the police and public that are sufficient to guard against the arbitrary deprivation of liberty interests."[144] Michigan's computer crime statute does not include a standard by which law enforcement can determine whether a Wi-Fi user has authorization or has exceeded authorization to use the service. Given that an unauthorized network user who successfully connects to an open Wi-Fi signal is using the service like any authorized user, police cannot ascertain who has authorization or who has exceeded authorization by simple observation. For example, the police only knew Sam Peterson was connected to the Re-Union Street Café's internet network because he said so.[145] Peterson could have been playing solitaire or writing a letter to his mother, neither of which required a network connection. Peterson could also have had internet access on his laptop through a cell phone network or his car;[146] neither of which would have been evident or distinguishable from a Wi-Fi connection from the café.

Because the only way to discover someone using a Wi-Fi network without authorization is to catch them in the act,[147] and because it is not obvious whether a computer user has accessed a Wi-Fi network without authorization, police must use their best guesses as to whether someone is breaking the law. However, this violates the Fourth Amendment because it allows police to

---

[143] *Id.* at 473-74.

[144] City of Chicago v. Morales, 527 U.S. 41, 52 (1999) (citing Kolender v. Lawson, 461 U.S. 352, 358, (1983)). Both cases deal with anti-loitering laws. *Id.*

[145] *Internet Freeloader in Trouble*, *supra* note 1, at A1. Police Chief Milanowski "didn't accuse Peterson immediately because he wasn't certain Peterson was breaking the law, but he figured some charge had to be on the books." *Id.*

[146] Fred Johnson, *Get Online with a Cell Phone*, MACWORLD, Nov. 2005, at 80-82 (explaining how to use a cell phone as a modem connected to a laptop computer); Doug Newcomb, *Chrysler Brings 'Infobahn' to Autobahn*, WIRED.COM, Jun. 21, 2008, http://www.wired.com/cars/coolwheels/news/2008/06/car_internet (describing Chrysler's UConnect system that creates a Wi-Fi hotspot in and around a car).

[147] Center, *supra* note 5 (quoting Kent County Assistant Prosecutor Lynn Hopkins as saying, "90 percent of the time we wouldn't know, frankly, that [piggybacking is] going on.").

arrest Wi-Fi users "for suspected conduct rather than for observable conduct."[148] Many anti-loitering laws have been struck down for the same reason.[149] Though an officer who has a reasonable suspicion based on "specific and articulable facts" may conduct a search according to *Terry v. Ohio*,[150] if there are no articulable facts to indicate that a Wi-Fi user is breaking the law and no guidelines in the statute to assist police, then the law may be arbitrarily enforced.

Conversely, law enforcement can arbitrarily enforce a vague statute by ignoring certain behavior .[151] If a police officer cannot reasonably determine that a Wi-Fi user has accessed the network without authorization, or if the officer is not concerned about a Wi-Fi user's activities, the officer can decide the law does not apply.[152]

Because the use of a Wi-Fi network without authorization is unobservable, a violation of the statute is indistinguishable from a legal use of a Wi-Fi network. Thus, Michigan's statute gives the police too much discretion since they can choose to ignore possible violations of the statute or choose to target every laptop user sitting in public places.

---

[148] Wheeler, *supra* note 76, at 489-90 (citing Newsome v. Malcolm, 492 F.2d 1166, 1173 (2d Cir. 1974) and Farber v. Rochford, 407 F. Supp. 529 (N.D. Ill. 1975)).

[149] *See* Papachristou v. Jacksonville, 405 U.S. 156 (1972) (striking down a City of Jacksonville vagrancy ordinance); Palmer v. Euclid, 402 U.S. 544 (1971) (finding city of Euclid, Ohio's suspicious person ordinance unconstitutionally vague); Newsome v. Malcolm, 492 F.2d 1166 (2d Cir. 1974) (invalidating a New York anti-loitering law); Chicago v. Youkhana, 660 N.E.2d 34 (Ill. App. 1995) (striking down a Chicago anti-loitering ordinance).

[150] 392 U.S. 1, 21 (1968).

[151] Forde-Mazrui, *supra* note 86, at 1517.

[152] *See id.*

ii. The Lack of Definition for "Authorization" Encourages Arbitrary Enforcement

Few states define "authorization" in their computer crime statues,[153] and courts rarely interpret unauthorized access statutes.[154] However, the term "authorization" is essential to a computer misuse statute. For example, in *Commonwealth v. Cocke*, Kentucky's Court of Appeals held one section of the Kentucky statute outlawing unauthorized computer access void for vagueness because the statute did not distinguish between the authorized and unauthorized altering, damaging, or destroying of data.[155] The court stated that "absent a requirement that the actor's alteration, damage or destruction must occur without authorization, the statute literally permits the prosecution of an authorized user for an alteration as innocuous and innocent as the deletion of an e-mail message."[156] Therefore, it is crucial to include the term "authorization" when appropriate, and necessary to define the term to ensure clarity.[157]

Michigan's statute does not explicitly define the term "authorization" in section 752.795, but section 752.797(6) uses a rebuttable presumption to indirectly establish meaning. [158] This section states that users are free of the rebuttable presumption that they are unauthorized or have exceeded authorization to use a computer network if: (1) they have written or oral permission by the owner; (2) the computer system tells them it is in the public domain; or (3) they access the

---

[153] Matthew Bierlein, *Policing the Wireless World: Access Liability in the Open Wi-Fi Era*, 67 OHIO ST. L.J. 1123, 1142 n.99 (2006).
[154] *Id*. at 1160 n.189 (listing cases in all states where courts have interpreted unauthorized access statutes).
[155] 58 S.W.3d 891, 894 (Ky. Ct. App. 2001).

