

NOTE

COPYSense AND SENSIBILITY – HOW THE WIRETAP ACT FORBIDS UNIVERSITIES FROM USING P2P MONITORING TOOLS

*Catherine R. Gellis**

TABLE OF CONTENTS

I. INTRODUCTION.....	341
A. <i>The Question Raised</i>	341
B. <i>The Question’s Importance</i>	342
II. BACKGROUND	343
A. <i>The Nature and History of the Wiretap Act</i>	343
B. <i>The Technical Nature of Internet Communications</i>	345
1. Internet Architecture.....	345
2. Challenges to Administration of Internet-Connected Networks	346
3. CopySense Technology	347
C. <i>Peeling Back the Layers of Law and Technology</i>	349
III. ANALYSIS	351
A. <i>How the Language of the Wiretap Act Prohibits CopySense</i>	351
1. Through the Language Generally	351
2. Through the Meaning of “Interception”	352
3. Through the Meaning of “Communication”	354
4. Through the Meaning of “Contents” and “Device”	355
B. <i>How the Specific Exceptions Permitting Interception Do Not Apply</i>	356
1. The Ordinary Course of Business Exception.....	356
2. The Maintenance Exception	358
3. The Extension Telephone Exception	362
4. How No Other Applicable Exceptions Could Be Inferred	363
C. <i>How University Students Have a Reasonable Expectation of Privacy Warranting Wiretap Act Protection</i>	364
D. <i>How There is No Valid Consent to Permit the Universities’ Interception of Students’ Communications</i>	368

* B.A., Mass Communications and Sociology, 1996, University of California at Berkeley;
J.D., 2006, Boston University School of Law.

2006]	<i>COPYSENSE AND SENSIBILITY</i>	341
	1. There Is No Implied Consent	368
	2. Universities Should Not Be Able to Extract Express Consent to Justify Their Interceptions of All Student Internet Communications	369
	E. <i>How the Goals and Purpose of the Wiretap Act are Extensible to the Interception of Internet Communications</i>	370
IV.	CONCLUSION	371

I. INTRODUCTION

A. *The Question Raised*

In 2003, Audible Magic, a company that provides “content management and identification services,”¹ and Palisade Software, a company that produces network management software,² announced a joint licensing deal to produce “the first network appliances that identify copyrighted works ‘on the fly’ combined with the ability to block individual trades.”³ The resulting product, the “CopySense® Network Appliance”⁴ (“CopySense”), has been heavily marketed by Audible Magic to university network administrators in order to crack down on song filesharing.⁵

The question is whether the deployment of this tool, or another like it,⁶ is permissible under the Federal Wiretap Act (“Wiretap Act”).⁷ The Wiretap Act explicitly states that unauthorized interception of communications is illegal, except under a limited list of enumerated exceptions.⁸ Audible Magic designed CopySense to intercept and identify the contents of communications without the network users’ knowledge.⁹ While the Wiretap Act prohibits such

¹ Audible Magic, *Audible Magic and Palisade Systems Partner to Filter Illegal P2P File Transfers*, Sept. 9, 2003, <http://www.audiblemagic.com/news/press-releases/pr-2003-09-09.asp> (last visited May 1, 2006) (on file with author).

² *Id.*

³ *Id.*

⁴ Audible Magic, *Audible Magic’s CopySense® Appliance*, Oct. 21, 2003, <http://www.audiblemagic.com/news/press-releases/pr-2003-10-21.asp> (last visited May 1, 2006) (on file with author).

⁵ *See, e.g.*, Audible Magic, *supra* note 1 (on file with author) (“The two companies anticipate particularly strong appeal within the university market . . .”); *see also* Audible Magic, *CopySense Appliance Customer Case Studies*, at <http://www.audiblemagic.com/products-services/copysense/case-studies.asp> (last visited May 1, 2006) (on file with author) (listing case studies for several national universities).

⁶ CopySense may be the leading – or only – product of its kind on the market at the moment, but the underlying technology, or its functional equivalent, could be developed for sale by other vendors.

⁷ Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 et seq. (2000).

⁸ *See* 18 U.S.C. § 2511. For a discussion of the specific language, *see infra* Part III.A.

⁹ *See* Audible Magic, *supra* note 1.

monitoring on traditional telephone networks, this paper argues that the Wiretap Act's sanction against interception extends to Internet communications as well. As such, use of CopySense, or any similar tool, amounts to an illegal invasion of communications privacy.

B. *The Question's Importance*

The legality of content-identifying network traffic intercepting tools is not an idle question. In targeting university network administrators as customers, Audible Magic has identified a potential customer base that has been under considerable pressure from the movie and music industries to crack down on filesharing.¹⁰ These industries have already demonstrated a willingness to sue students for filesharing,¹¹ and the legal risk students face if their university intercepts and identifies their network traffic is very real.¹²

The purpose here, however, is not to evaluate the legal merits of such lawsuits, but rather to point out at least one very plausible and significant consequence for users if their university intercepts their network traffic. Even without facing this specific consequence, however, users face a general loss of privacy in their communications with this kind of interception because all communications over the Internet are vulnerable if universities can use tools like CopySense. While universities currently deploy CopySense primarily to identify song files sent using peer-to-peer technology ("P2P"),¹³ either CopySense or another tool could intercept any other type of private communication that uses any other Internet technology. While such a tool could be looking for song files today, presumably it could be looking for any other type of content tomorrow.¹⁴

¹⁰ See, e.g., John Borland, *RIAA targets students in new file-swapping suits*, CNET NEWS.COM, Oct. 29, 2004, <http://asia.cnet.com/news/industry/0,39037106,39199262,00.htm>; USC Copyright Complaint Letter, annotated by Cory Doctorow, available at <http://craphound.com/usccopyrightcompliance.html> (last visited Aug. 25, 2006).

¹¹ *Id.*; Recording Industry Association of America, *Illegal File Sharing Targeted In Wave Of New Lawsuits*, Nov. 18, 2004, <http://www.riaa.com/news/newsletter/111804.asp> (last visited May 20, 2006) (on file with author).

¹² See, e.g., Kristen Philipkoski, *University Snoops for MP3s*, WIRED NEWS, Nov. 13, 1999, <http://www.wired.com/news/technology/0,1282,32478,00.html>.