[156] *Id*.

[157] Kerr notes that much of the literature assumes the term "authorization" is obvious in meaning. Kerr, *supra* note 65, at 1598 n.10. However, some courts have acknowledged that the term's meaning "has proven to be elusive." *Id*. at 1600 n.16 (citing EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001)).

[158] MICH. COMP. LAWS ANN. § 752.797(6) (West 2004). Other states that use a rebuttable presumption to indirectly define "authorization" are Illinois (720 ILL. COMP. STAT. 5/16D-7 (West 2003)) and Louisiana (LA. REV. STAT. ANN. § 73.7(B)(2) (2006)).

computer system without hacking into it.[159] However, a rebuttable presumption is not the same as defining "authorized"—it only releases defendants from the presumption that they were not authorized without actually identifying a meaning for the term. One can assume that "unauthorized" would mean that one or more of these three conditions did not exist, though this term is not explicitly defined either. The lack of a straightforward definition of "authorization" opens the door for law enforcement to arbitrarily and discriminatorily enforce the statute.[160]

For example, police are likely to use Michigan's computer crime law to prosecute some crimes and not others. In *People v. Golba*, the defendant was convicted under section 752.795 of accessing a school computer intentionally and without authorization, or by exceeding "valid authorization" by sending sexually explicit e-mail to a minor student and violating the school's computer use policy.[161] Golba accessed the computer without hacking into it, so he was not presumed to have been "unauthorized" under section 752.797(6)(c).[162] The trial court construed Golba's breach of the school's terms of computer use as an unauthorized act, and the Michigan Court of Appeals affirmed this decision.[163] Along these same lines, a college student who violates her college's computing terms of use is also guilty under section 752.795 when she downloads a song from a peer to peer file sharing network.[164] Both have committed a felony

---

[159] MICH. COMP. LAWS § 752.797(6) (West 2004).

[160] Ned Snow, *The Law of Computer Trespass: Cyber Security or Virtual Entrapment?* 2007 ARK. L. NOTES 109, 111 (2007) (arguing that the use of unsecured Wi-Fi networks without permission has become an accepted societal practice and punishing that activity invites prosecutorial abuse).

[161] 729 N.W.2d 916, 923.

[162] *Id.* (stating that Golba's act of accessing a computer to send sexually explicit email to a student was contrary to the school's computer use policy and sufficient to sustain his conviction under section 752.795).

[163] *Id.*

[164] Kalamazoo College, Information Technology Services: Prohibited Uses (Oct. 1, 2008), http://reason.kzoo.edu/is/policies/prohibited_uses/ [hereinafter Kalamazoo College] (stating that "users of the Kalamazoo College network may not use peer-to-peer file sharing programs, including, but not limited to, Kazaa, Gnutella, Morpheus, Audiogalaxy Satellite, Win MX, etc."). Peer to peer file sharing networks allow users to

according to the statute,[165] but authorities are probably more likely to prosecute the sex offender than the student from an affluent private college because of socioeconomic factors and the seriousness of the crime. [166] Certainly, law enforcement cannot possibly catch every statutory violation, but colleges routinely receive warnings from the Recording Industry Association of America (RIAA) about peer to peer file sharing violations on their campuses,[167] so interested prosecutors could easily determine which students are violating the statute. A sex offense may be a more egregious crime, but under the statute the abuse of computing resources is the same regardless of purpose.

Some may argue that law enforcement should conserve its resources for the worst offenses, such as sex offenses, rather than expending time and money on less significant illegal acts. However, after Sam Peterson's arrest, the police staked out the café area to enforce the statute rather than focusing on more substantial crimes. The same police officers that arrested Peterson caught another man outside the Re-Union Street Café using the café's Wi-Fi from his car.[168] The police called the café owner, Donna May. She asked to speak to the man and advised him that "he should tell the police he'd used the café restroom and asked her permission to use her Wi-Fi from his car. The man, in turn, told this to the policeman who was, according to

download music from the computers of other users. Neil Strauss, *Online Fans Start to Pay the Piper*, N.Y. TIMES, Sept. 25, 2002, at E1.

[165] MICH. COMP. LAWS ANN. § 752.797(2) (West 2004).