¹³ See AUDIBLE MAGIC CORPORATION, WHITE PAPER: MANAGING PEER-TO-PEER TRAFFIC WITH THE COPYSENSE™ NETWORK APPLIANCE 6, http://audiblemagic.com/documents/P2P_Managing.pdf (last visited Mar. 25, 2006) (on file with author) [hereinafter WHITE PAPER]. Currently, filesharing is most typically done using P2P technology, although files can be exchanged using other types of Internet technology as well. In its current incarnation, CopySense only monitors P2P traffic, but Audible Magic could probably enhance the core interception technology in a later release to intercept other types of traffic.

¹⁴ Tomorrow may already be here. CopySense can now discover other types of content, including video, software, and sexual content. *Audible Magic Device Scans for Video, Software and Porn*, THE ONLINE REPORTER, May 22-28, 2004,

As the public relies upon the Internet more and more as a tool for communication, the Internet replaces the previous technologies that have long enjoyed clearer legal protection.¹⁵ This makes articulating the boundaries of protection for private communications in this new medium all the more critical. There should be no question that the existing privacy protections apply as broadly to Internet communications as they have to communications made with earlier technologies. This analysis therefore explains how both the existing language and the policy goals of the Wiretap Act support expansive privacy protection for Internet communications generally, and forbid the CopySense type of Internet traffic monitoring specifically.

II. BACKGROUND

A. *The Nature and History of the Wiretap Act*

As telephone use became more widespread in the United States,¹⁶ there was an increasing awareness that the mechanics of information technology could potentially undermine the protections set forth by the Fourth Amendment.¹⁷ Justice Brandeis, dissenting in *Olmstead v. U.S.*, stated that “[a]s a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping.”¹⁸ In the 1930s, Congress passed the Communications Act of 1934,¹⁹ which might have served the purpose of effectively forbidding wiretaps, had courts not subsequently

<http://www.onlinereporter.com/TORbackissues/TOR397.htm> (on file with author) (“‘The strategy we have developed, working with content owners to register and identify songs, is easily extended to other forms of content,’ said Audible Magic founder and CEO Vance Ikezoye. ‘Movies and porn are areas of increasing concern on P2P networks, especially as more and more consumers adopt high-speed connections.’”).

¹⁵ See, e.g., *Glazner v. Glazner*, 347 F.3d 1212, 1215 (11th Cir. 2003) (reiterating that the Wiretap Act applies to telephony). While the Wiretap Act had clearly applied to the telephone network, the Internet is increasingly providing communication functions formerly served by the telephone network. For example, the availability of emailing and instant messaging (“IM”) has substantially supplanted the need for telephoning. In addition, Voice over IP (“VoIP”) technology can facilitate phone calls themselves. See generally Ben Charny, *Sales of Net phone gear surge on VoIP*, CNET NEWS.COM, Feb. 24, 2004, <http://www.zdnetasia.com/news/hardware/0,39042972,39169373,00.htm>.

¹⁶ By 1930, 40 to 50% of non-farm households had telephone service. CLAUDE FISHER, *AMERICA CALLING: A SOCIAL HISTORY OF THE TELEPHONE TO 1940*, 93 fig.4 (1992).

¹⁷ U.S. CONST. amend. IV (“The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated; and no warrants shall issue but upon probable cause, supported by oath or affirmation and particularly describing the place to be searched and the persons or things to be seized.”).

¹⁸ *Olmstead v. U.S.*, 277 U.S. 438, 476 (1928) (Brandeis, J., dissenting).

¹⁹ Communications Act of 1934, ch. 652, 48 Stat. 1064 (codified at 47 U.S.C. § 605 (1958) (amended 1968)).

limited it to narrow circumstances where there had been physical trespass.²⁰ In the decades that followed, the tension between the government's need to use wiretapping to prosecute crime and citizens' Fourth Amendment rights continued to build.²¹ Then, in 1967, the Supreme Court announced in two cases, *Berger v. New York*²² and *Katz v. U.S.*,²³ the constitutional basis for an interdiction on wiretapping that Congress used in 1968 as the underpinnings of its new Wiretap Act.²⁴

However, by 1986, Congress faced growing concern that the Wiretap Act's language barring interception of "oral" or "wire communication" may not cover new communication technologies developed since 1968.²⁵ Consequently, Congress passed the Electronics Communication Privacy Act ("ECPA")²⁶ specifically to add "electronic communication" to the list of protected communications.²⁷ Thus, with ECPA, Congress attempted to bring the Wiretap Act to the electronic age. Unfortunately, having done so before the popularization of the Internet, the new statutory language did not directly address the unique nature of Internet communications.²⁸ Nevertheless, the privacy interests protected by the Wiretap Act are as equivalently present in Internet communications as they have been in their non-Internet and explicitly

²⁰ Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 21-22 (2004). For a more thorough discussion on the history of the Wiretap Act's evolution, *see id.* at Part II.

²¹ *Id.* at 23-24.

²² 388 U.S. 41 (1967).

²³ 389 U.S. 347 (1967). In *Katz* the Court removed the physical trespass requirement by announcing that the "Fourth Amendment protects people, not places." *Id.* at 351-53; Freiwald, *supra* note 20, at 21-22.

²⁴ Freiwald, *supra* note 20, at 23-24.

²⁵ *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 503 (2d Cir. 2005) (quoting Sen. Rep. No. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555, "Through the enactment of ECPA, Congress amended the Federal wiretap law in order to 'update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.'").

²⁶ Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1999).

²⁷ *Hall*, 396 F.3d at 503. ECPA had two parts: Title I, which updated the Wiretap Act to cover unauthorized interception of electronic communications, codified at 18 U.S.C. §§ 2510-2522 (2000), and Title II, which created the Stored Communications Act, codified at 18 U.S.C. §§ 2701-2711 (2000) ("govern[ing] unauthorized access to stored communications"). *Hall*, 396 F.3d at 503.

²⁸ Congress significantly amended the Wiretap Act two other times, with the Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103-414, 108 Stat. 4279 (1994), and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act"), Pub. L. No. 107-56, 115 Stat. 272 (2001). Neither, however, made any changes to the Wiretap Act that bears directly on this analysis.

covered forms, and thus the Wiretap Act should still extend to them.²⁹

B. The Technical Nature of Internet Communications

1. Internet Architecture

The Internet is a collection of interconnected packet-switched networks.³⁰ “Packet-switched” means that data is divided up and transmitted in chunks, with each chunk or packet containing both a piece of the original data and the information necessary to deliver it.³¹ These packets travel independently of each other, with their own address information instructing each gateway or router it passes through how to switch them or pass them off from one physical network to another until they reach their final destination.³²

The TCP/IP protocol suite is what facilitates this type of data transmission over the Internet.³³ TCP/IP is comprised of various different protocols that interact on one of four layers: the link layer, the network layer, the transport layer, and the application layer.³⁴ The link layer is where the data packets interface with the hardware handling the network traffic, such as network cards.³⁵ The network layer handles the addressing of packets for routing through the network,³⁶ while the transport layer provides for the flow between destination points on the network.³⁷ The application layer is where the software application creates the data requiring transmission across the network (although it is important to note that unlike the other layers it does not itself affect this transmission).³⁸ All these layers work together to produce, send, and interpret data sent through the Internet: as an application generates data to send across the network, each packet of data gets header information prepended (or sometimes appended) to it by each layer as it passes through it.³⁹ This header information cumulatively allows the packet to be routed to its destination and the receiving application to handle it correctly at the other end.⁴⁰ It includes the address of the destination machine, and often a port

²⁹ See discussion *infra* Part III.

³⁰ CRAIG HUNT, TCP/IP NETWORK ADMINISTRATION 3-4 (2d ed. 1998).

³¹ *Id.* at 12.

³² *Id.* at 12-13.

³³ W. RICHARD STEVENS, TCP/IP ILLUSTRATED, VOLUME 1, at 16 (1994).

³⁴ *Id.* at 6. Other references label these four layers slightly differently, and some Internet architecture documentation refers to as many as seven layers. See, e.g., HUNT, *supra* note 30, at 7-9. However, for all intents and purposes, here the following labels will illustrate the essential operation of the Internet sufficiently.

³⁵ STEVENS, *supra* note 33, at 2.

³⁶ *Id.*

³⁷ *Id.*

³⁸ *Id.* at 4.

³⁹ HUNT, *supra* note 30, at 9.

⁴⁰ STEVENS, *supra* note 33, at 3.

number, which helps the destination machine know what software application it should use to process the data.⁴¹ These applications vary widely, from Web browsers, IM clients, and filesharing programs⁴² to email clients, other file transfer clients (“FTP” is a commonly used protocol),⁴³ remote login programs,⁴⁴ or any other program that communicates data to a remote computer.

2. Challenges to Administration of Internet-Connected Networks

An issue network administrators constantly face is the invasion of unwanted packets on its network.⁴⁵ Not only do these packets consume bandwidth the administrators would prefer to have available for authorized communications, but they also frequently pose threats to the security of computers on the local network.⁴⁶ Often these threats come masked as packets of more benign purpose. For instance, packets usually come with port destinations as part of their address information in order to help the destination computer know which software application to use to process it.⁴⁷ Web traffic, as one example, typically contains a destination address for port 80.⁴⁸ However, network administrators can’t simply presume that any packet with a port 80 address is Web traffic since malevolent Internet users have learned to give their more sinister packets a port 80 address in order to trick the network into thinking that the sinister packets are harmless and into allowing them onto the network.⁴⁹ Sinister packets may very well be attempts to invade and control a network host, perhaps as a virus, or a worm, or some other stream of data that, if permitted to proceed to its destination unchecked, could cause disruption to the normal operation of the network or any of its computers’ legitimate applications. They may also potentially steal or corrupt users’ data or attack

⁴¹ HUNT, *supra* note 30, at 43.

⁴² STEVENS, *supra* note 33, at 3.

⁴³ CHRIS MCNAB, NETWORK SECURITY ASSESSMENT 186 (2004).

⁴⁴ STEVENS, *supra* note 33, at 3. Telnet, SSH, and Citrix clients are just a few examples of applications that allow someone to remotely connect to another machine to run applications on it. *See generally* MCNAB, *supra* note 43, at 155-185.

⁴⁵ MCNAB, *supra* note 43, at iii.

⁴⁶ *Id.* at 1-2.

⁴⁷ HUNT, *supra* note 30, at 43.

⁴⁸ Apache is an example of common Web server which by default binds to port 80. Apache HTTP Server Project, *Apache Server Frequently Asked Questions*, at <http://httpd.apache.org/docs/misc/FAQ.html#fdlim> (last visited May 20, 2006). *See also* Doug Brown, *Security Basics*, at <http://www.ibiblio.org/security/articles/ports.html> (last visited May 20, 2006).

⁴⁹ *See, e.g.*, Mark Grennan, *Firewall and Proxy Server HOWTO*, at <http://www.tldp.org/HOWTO/Firewall-HOWTO-7.html> (last visited Mar. 25, 2006) (“Because port 80 doesn’t have to [be] used as a Web port, a smart hacker might use this port to create a virtual private network (VPN) through the firewall.”)

systems in such a way as to prevent their further use.⁵⁰ These threats are so pervasive that unauthorized users can take over a machine running a new installation of a Windows operating system, without any antivirus or firewall protection, in a matter of minutes.⁵¹

Another consequence of these kinds of masquerade attacks is that they inhibit the network administrator from easily throttling bandwidth to prioritize certain types of application traffic. For instance, an administrator might want to prioritize Web traffic over P2P traffic, but it will not be able to do so reliably simply by looking at the address headers. The administrator might ultimately need to look at the content of the data itself, at the application level, in order to reliably ascertain what type of application it truly represents.⁵² In fact, the nature of Internet technology and the seriousness of the invasive threats may require that packets be constantly intercepted, analyzed, and recorded in order to successfully manage and protect the network.⁵³

3. CopySense Technology

CopySense is a network tool that intercepts,⁵⁴ analyzes,⁵⁵ and records⁵⁶ Internet communications at the content level,⁵⁷ silently⁵⁸ and automatically,⁵⁹

⁵⁰ *Id.* For a list of possible network threats, see MCNAB, *supra* note 43, at x.