[166] *See generally* GREGG BARAK, PAUL LEIGHTON & JEANNE FLAVIN, CLASS, RACE, GENDER, AND CRIME: THE SOCIAL REALITIES OF JUSTICE IN AMERICA *passim* (2d ed. 2006) (discussing the impact of race, class, and gender on criminal prosecution and how these factors structure society's view of crime); SCOTT, *supra* note 56, at 513-24; SCOTT & SHIELDS, *supra* note 40, at 24-1 to 24-11 (discussing federal prosecutorial discretion for computer crimes, including factors such as the nature and seriousness of the offense).

[167] John Schwartz, *More Lawsuits Filed In Effort to Thwart File Sharing*, N.Y. TIMES, Mar. 24, 2004, at C4.

[168] Gibbs, *supra* note 7, at 34.

May, rather annoyed and said that they wouldn't refer such cases to May in future."[169] May never pressed charges against Peterson and apparently was not concerned about the public using her Wi-Fi network.[170] However, law enforcement appeared to be concentrating their efforts on one particular kind of network user despite the fact that the network owner was unconcerned about the issue. This situation exemplifies the arbitrary enforcement the vagueness doctrine attempts to eliminate.

These scenarios also show that law enforcement cannot reasonably rely on network owners to define "authorization." First, network owners may not enforce their own policies consistently.[171] For instance, a business owner who forgives one employee for breaching the company's computer use policy may retaliate against a different employee. Furthermore, computer use policies at businesses or educational institutions can be badly written, inconsistent, or nonexistent.[172] Some policies use the term "unauthorized" but, like the statute, do not define the word or explain who determines when conduct is authorized.[173] In these cases, courts must

---

[169] *Id.*

[170] *Id.*

[171] *See* William A. Herbert, *The Electronic Workplace: To Live Outside the Law You Must be Honest*, 12 EMP. RTS. & EMP. POL'Y J. 49, 71-72 (2008) (citing Doe v. XYC Corp., 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005), where the employer did not enforce its policy consistently); Jamila Johnson, *Employee Internet Misuse: How Failing to Investigate Pornography May Lead to Tort Liability*, 4 SHIDLER J. L. COM. & TECH. 1, para. 22, 24-28 (2007) (discussing an employer's duty to investigate suspected violations of its computer use policy).

[172] *See* Kelley Baker, *Public Schools and the Internet*, 79 NEB. L. REV. 929, 951-54 (2000) (suggesting clear language for public school computer use policies); Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1643 n.11 (1995) (noting that some schools within the University of Pennsylvania prohibit anonymous messages while others do not); Sharon Burger, *Heads Up: Attorney-Client Privilege Meets E-mail*, 51 B.B.J. 5, 6 (2007) (citing TransOcean Capital, Inc. v. Fortin, 21 Mass. L. Rptr. 597 (Mass. Super. Ct., Oct. 18, 2006), where the employer relied on a third party's policy); AMERICAN MANAGEMENT ASSOCIATION, 2005 ELECTRONIC MONITORING & SURVEILLANCE SURVEY 3 (2005) http://www.amanet.org/research/pdfs/EMS_summary05.pdf (documenting that sixteen to eighty percent of employers surveyed had not established computer use policies for specific uses of the internet).

[173] *See* Albion College Library Public Access Computer-Use Policy (Nov. 10, 1999), http://www.albion.edu/library/computer_use_policy.asp (restricting "unauthorized access to computing resources or accounts"); Kalamazoo College, *supra* note 169 (stating that "[u]nauthorized reading, copying, deletion or modification of someone else's data or electronic mail, unauthorized use of another person's password, or distribution of a personal account password is not allowed"); Lake Michigan College, Acceptable Use Policy

speculate about what behavior might be authorized by a particular institution and, in the case of a place of business without a policy, who might authorize it. This encourages courts to legislate, promotes inconsistent enforcement of the law, and is evidence that the term "authorization" should be more clearly defined.[174]

Only four Michigan Court of Appeals cases mention this statute,[175] and in all four cases the court seems to define authorization in terms of the permissions given to the defendant by the employer.[176] In *People v. Schilke*, No. 253117, 2005 WL 1027039 (Mich. Ct. App. May 3, 2005), the court found the defendant guilty of unauthorized access for accessing her work computer from home after her termination, changing the administrative password, and deleting files.[177] In *People v. Golba*, the defendant sent sexually explicit e-mail to a minor student and violated a school's policy of unacceptable computer use.[178] But in *People v. Helleman*, the court found the defendant was not unauthorized to access his work computer after he was fired

---

(Aug. 8, 2008), http://www.lakemichigancollege.edu/index.php?option=com_content&task=view&id=2260&Itemid=2293 (making "[a]ny attempt to gain unauthorized access to information" a violation of the policy); Michigan Technological University Computer Use Policy (Aug. 8, 2001), http://www.cec.mtu.edu/cacsec/info/cup_approved.html (stating that individuals may not "engage in unauthorized conduct to place MTU in the position of being considered a service provider for third parties.").