⁵¹ See, e.g., University of Illinois at Urbana-Champaign, *How to set up a Windows XP computer for GSLIS*, at http://support.lis.uiuc.edu/sysdocs/windowsxp/windows_XP_setup.htm (last visited May 20, 2006) (“It is very important that while you’re installing Windows onto a new computer that you do it behind a NAT box. Windows when installed from scratch is incredibly insecure (yes, even if it has service pack 2). We’ve had computers hacked within 2 or 3 minutes of being installed, so we never install a fresh unpatched Windows computer without being behind a NAT box first.”).

⁵² The need and ability to “packet sniff” already exist, and network administrators frequently employ packet sniffing in the ordinary course of protecting their network. See, e.g., Red Squirrel, *What are Packet Sniffers and Are They Good or Bad?*, ICETEKS, at <http://www.iceteks.com/articles.php/packetsniffers/1> (last visited May 20, 2006). Of course, these tools themselves raise an eavesdropping concern. For a discussion of the legal issues raised, see *infra* Part III.B.2.

⁵³ For a partial list of tools available to assist in “packet sniffing,” see *Packet Sniffing*, TECH-FAQ.COM, at <http://www.tech-faq.com/packet-sniffer.shtml> (last visited May 20, 2006).

⁵⁴ WHITE PAPER, *supra* note 13, at 3 (“[CopySense] passively monitors all network traffic . . .”).

⁵⁵ *Id.* at 2 (“CopySense . . . can discern the electronic signatures of copyrighted media.”)

⁵⁶ *Id.* at 3 (“The CopySense Appliance logs all P2P transactions and attempts.”); *Id.* at 4 (listing reporting capabilities that include copyrighted content uploaded and downloaded by IP address).

⁵⁷ *Id.* at 5 (“By utilizing technology that works on both the application and the content level, Audible Magic’s CopySense Appliance is unique.”).

⁵⁸ See Audible Magic, *Technology*, at <http://web.archive.org/web/20041016025900/http://audiblemagic.com/technology.html> (last visited May 20, 2006) (on file with author)

enabling also the identification of the user.⁶⁰ The Audible Magic White Paper further describes the CopySense operation:

[T]he appliance monitors packet traffic via a router, hub or mirror port of a switch. Because TCP/IP breaks up a transmission into smaller packets, the CopySense Appliance must reassemble the streams. These streams are then decoded to identify the application in use. When a P2P stream such as Gnutella is recognized, that information is recorded into a log. For any P2P stream, an attempt is made to identify copyrighted content. The content can be determined using header or file information, or a more sophisticated electronic signature matching process can be performed. Once the stream has been identified, the information generated can be collated for reporting purposes or utilized to actively block the transaction. The appliance can be set to block all P2P transactions or block only copyrighted content traded via P2P. P2P bandwidth throttling is also an option.⁶¹

Where it differs technically from other network tools that also monitor packet data, even at the content level, is in its “fingerprinting” technology, which identifies the exact content transmitted by matching the content’s signature with a database of known copyrighted materials.⁶² The CopySense

(“The technology is able to passively monitor the data traffic of a network and capture information about digital media transmission activity. Since the technology is not located ‘in-stream,’ there is no performance impact of the monitoring on the network.”).

⁵⁹ See Audible Magic, *CopySense Network Appliance Privacy Policy*, at http://web.archive.org/web/20041020113425/http://audiblemagic.com/copysense_privacy.html (last visited Mar. 25, 2006) (on file with the author) (“... the Appliance acts autonomously and without user intervention to execute the rules designated for the appliance.”).

⁶⁰ See, e.g., WHITE PAPER, *supra* note 13, at 6 (“The CopySense Appliance captures IP addresses and ports of every transaction monitored . . .”).

⁶¹ *Id.* at 4.

⁶² *Id.* at 6 (“The CopySense™ technology examines the perceptual characteristics of a media file and compares that signature with those contained in a database of protected works. Publishers of media content register their works in Audible Magic’s database. The database is regularly updated in the CopySense Appliance as part of a content update subscription.”); *Id.* at 2 (“Audible Magic’s CopySense technology is unique among all network products. Operating similarly to anti-virus processes, CopySense (Copyright-Sensing) technology can discern the electronic signatures of copyrighted media. The technology does not rely on meta tags and operates independently of file format or encoding techniques. The technology has already been proven in Audible Magic’s revolutionary RepliCheck service, which is now a recognized anti-piracy standard in the disk replication industry. Through RepliCheck, Audible Magic has developed agreements with all the major US record labels as well as hundreds of independent media publishers. This has resulted in a signature database of over 3.7 million protected works, with hundreds of signatures added weekly.”).

tool can then automatically block the transmission⁶³ or leave it to network administrators to take further action based on the information CopySense records and reports, including divulging that information to university officials or representatives of the potential copyright owners.⁶⁴

C. *Peeling Back the Layers of Law and Technology*

Analyzing CopySense's permissibility under the Wiretap Act requires analyzing the legality of intercepting Internet communications more generally. However, with so many legal, technical, and situational permutations involved with Internet communications, applying the Wiretap Act to each of them could easily send the analysis off into a tangent, where something particular to one of these aspects could skew the analysis and subsume the underlying legal question. Therefore, for purposes here, this Note will initially strip down the question to a core group of technologies: contemporaneous internet technologies, including P2P and IM,⁶⁵ but excluding email and Web browsing, and to a specific environment: universities. Such a breakdown serves several purposes: for one, it effectively focuses the analysis. For another, technologies like email⁶⁶ and Web tracking technology (e.g., cookies)⁶⁷ have their own

⁶³ *Id.* at 5 ("The CopySense Appliance can block or shape P2P streams in real-time, based upon a set of business rules selected from a Web browser interface. When encountering a P2P packet matching a block or shaping rule, the appliance issues a TCP/IP Reset command that is communicated to both the upload and download addresses and automatically terminates the connection.").

⁶⁴ Universities often receive subpoenas to divulge the identities of its network users, as known by their IP addresses. *See, e.g.,* Josh Brodie, *University receives RIAA suit subpoena*, THE DAILY PRINCETONIAN, May 7, 2004, available at <http://www.dailyprincetonian.com/archives/2004/05/07/news/10529.shtml> (last visited Aug. 30, 2006).

⁶⁵ IM clients can often facilitate a variety of types of communication transfers themselves, including voice and data. *See, e.g.,* Yahoo!, *Yahoo! Messenger Features*, at http://messenger.yahoo.com/features.php?_ylt=AnyB2NejPqnt25rMWcXBW9VwMMIF (last visited May 20, 2006). Some IM clients and services also can queue messages for later delivery if the intended recipient is not online when the sender sends the message. *See, e.g.,* Yahoo!, *Yahoo! Messenger Help*, at <http://help.yahoo.com/help/us/messenger/win/im/im-07.html> (last visited May 20, 2006). However, for simplicity, this Note will focus only on the aspect of IM that supports real-time communications.

⁶⁶ *See, e.g.,* Hall v. Earthlink Network, Inc., 396 F.3d 500 (2nd Cir. 2005); Fraser v. Nationwide Mutual Insurance Co., 352 F.3d 107 (3rd Cir. 2003). Another major case involving the legality of intercepting email is *U.S. v. Councilman*, 418 F.3d 67 (1st Cir. 2005). Because email is stored as part of its transmission, courts have grappled with whether this storing aspect puts email under the purview of the Wiretap Act, or the less-restrictive Stored Communications Act. 18 U.S.C. §§ 2701-2711 (2000). Contemporaneous Internet communications do not necessarily employ storage in the process of their delivery in the same way, and so they analogize better to traditional phone communications, clearly covered by the Wiretap Act. *See, e.g.,* Glazner v. Glazner, 347 F.3d 1212, 1215 (11th Cir. 2003).

bodies of case law and literature that address their own particular technological architecture, which does not necessarily relate to the contemporaneous communications technologies addressed here. In addition, because some courts have found that expectation of privacy may vary depending on the environment where an individual communicates,⁶⁸ the analysis here will focus only on the university environment, as that is a prime target of Audible Magic's marketing.⁶⁹ Once there is an answer to the question as to whether university monitoring of contemporaneous Internet communications violates the Wiretap Act, that analysis should accordingly apply to other technologies and environments.

There are two other points to note here: one, that P2P does not automatically entail song filesharing (which itself does not automatically entail *illegal* filesharing).⁷⁰ P2P is a file transfer architecture that allows Internet users to exchange data more efficiently than traditional client-server architecture (which requires a centralized system to distribute data to any machine requesting it).⁷¹ Instead, P2P allows the nodes on the network to serve as servers themselves, thus not burdening a single system at the core.⁷² All sorts of applications take advantage of this beneficial arrangement, beyond just the infamous Morpheus and Grokster⁷³ et al. clients, such as the Internet telephony software Skype.⁷⁴ It is therefore important to note that "P2P" and "filesharing" are not actually synonymous. However, the CopySense software, by currently focusing only on P2P traffic, treats them as though they are.⁷⁵ Since the most common filesharing software is P2P-based, for simplicity, this analysis will also adopt the same convention, but not without first noting that files can be exchanged via other technologies,⁷⁶ and that P2P software also allows for

⁶⁷ See, e.g., *Blumofe v. Pharmatrak, Inc. (In re Pharmatrak Privacy Litig.)*, 329 F.3d 9 (1st Cir. 2003).

⁶⁸ See, e.g., *United States v. Bailey*, 272 F. Supp. 2d 822, 834-37 (D. Neb. 2003) (discussing the conditions under which an employee might have a reasonable expectation of privacy in work email).

⁶⁹ See discussion *supra* Part I.B.

⁷⁰ See, e.g., Brief of Amici Curiae Law Professors in Support of Respondents at 2, *MGM*, 125 S.Ct. at 686 (No. 04-480), available at http://www.eff.org/IP/P2P/MGM_v_Grokster/20050301_lunney.pdf (last visited Aug. 30, 2006). See also *MGM Studios, Inc. v. Grokster, Ltd.*, 125 S.Ct. 2764, 2770 (2005).

⁷¹ *Peer-to-peer*, WIKIPEDIA, at <http://en.wikipedia.org/wiki/Peer-to-peer> (last visited Aug. 25, 2006).

⁷² *Id.*

⁷³ *MGM Studios*, 380 F.3d at 1154.

⁷⁴ Skype Technologies S.A., *Skype P2P Telephony Explained*, at <http://www.skype.com/products/explained.html> (last visited May 20, 2006).

⁷⁵ WHITE PAPER, *supra* note 13, at 6.

⁷⁶ See, e.g., *id.* (stating that CopySense operates only on P2P applications and not on downloads made from other Internet sources).

many unquestionably permissible uses.⁷⁷

Internet telephony⁷⁸ is the second item worth mentioning at this point because it is possible to consider Internet telephony a contemporaneous communication. However, because its technology raises a host of issues of its own, this analysis will omit it, for the most part, except to point out occasionally that any legal paradigm that would permit interception of other contemporaneous Internet communications could conceivably also apply to Internet telephony in the same way. Should that happen, it would result in an inconsistency between the privacy protections available for phone calls made by the ordinary telephone network – which are more clearly protected⁷⁹ – and those made over the Internet infrastructure, even though the privacy interests themselves could be the same. Alternatively, if Internet telephony did happen to receive the same kind of protection as conventional telephony, there would be an inconsistency in the privacy protections for an Internet communication depending on whether the communicator used voice or data, conceivably even if made by the same software application.⁸⁰ This Note will argue that such inconsistent results provide further support to the conclusion that Internet communications of all sorts – but particularly contemporaneous ones – should be entitled to the same protections currently available for regular telephone calls.

III. ANALYSIS

A. *How the Language of the Wiretap Act Prohibits CopySense*

1. Through the Language Generally

The Wiretap Act provides a private right of action against individuals who make unauthorized interceptions of a communication,⁸¹ barring limited enumerated exceptions.⁸² Plaintiffs “must show five elements to make their claim under Title I of ECPA: that a defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a

⁷⁷ See, e.g., 17 U.S.C. § 107.

⁷⁸ Including VoIP. See, e.g., Federal Communications Commission, *Voice-Over-Internet-Protocol*, at <http://www.fcc.gov/voip/> (last visited May 20, 2006).

⁷⁹ See, e.g., Freiwald, *supra* note 20, at 14; see also discussion *infra* Part III.

⁸⁰ Skype, for instance, can facilitate the sending of voice, video, binary, or textual communications at the same time. See generally Skype Web site, at <http://www.skype.com/> (last visited Aug. 30, 2006).