[174] *See* Alex Hortis, Note, *Valuing Honest Services: The Common Law Evolution of Section 1346*, 74 N.Y.U. L. REV. 1099, 1110 (1999) (contending that critics and courts found the federal mail fraud statute "so vague that it forces federal courts to define the statute's terms and legislate the offense from the bench."); *see e.g.* Kenneth J. Schweiker, Comment, *Military Chaplains: Federally Funded Fanaticism and the United States Air Force Academy*, 8 RUTGERS J. L. & RELIGION 5, 28 n.108 (2006) (citing other instances where indistinct statutory language could require courts to act beyond their power).

[175] A fifth case only deals with the statute tangentially, but seems to disregard the rebuttable presumption in section 752.797(6) because the court found that the plaintiff failed to show that the defendant accessed the plaintiff's email without authorization. Martinez v. Mueller, No. 266200, 2006 WL 1115534, at *3 (Mich. Ct. App. Apr. 27, 2006).

[176] Though the court might have narrowed the definition of "authorization" through these decisions, it did not do so. *See* Edward Comitz, Comment, *Extinguishing the Burning Crosses: Washington's Malicious Harassment Statute in Light of the Issues of Overbreadth and Vagueness*, 16 U. PUGET SOUND L. REV. 373, 386-87 (1992) (stating that the Supreme Court has been willing to allow state courts to narrow overbroad statutes); Goldsmith, *supra* note 20, at 295 (stating that federal courts can narrow federal legislation);.

[177] *Id.*

[178] 729 N.W.2d 916, 923 (2007).

because he was allowed to access his computer without supervision after his termination.[179] The employer's computer use policy, if any, was overridden by the employer's actions in allowing the defendant to use his work computer after he was fired. In *People v. Brunk*, the court found the defendant had general authority to access the State's computer network and authority to retrieve certain files in the course of his employment even though he lacked a work order to do so.[180] Here, the employer had no policy stating whether the defendant could or could not act in the way he did.[181] These cases demonstrate that a third party's policies may be unclear, nonexistent, or overridden by its own actions. Therefore, the definition of "authorization" cannot depend on the policies of third parties because this leads to arbitrary enforcement.

Michigan's statute gives too much discretion to law enforcement, and is void for vagueness because it does not explicitly define the term "authorization" or at least give examples of prohibited behavior.[182] Law enforcement currently relies on third parties to give meaning to the term "authorization," because it is not a clear standard for them to follow. The lack of guidelines for determining when one is unauthorized or when one has exceeded authorization to access a computer network creates an opportunity for arbitrary enforcement of the statute.

---

[179] No. 217190, 2001 WL 1352355, at *2 (Mich. Ct. App. Sept, 10, 2001). In this case, the court seems to contradict the essence of having a rebuttable presumption in stating that the prosecution "failed to establish a presumption of unauthorized access in accordance with subsection 7(3)." *Id.*

[180] No. 273858, 2008 WL 376421, at *4 (Mich. Ct. App. Feb. 12, 2008).

[181] *Id.* at *3.

[182] *See* Wheeler, *supra* note 76, at 471 (stating that "[l]oitering legislation is particularly prone to judicial disapproval where the legislature fails to sufficiently define or give examples of loitering so as to give the public notice of prohibited conduct and to narrow law enforcement discretion.").

IV. SOLUTIONS

a. Eliminate the Term "Valid"

The legislature should eliminate the term "valid" from section 752.795 because it does not add meaning to the term "authorization." If the phrase "valid authorization" is essential to the statute, then the legislature should define it and give examples of valid authorization directly in the statute.[183] However, since the term only appears in section 752.795 and not section 752.797(6), it is unlikely that the legislature would consider it crucial for the interpretation of the statute. Eliminating the word "valid" would solve the fair notice issue in interpreting the statute.

b. Clearly define "Authorization" and "Exceeding Authorization"

The legislature should define the terms "authorization" and "exceeding authorization" to discourage arbitrary enforcement of the statute. This definition should also include a reference to third parties that could determine authorization.[184] Though many states have statutes that prohibit unauthorized access to computers,[185] most have not defined "authorization" or "without authorization"[186] However, some have done so sufficiently. For example, North Carolina's statute defines "authorization" as "having the consent or permission of the owner, or of the person licensed or authorized by the owner to grant consent or permission to access a computer,

---

[183] See *id.*

[184] *See generally* People v. Lueth, 660 N.W.2d 322 (Mich. Ct. App. 2002) (holding that a statute is not vague because it refers to third party rules to define prohibited conduct).

[185] Max Stul Oppenheimer, *Internet Cookies: When is Permission Consent?* 85 NEB. L. REV. 383, 397 n.82 (2006) (listing states with unauthorized access statutes). For a handy list of state computer hacking laws, *see* National Conference of State Legislatures, Computer Hacking and Unauthorized Access Laws (Mar. 10, 2006), http://www.ncsl.org/programs/lis/CIP/hacklaw.htm.

[186] Kerr, *supra* note 65, at 1623-24. California's statute, which does not define "authorized," was challenged as vague and upheld. Hawkins v. Cavalli, No. C 03-3668 PJH, 2006 WL 2724145, at *7-9 (N.D. Cal. Sept. 22, 2006). Wisconsin's unauthorized access statute was also upheld on the challenge that it did not define "without authorization." State v. Corcoran, 522 N.W.2d 226, 232-33 (Wis. App. 1994). Conversely, the Kentucky Court of Appeals found that state's statute void for vagueness because it did not differentiate between authorized and unauthorized access. Commonwealth v. Cocke, 58 S.W.3d 891, 893 (Ky. Ct. App. 2001). The Ohio Court of Appeals expressed concerns about that state's unauthorized access statute failing fair notice and arbitrary enforcement, but did not address the issue on appeal. State v. Washington, 710 N.E.2d 307, 316 (Ohio App. 2 Dist. 1998).

computer system, or computer network in a manner not exceeding the consent or permission."[187] Unfortunately, the statute does not describe how one would exceed consent or permission. Likewise, Minnesota's statute simply defines "authorization" as "with the permission of the owner of the computer, computer system, computer network, computer software, or other property."[188] However, the statute refines the definition by allowing the computer owner to limit authorization by "(1) giving the user actual notice orally or in writing; (2) posting a written notice in a prominent location adjacent to the computer being used; or (3) using a notice displayed on or announced by the computer being used."[189]

Colorado's statute only considers express consent. It defines "authorization" as "the express consent of a person which may include an employee's job description to use said person's computer, computer network, computer program, computer software, computer system, property, or services. . . ."[190] This definition takes into account how an employer might limit a computer user's authorization, but it does not consider any implied permissions. However, the same law specifies how a user would exceed his or her authorization. According to the Colorado statute, "exceeding authorized access" is "to access a computer with authorization and to use such access to obtain or alter information, data, computer program, or computer software that the person is not entitled to so obtain or alter."[191] These definitions take into account both users without permission from network owners as well as users with permission who abuse their

[187] N.C. GEN. STAT. ANN. § 14-453(1a) (West 2007).

[188] MINN. STAT. ANN. § 609.87(2a) (West 2003 & Supp. 2008).

[189] *Id.*

[190] COLO. REV. STAT. § 18-5.5-101(1) (2004).

[191] COLO. REV. STAT. § 18-5.5-101(6.7) (2004).

privileges. Though Michigan's statute attempts to do the same,[192] Colorado's definitions are clearer because they are explicit.

Unlike Colorado, North Carolina, and Minnesota, some states incorporate both express and implied consent. In Utah's statute, "authorization" means "having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission."[193] Similarly, West Virginia (and New Hampshire, with minor modifications) defines "authorization" as "the express or implied consent given by a person to another to access or use said person's computer, computer network, computer program, computer software, computer system, password, identifying code or personal identification number."[194]

Other states add a reasonable person standard to include situations the definition might not consider. For example, New Jersey's statute defines "authorization" as:

> [P]ermission, authority or consent given by a person who possesses lawful authority to grant such permission, authority or consent to another person to access, operate, use, obtain, take, copy, alter, damage or destroy a computer, computer network, computer system, computer equipment, computer software, computer program, computer storage medium, or data. An actor has authorization if a reasonable person would believe that the act was authorized.[195]

This definition also takes into account that the permission, authority, or consent must be lawful.

---

[192] MICH. COMP. LAWS ANN. § 752.797(6) (West 2004).

[193] UTAH CODE ANN. § 76-6-702(2) (2003 & Supp. 2008).

[194] W. VA. CODE ANN. § 61-3C-3(b) (LexisNexis 2005). New Hampshire's code contains two minor variations on West Virginia's code, omitting the term "computer system" and placing a comma between "code" and "or." N.H. REV. STAT. ANN. § 638:16(II) (2007).

[195] N.J. STAT. ANN. § 2C:20-23(q) (West 2005).

New York's statute, though not straightforward, has a scienter requirement.[196] Its statute defines what it means to be "without authorization":

> "Without authorization" means to use or to access a computer, computer service or computer network without the permission of the owner or lessor or someone licensed or privileged by the owner or lessor where such person knew that his or her use or access was without permission or after actual notice to such person that such use or access was without permission. It shall also mean the access of a computer service by a person without permission where such person knew that such access was without permission or after actual notice to such person, that such access was without permission.
>
> Proof that such person used or accessed a computer, computer service or computer network through the knowing use of a set of instructions, code or computer program that bypasses, defrauds or otherwise circumvents a security measure installed or used with the user's authorization on the computer, computer service or computer network shall be presumptive evidence that such person used or accessed such computer, computer service or computer network without authorization.[197]

This kind of definition protects against the user who unwittingly accesses a computer network without authorization.[198] Unfortunately, it requires law enforcement to show that the user knew or had notice that her access was without permission.[199] This may not deter police from arbitrarily enforcing this statute, since police cannot identify what a user knows unless that user has actual notice. On the other hand, it may deter arbitrary prosecution because it is more difficult to successfully prosecute a crime when law enforcement must prove what a suspect knew.