⁸¹ 18 U.S.C. § 2520. It is also impermissible to divulge the contents of intercepted communications, 18 U.S.C. § 2511(1)(C), but liability for interception is not contingent on whether or not those contents are revealed to another party.

⁸² *Blumofe v. Pharmatrak, Inc. (In re Pharmatrak Privacy Litig.)*, 329 F.3d 9, 18 (1st Cir. 2003).

device.”⁸³ In the case of an application like CopySense, there is little question as to whether its interception of data is intentional. Administrators purposefully deploy CopySense on a network with the stated goal of intercepting Internet communications. The other elements above require further analysis, however.

2. Through the Meaning of “Interception”

Because of the nature of Internet technology, it is more difficult to determine what constitutes an interception of Internet communications within the meaning of the Wiretap Act than it is for telephone communications. The Wiretap Act defines interception as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.”⁸⁴ The terms themselves are not dependent on a specific communications network technology, but courts’ concepts of what constitutes interception may be.⁸⁵ Through decades of jurisprudence, courts have acclimated to telephone networks, which are circuit-switched and simply involve tapping directly into the circuit to intercept the content of the communications.⁸⁶ They are not yet necessarily equally familiar with the packet-switched architecture of the Internet.⁸⁷ Instead of being transmitted over complete circuits, Internet communications are split up into separate packets and sent in small chunks, via all sorts of routes, independent of the other chunks necessary to reconstitute it into a whole communication, and often interspersed with the chunks of other unrelated communications.⁸⁸ In addition, sometimes, at various points in delivery, the packets are transiently stored before they reach the intended recipient.⁸⁹

Consequently, courts have struggled with determining what would constitute “interception” of Internet communications under the language of the Act.⁹⁰ Simply *acquiring* the contents of a communication did not seem to be sufficient.⁹¹ For better or worse, courts’ analyses have tended to hinge on

⁸³ *Id.* (citing 18 U.S.C. § 2511(1)(a)).

⁸⁴ 18 U.S.C. § 2510(4).

⁸⁵ *See, e.g.*, U.S. v. Councilman, 418 F.3d 67, 79-81 (1st Cir. 2005).

⁸⁶ *Telephone Tapping*, WIKIPEDIA, at http://en.wikipedia.org/wiki/Wire_tap#Wiretapping_methods (last visited May 20, 2006).

⁸⁷ *See, e.g.*, *Councilman*, 418 F.3d at 71, where an en banc panel reversed the earlier appellate panel decision. 373 F.3d 197 (1st Cir. 2004).

⁸⁸ *See supra* Part II.B.1.

⁸⁹ *See Councilman*, 418 F.3d at 69-70.

⁹⁰ *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002) (“We observe that until Congress brings the laws in line with modern technology, protection of the Internet and Web sites such as Konop’s will remain a confusing and uncertain area of the law.”).

⁹¹ *Id.* at 876 (“‘Intercept’ is defined [in the Wiretap Act] as ‘the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.’ Standing alone, this definition would seem to

whether contents were acquired from electronic storage, or whether they were intercepted contemporaneously with transmission.⁹² If the contents had been stored, their “interception” did not implicate Title I of ECPA, but rather Title II, the Stored Communications Act,⁹³ and the Wiretap Act’s interdiction against interception would not apply.⁹⁴ Although the Stored Communications Act does prohibit certain types of access to stored electronic communications, its level of protection is less than that of the Wiretap Act.⁹⁵

In cases involving Internet communications like email, the unsettled question had revolved around whether “interception” (in the legal sense of the term) can occur when there is retrieval from electronic storage or whether interception occurs only with “acquisition contemporaneous with transmission.”⁹⁶ The question is not completely settled, but it does seem clear that, at minimum, interceptions made contemporaneous with transmission would constitute “interceptions” as forbidden by the Wiretap Act.⁹⁷

The problem with focusing on contemporaneousness, however, is that some types of Internet communications, like email, involve a period of storage before delivery but still feel contemporaneous to the user,⁹⁸ while other types, like IM, generally feel more contemporaneous, but can still be held before delivery.⁹⁹ Hanging Wiretap Act protections on this criterion ties them too tightly to the architecture of the communications medium and not the communications purpose or liberty interest at stake. Recalling *Katz*’s admonition that the “Fourth Amendment protects people, not places,”¹⁰⁰ it

suggest that an individual ‘intercepts’ an electronic communication merely by ‘acquiring’ its contents, regardless of when or under what circumstances the acquisition occurs. Courts, however, have clarified that Congress intended a narrower definition of ‘intercept’ with regard to electronic communications.”).

⁹² *Id.* at 876-77 (citing *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 460 (5th Cir. 1994)).

⁹³ 18 U.S.C. §§ 2701-2711.

⁹⁴ *Konop*, 302 F.3d at 877 (“The *Steve Jackson* court further noted that the ECPA was deliberately structured to afford electronic communications in storage less protection than other forms of communication.”). Ironically, much of what motivated courts making this distinction was that the language of ECPA had parsed in such a way that storage seemed to apply to storage of aural communications, like voicemails, but not to storage of electronic communications. *Id.* The irony is that with the passage of the USA PATRIOT Act subsequent to the *Steve Jackson Games* decision, Congress removed protection of voicemails from the purview of the Wiretap Act. *Id.*

⁹⁵ *Id.* at 879 (“Congress chose to afford stored electronic communications less protection than other forms of communication.”).

⁹⁶ *Id.* at 878.

⁹⁷ *U.S. v. Councilman*, 418 F.3d 67, 80 (1st Cir. 2005).

⁹⁸ *Id.* at 69.

⁹⁹ See, e.g., Yahoo!, *Yahoo! Messenger Help*, at <http://help.yahoo.com/help/us/messenger/win/im/im-07.html> (last visited May 20, 2006).

¹⁰⁰ *Katz*, 389 U.S. at 351-53.

would be better for courts to base their future analysis on the type of communication facilitated and whether its protection would be consistent with analogous communication purposes enabled by the telephone.¹⁰¹ Still, at least as far as contemporaneous P2P file transfers between a sender and receiver are concerned, parties simultaneously engaged in a closed relationship for the exchange of information, CopySense would seem to make an “interception” as within the meaning of the statute.