---

[196] N.Y. PENAL LAW § 156.00(8) (McKinney 1999 & Supp. 2008).

[197] *Id.*

[198] *See generally* Ethan Preston, Note, *Finding Fences in Cyberspace: Privacy, Property and Open Access on the Internet*, 6 J. TECH. L. & POL'Y 57, 91 (2001) (noting that a few state statutes take into account users who "reasonably believed that they were authorized or could not have known they were unauthorized.").

[199] N.Y. PENAL LAW § 156.00(8) (McKinney 1999 & Supp. 2008). The first paragraph of the statute criminalizes a person accessing a computer where he or she "knew that his or her use or access was without permission or after actual notice to such person that such use or access was without permission." *Id.*

Professor Kerr suggests that these statutes should restrict the scope of "authorization" to code-based circumvention of computer security (hacking) rather than breaches of computer use contracts.[200] This allows users to utilize the internet and other computer networks without possible criminal sanctions from breaching "terms of use" contracts.[201] According to Kerr, contract law and traditional criminal laws would still apply, but unauthorized computer use laws "would no longer threaten to transform disagreements with computer owners into criminal violations."[202] If applied in Michigan, this would only provide Wi-Fi owners protection from piggybackers who hacked into their network. Wi-Fi network owners would be responsible for protecting their signals with passwords or other security if they did not want them to be publicly available.[203] On the other hand, technologies that routinely use unsecured Wi-Fi networks, such as Wi-Fi cell phones, would not violate such a statute. Though some states are moving away from putting the onus on the Wi-Fi network owner,[204] as these technologies become more prevalent it makes sense to ensure the law does not criminalize ordinary behavior.[205]

---

[200] Kerr, *supra* note 65, at 1649-50.

[201] *Id*. at 1651. Federal courts have found unauthorized access through violations of "terms of service" agreements without relying on federal law to define "unauthorized." Hale*, supra* note 37, at 545-46.

[202] Kerr, *supra* note 65, at 1651.

[203] Snow, *supra* note 160, at 111 (arguing that the law should only punish unauthorized use if a network owner has not implemented security measures). The Maryland public defender's office used the same argument in opposing a bill criminalizing intentional use of a wireless internet connection without permission. Schotz, *supra* note 16.

[204] Before 2006, New York's statute provided protection only when a network owner implemented security measures, but the state revised its statute in 2006 to include unsecured computers and networks. 2006 Sess. Law News of N.Y., 229th Leg., Ch. 558 (A. 891-F) (McKinney 2006). Similarly, New Hampshire introduced a bill in 2003 that explicitly put the responsibility of encryption on the wireless network owner. An Act Relative to Unauthorized Access to a Wireless Computer Network, H.B. 495, 2003 Leg., 158th Sess. (N.H. 2003), *available at* http://www.gencourt.state.nh.us/legislation/2003/HB0495.html. The bill attempted to "protect those who innocently stumble upon insecure wireless networks." Brian McWilliams, *Licensed to War Drive in N.H.,* WIRED.COM, Apr. 29, 2003, http://www.wired.com/gadgets/wireless/news/2003/04/58651?currentPage=all. The bill passed the state house but not the senate. 29 N.H. House Journal (Mar. 25, 2003), *available at* http://www.gencourt.state.nh.us/house/caljourns/journals/2003/houjou2003_12.html; 22 N.H. Senate Journal 877 (Sept. 4, 2003), *available at* http://www.gencourt.state.nh.us/scaljourns/Journals/2003/SJ%2023.pdf. The bill may have duplicated or weakened existing legislation, but why it did not pass is ultimately unclear. Patrick S. Ryan, *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, 9 VA. J.L. & TECH. 7, ¶. 62, n.193 (2004) (citing Posting of Orin Kerr on Would a New Hampshire Bill Really Legalize War Driving? to The Volokh Conspiracy, http://volokh.com/2003_04_27_volokh_archive.html#200223941 (Apr.

There are several pros and cons to this approach. Two arguments in support of this proposal are: 1) encouraging access to the internet through unsecured Wi-Fi networks increases its value and furthers the public good,[206] and 2) Wi-Fi owners can combat piggybacking by closing the network at any time with built-in security measures.[207] The internet abounds with free advice on securing Wi-Fi networks,[208] and companies that make wireless home routers have step-by-step information available as well.[209] On the other hand, an outside party using Wi-Fi resources can compromise network performance for the Wi-Fi network owner and the risk of passing viruses from one computer to another increases.[210] Furthermore, the ordinary person may not have the technical expertise to apply security measures to their home or business Wi-Fi network, or just may not take the time to do so.[211]

Another argument in support of making network owners responsible for security is that network owners may rely on laws that protect Wi-Fi networks against unwanted access and they may fail to take appropriate action to secure their network if not encouraged by the law to do

---

27, 2003, 14:12 PST) (suggesting the bill would have no effect)); Brian McWilliams, *Licensed to War Drive in N.H.,* WIRED.COM, Apr. 29, 2003 http://www.wired.com/gadgets/wireless/news/2003/04/58651?currentPage=all (quoting a New Hampshire legislator concerned about undercutting the existing statute).