3. Through the Meaning of “Communication”

With regard to “communication,” the original Wiretap Act language protected only oral or wire communication.¹⁰² These terms covered telephone technologies, but it was less clear if they would cover electronic communications.¹⁰³ To address this concern, Congress added electronic communication to the statutory language.¹⁰⁴ The Wiretap Act now defines communication as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce.”¹⁰⁵ However, these changes took place in 1986, before the Internet had attained its current level of diffusion and uses.¹⁰⁶ The language therefore did not necessarily address Internet technology, although it did not necessarily exclude it either. The Wiretap Act explicitly excludes some types of electronic communication from protection.¹⁰⁷ Those exclusions, however, are generally isolated to specific kinds of data transmission, like electronic funds transfers.¹⁰⁸

The problem that arises is one similar to that involving the definition of

¹⁰¹ Toward this end a safer definition of interception might be the one proposed by the *Steve Jackson Games* appellants, that “to seize something before it is received is to intercept it.” *Steve Jackson*, 36 F.3d at 460-61.

¹⁰² *Freiwald*, *supra* note 20, at 41.

¹⁰³ *Hall v. Earthlink Network, Inc.*, 396 F.3d 500, 503 (2d Cir. 2005) (citing Sen. Rep. No. 99-541, at 1 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3555. (“Through the enactment of ECPA, Congress amended the Federal wiretap law in order to ‘update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.’”)).

¹⁰⁴ *Id.*

¹⁰⁵ 18 U.S.C. § 2510(12).

¹⁰⁶ While it has always been difficult to make an exact count of Internet users, various studies have indicated that, by whatever metric, those numbers have been rapidly increasing over even just the last 10 years. *See, e.g.*, United States Department of Commerce, *Computer Use Up Sharply; One in Five Americans Uses Internet, Census Bureau Says*, Oct. 14, 1999, at <http://www.census.gov/Press-Release/www/1999/cb99-194.html>; Pew Internet and American Life Project, *73% of Americans go online*, Mar. 31, 2006, at http://www.pewinternet.org/press_release.asp?r=127.

¹⁰⁷ 18 U.S.C. § 2510(12)(B-D).

¹⁰⁸ 18 U.S.C. § 2510(12)(D).

“interception.”¹⁰⁹ Because Internet communications can involve a period of transient storage in the process of delivery, there has been the question of whether that storage precluded them from being electronic communications as covered by the Wiretap Act.¹¹⁰ Courts have nonetheless been willing to see Internet communications as communications as defined by the Wiretap Act.¹¹¹ These courts found that Congress meant to cover “a broad range of communication activities.”¹¹² The problem is that the framework Congress used does not exactly match the reality of Internet technology. It appears that Congress intended for voice communications to be covered by the pre-ECPA wire communication definition, and the ECPA “electronic communication” to cover data communications.¹¹³ Of course, with telephonic technology like fax machines sending data communications and Internet technology like VoIP sending voice communications, that model breaks down.¹¹⁴ The best reading of the post-ECPA Wiretap Act is to find that in light of the absence of any specific exclusion, Congress intended generally to protect all electronic communication, and it simply did not have the prescient vocabulary to have done it more precisely. Thus, “electronic communications” should cover Internet communications, and Internet communications are therefore entitled to protection from interception under the Wiretap Act.¹¹⁵

4. Through the Meaning of “Contents” and “Device”

As to the remaining elements, CopySense is very much a “device” that has the very purpose to intercept the “contents” of the communication. Physically, CopySense is a separate entity that requires its own two ports on the network.¹¹⁶ Although its operation is software-driven, the language of the statute does not preclude such operation from the definition of “device.”¹¹⁷ Additionally, the sole purpose of its deployment is to identify the content being transmitted.¹¹⁸ There might be ambiguity if CopySense simply dealt with a packet based on its routing address information. However, CopySense, by its design, looks beyond the address information to the content layer of the packet

¹⁰⁹ See *supra* Part III.A.ii.

¹¹⁰ *Councilman*, 418 F.3d at 72-79.

¹¹¹ *Id.* at 79; *Blumofe v. Pharmatrak, Inc. (In re Pharmatrak Privacy Litig.)*, 329 F.3d 9, 18 (1st Cir. 2003) (“The ECPA adopts a “broad, functional” definition of an electronic communication,” citing *Brown v. Waddell*, 50 F.3d 285, 289 (4th Cir. 1995)).

¹¹² *Councilman*, 418 F.3d at 77 (citing H.R. Rep. No. 99-647 (1986), at 35).

¹¹³ *Id.*

¹¹⁴ Consider that even a song file may contain the sound of the human voice.

¹¹⁵ *Councilman*, 418 F.3d at 79 (finding that emails constituted electronic communications protected by the Wiretap Act).

¹¹⁶ WHITE PAPER, *supra* note 13, at 3.

¹¹⁷ 18 U.S.C. § 2510(5).

¹¹⁸ See discussion of CopySense technology *supra* Part II.B.3.

in order to identify what that content is.¹¹⁹ Barring any specific exception within the language of the Wiretap Act that would permit its deployment, CopySense appears to be the very thing Congress intended the Wiretap Act to forbid.

B. How the Specific Exceptions Permitting Interception Do Not Apply

1. The Ordinary Course of Business Exception

The Wiretap Act excludes from its prohibition against interception devices “being used by a provider of wire or electronic communication service in the ordinary course of its business.”¹²⁰ Such an exception makes sense, particularly for Internet communications, since their transmission requires devices (such as routers and switches) that inherently intercept the communication stream in order to direct it.¹²¹ It would otherwise make it legally impossible to provide a communications network if facilitating the communications transmission exposed the provider to liability under the Wiretap Act.

The operative question here, however, is whether preventing copyrighted material from passing through the network is sufficiently part of the university’s ordinary course of business, or, alternatively, if the attempt to avoid any contributory liability, and thus protect its assets, would be part of the university’s ordinary course of business.