[205] Snow, *supra* note 160, at 111 (suggesting that using unsecured Wi-Fi without explicit permission has become a social norm).

[206] *Id.* at 110.

[207] Anita Ramasastry, Jane K. Winn & Peter Winn, *Will Wi-Fi Make Your Private Network Public? Wardriving, Criminal and Civil Liability, and the Security Risks of Wireless Networks*, 1 SHIDLER J. L. COM. & TECH. 9, ¶ 26-30 (2005), *available at* http://www.lctjournal.washington.edu/Vol1/a009Ramasastry.html; Ryan, *supra* note 204, at ¶ 4; Kern, *supra* note 35, at 112; Snow, *supra* note 160, at 111.

[208] Bradley Mitchell, *10 Tips for Wireless Home Network Security*, ABOUT.COM, http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm (last visited Oct. 26, 2008); How to Secure a Wireless LAN (WLAN), DAILY WIRELESS, Feb. 15, 2007, http://www.dailywireless.com/features/secure-wireless-lan-021507/; Becky Waring, *How to Secure Your Wireless Network*, PC WORLD, Apr. 9, 2007, http://www.pcworld.com/article/130330/how_to_secure_your_wireless_network.html.

[209] Linksys.com,Learning Center/Network Security/How to Secure Your Network, http://tinyurl.com/3bhmn3 (last visited Nov. 8, 2008).

[210] Ned Snow, *Accessing the Internet Through the Neighbor's Wireless Internet Connection: Physical Trespass in Virtual Reality*, 84 NEB. L. REV. 1226, 1244-46 (2006).

[211] Ryan, *supra* note 204, at ¶108.

so.[212] Moreover, some argue that by leaving a network unsecured, a network owner may be signaling that it is acceptable for anyone to use it,[213] or that Wi-Fi radio waves encroaching on their property entitles them to use the network.[214] Conversely, others contend that this is analogous to leaving a car unlocked with the keys in the ignition or the front door of a house wide open;[215] though these situations may facilitate trespass or theft, the owner's carelessness does not negate the crime. The circumstances are the opposite for Wi-Fi. Because some network owners purposely leave their networks unsecured for others to use—unlike cars and houses—the carelessness of the network owner should negate the crime. Furthermore, security measures for Wi-Fi are turned on once, unlike car or house doors that are routinely locked and unlocked.

Another argument against making the Wi-Fi network owner responsible for security is that network users can commit crimes (such as downloading child pornography or sending spam) from open Wi-Fi and it would track to the Wi-Fi owner.[216] However, federal legislators have recognized that network owners should not be responsible for the illegal activities of others.[217] Some also argue that legislation must protect internet service providers, such as phone and cable companies, from the theft of service that unsecured Wi-Fi can entail.[218] But internet service providers may be able to recover under cable television laws, either from subscribers or from manufacturers of wireless routers.[219]

---

[212] See Kern, *supra* note 35, at 112.

[213] Small, *supra* note 17, at 181.
[214] *Id*. at 182-83.

[215] Corbett, *supra* note 60, at 14; Small, *supra* note 17, at 184.
[216] Seth Schiesel, *Growth of Wireless Internet Opens New Path for Thieves*, N.Y. TIMES, Mar. 19, 2005, at A1; Ryan, *supra* note 204, at para. 8.

[217] Kern, *supra* note 35, at 115-16.
[218] Herrman, *supra* note 121, at 1096.
[219] *Id.* at 1125-29.

Making access to unsecured Wi-Fi networks presumptively legal "encourages network providers to take responsibility for enabling security mechanisms, mitigates user confusion, and promotes access."[220] It also ensures that the law does not criminalize everyday activities, as more gadgets rely on open Wi-Fi networks for their operations. Until other technologies such as 3G become more commonplace,[221] open Wi-Fi is the source for many mobile devices to find and use the internet.

Michigan's legislature should make the use of unsecured Wi-Fi presumptively legal[222] and take the best of other states' definitions to create a clear meaning for both "authorization" and "exceeding authorization." However, it is necessary to include language defining "exceeding authorized access" in a computer abuse statute to mitigate some of the concerns over a strict code-based definition of access. Though this may seem inconsistent because exceeding access implies a contractual relationship,[223] a definition of "exceeding authorized access" expands the statute and gives law enforcement muscle to pursue violations where a user did not hack into the system for initial access.[224] Therefore, a definition of "authorization" could read:

> "Authorization" means express or implied consent or permission of a person who possesses lawful authority to grant such permission, such as a computer or network owner or operator, or of a person approved by the owner to grant consent or permission, to access, operate, use, alter, or destroy said person's computer program, computer, computer system, or computer network without the use of a set of instructions, code, or computer program that bypasses, defrauds, or

---

[220] Bierlein, *supra* note 153, at 1123.

[221] 3G is a network technology that allows cell phones to access the internet without relying on Wi-Fi. Steven J. Vaughan-Nichols, 802.11 v. 3G (Jan. 31 2003), http://www.wi-fiplanet.com/tutorials/article.php/1577551. Even laptops can utilize 3G networks for internet access. *Wireless Laptop Access Solution Uses 3G Technologies*, 55 ELECTRONIC DESIGN 24 (2007).

[222] This presumptive approach differs from the explicit and unsuccessful approach other states have attempted. *See* An Act Relative to Unauthorized Access to a Wireless Computer Network, H.B. 495, 2003 Leg., 158th Sess. (N.H. 2003) *available at* http://www.gencourt.state.nh.us/legislation/2003/HB0495.html (stating that "[t]he owner of a wireless computer network shall be responsible for securing such computer network."); *see* discussion *supra* note 204.

[223] Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW 1395, 1420-21 (2007).

[224] *Id.* (suggesting scenarios that would not be encompassed in a strict code-based definition of "authorization.").

> otherwise circumvents the pre-programmed access procedure for the computer program, computer, computer system, or computer network. An actor has authorization if a reasonable person would believe that the act was authorized.

This definition of "authorization" identifies a person who has lawful authority to grant permission (or her agent), identifies what the authorized user can do and what they can access, specifies that the user cannot hack into the system, and includes a reasonable person standard to catch other scenarios. Similarly, the definition of "exceeding authorized access" could read:

> "Exceeding authorized access" means to access a computer program, computer, computer system, computer network, or services with authorization and to use such access to obtain or alter information, data, computer programs, computers, computer systems, or computer networks that the person is not entitled to so obtain or alter according to a person who possesses lawful authority to grant such authorization, or of a person approved by the owner to grant authorization. An actor has exceeded authorization if a reasonable person would believe that the act had exceeded authorization.

Michigan's recently introduced bills take a step toward reducing arbitrary enforcement by including explanations of "authorized user,"[225] but it is still imperative to incorporate a definition of "authorization" and "exceeding authorization." This helps solve the arbitrary enforcement issue in interpreting the statute because these definitions provide guidelines for law enforcement, such as identifying a person who has lawful authority to grant permission (or their agent), categorizing what the authorized user can do and what they can access, and specifying that the user cannot hack into the system. By making access to an unsecured Wi-Fi network presumptively legal, law enforcement also does not have responsibility for preventing users from piggybacking on open networks. This would solve the arbitrary enforcement issue.

[225] S. 144, 94th Leg., Reg. Sess. (Mich. 2007), *available at* http://www.legislature.mi.gov/documents/2007-2008/billintroduced/Senate/pdf/2007-SIB-0144.pdf; S. 145, 94th Leg., Reg. Sess. (Mich. 2007), *available at* http://www.legislature.mi.gov/documents/2007-2008/billintroduced/Senate/pdf/2007-SIB-0145.pdf.

c. Eliminate Section 752.797(6)

The legislature should eliminate the rebuttable presumption in section 752.797(6). This section is problematic for a number of reasons. First, it seems to define "authorization" in a backhanded way, but is ultimately unclear. Second, the rebuttable presumption itself may be unconstitutional because it could violate the constitutional presumption of innocence.[226] Therefore, the legislature should eliminate section 752.797(6) altogether and instead amend section 752.792 to include definitions of "authorization" and how one exceeds authorization, as suggested above. Some commentators contend that removing the phrase "rebuttable presumption" and replacing it with the phrase "it may be inferred" converts the mandatory presumption into a constitutionally acceptable permissive inference.[227] However, given that the term "authorization" should be defined more clearly anyway, it would be extraneous to preserve the rebuttable presumption in section 752.797(6) in any form.

V. CONCLUSION

Michigan's current computer crime statute is void for vagueness because it does not define "valid authorization" or the term "authorization" itself. Therefore, the statute should be amended to define key terms and eliminate extraneous language. The vagueness doctrine focuses on two issues: fair notice and arbitrary enforcement of the law.[228] The term "valid" is vague because it has multiple meanings. This creates a fair notice issue, since the ordinary person cannot know how it should be interpreted in the statute. This is especially true for unsecured Wi-Fi networks, where users could be violating the statute according to how the term

[226] Kerr, *supra* note 65, at 1624 n.110.

[227] Gottfried, *supra* note 65, at 723.

[228] Batey, *supra* note 22, at 4.

"valid" is defined by third parties. Additionally, the lack of a definition for "authorization" encourages arbitrary and discriminatory enforcement of the statute because there are no guidelines for police and prosecutors that help them enforce the law consistently. Users of unsecured Wi-Fi networks must rely on third parties to determine whether they are "authorized" as well. Simple elimination of extraneous language and rewording the statute to include definitions of "authorization" and "exceeding authorization" clarify the law and eliminate constitutional challenges.