This Note does not attempt to analyze whether or not a university would face any legal liability for contributory liability for copyrighted works passing through its network, but assuming *arguendo* that it would, it still would not justify the interception of their transmission. The rationale for such interception would be, presumably, to reduce the risk of an expensive lawsuit and thus protect the university’s assets. However, asset protection does not appear to be a sufficiently compelling justification for constant interception through the ordinary course of business exemption.¹²² Courts have generally

¹¹⁹ *Id.*; WHITE PAPER, *supra* note 13, at 4 (“... [T]he appliance monitors packet traffic via a router, hub or mirror port of a switch. Because TCP/IP breaks up a transmission into smaller packets, the CopySense Appliance must reassemble the streams. These streams are then decoded to identify the application in use... [Then] an attempt is made to identify copyrighted content. The content can be determined using header or file information, or a more sophisticated electronic signature matching process can be performed.”).

¹²⁰ 18 U.S.C. § 2510(5)(a)(ii).

¹²¹ See discussion *supra* Part II.B.1.

¹²² See, e.g., *Deal v. Spears*, 980 F.2d 1153, 1158 (8th Cir. 1992) (“We do not quarrel with the contention that the Spearses had a legitimate business reason for listening in: they suspected Deal’s involvement in a burglary of the store and hoped she would incriminate herself in a conversation on the phone... But the Spearses recorded twenty-two hours of calls, and Newell Spears listened to all of them without regard to their relation to his business interests. Granted, Deal might have mentioned the burglary at any time during the

construed this exemption narrowly,¹²³ even in the face of significant asset loss.¹²⁴

In *Deal v. Spears*, the defendants' store was robbed of \$16,000.¹²⁵ Suspecting an inside job, the employer defendants listened in on and recorded calls that the employee plaintiff made or received on the office phone, without the employee's knowledge.¹²⁶ These calls were multitudinous and personal, as the plaintiff was embroiled in a complex romantic relationship.¹²⁷ In fact, even before the surreptitious recording began, the employers had warned the employee to cut down on personal calls or risk having them monitored.¹²⁸ Still, the court found that the defendants had no business reason sufficient to justify the wholesale recording of twenty-two hours of calls that, in view of their personal nature, were unrelated to the ordinary course of business.¹²⁹ Even with the \$16,000 loss the defendants hoped to recover, the court found the interception impermissible.¹³⁰ Nor did the violation of store policy to make and receive personal calls justify their interception and recording – indeed, once it was ascertained that the calls were personal, the justification for their interception ended.¹³¹ The court cited *Watkins v. L.M. Berry & Co.*,¹³² which found that “a personal call may not be intercepted in the ordinary course of business under the exemption in section 2510(5)(a)(i), except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not. In other words, a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents.”¹³³

If *Spears* could not monitor all of an employee's calls in order to recover

conversations, but we do not believe that the *Spearses'* suspicions justified the extent of the intrusion.”).

¹²³ *See, e.g., id.* at 1157 (“The exception is actually a restrictive definition.”).

¹²⁴ *Id.* at 1155.

¹²⁵ *Id.*

¹²⁶ *Id.*

¹²⁷ *Id.*

¹²⁸ *Id.* at 1155-56.

¹²⁹ *Id.* at 1158 (“But the *Spearses* recorded twenty-two hours of calls, and *Newell Spears* listened to all of them without regard to their relation to his business interests. Granted, *Deal* might have mentioned the burglary at any time during the conversations, but we do not believe that the *Spearses'* suspicions justified the extent of the intrusion.”).

¹³⁰ *Id.* (“We do not quarrel with the contention that the *Spearses* had a legitimate business reason for listening in: they suspected *Deal's* involvement in a burglary of the store and hoped she would incriminate herself in a conversation on the phone.”).

¹³¹ *Id.* (“Moreover, *Deal* was abusing her privileges by using the phone for numerous personal calls even, by her own admission, when there were customers in the store. The *Spearses* might legitimately have monitored *Deal's* calls to the extent necessary to determine that the calls were personal and made or received in violation of store policy.”).

¹³² 704 F.2d 577 (11th Cir. 1983).

¹³³ *Id.* at 583.

\$16,000 – a very direct and discrete property interest backed up by reasonable suspicions that intercepting the communications would aid in the recovery of the property interest – it follows that universities should not be able to monitor their users to protect their more ephemeral business interests either. Moreover, universities certainly could not monitor their users through systematic and wholesale monitoring of every byte of information communicated. CopySense does have a means of determining what content is P2P, and perhaps it disposes of anything that is not, but it still remains on the network, monitoring everything, waiting for the eureka moment when it finds something P2P.¹³⁴ Even assuming that there is no justification for a user sending a copyrighted work (and there very well may be: CopySense cannot determine whether there is a fair use or other right entitling the student to send or receive the copyrighted work, and the university might not know either¹³⁵), and even assuming that the university has a legitimate interest in stopping its transmission, employing CopySense would be the equivalent of Spears waiting for the eureka moment when it would, somewhere in the twenty-two hours of communications, hear a confession to the theft. Since in the context of the telephone this kind of interception is impermissible, even under the business exception, it should not be permissible in the context of the Internet either. The particular nature of packet technology should not entitle universities to do an end-run around the otherwise clear statutory interdiction.

Furthermore, it is not enough that an individual undertakes interception to protect a business interest – the individual must monitor the communication itself in the ordinary course of business.¹³⁶ A university's business, presumably, is the education of its students – its *raison d'être* is not to police its students in the service of copyright holders. When the university takes on that role, it goes beyond the scope of its normal business activities. An exemption that covers conduct done in the ordinary course of business should not immunize such behavior when it is not done in the ordinary course of a university's business.

2. The Maintenance Exception

Any communications network requires some intervention to make sure it remains operational.¹³⁷ The original Wiretap Act contained an exception permitting communications providers to make interceptions if they were

¹³⁴ WHITE PAPER, *supra* note 13, at 4.

¹³⁵ CopySense simply matches the content to a database of copyrighted works. WHITE PAPER, *supra* note 13, at 6. It does nothing to evaluate the factors that may justify the use or transmission of that content by fair use. 17 U.S.C. § 107 (1976).

¹³⁶ *See, e.g.*, U.S. v. Murdock, 63 F.3d 1391, 1397 (6th Cir. 1995) (“We find that the indiscriminate recording of both incoming and outgoing calls by Mrs. Murdock does not constitute conduct within the ordinary course of the funeral home business in which she had an interest as a part owner.”).

¹³⁷ *See* discussion *supra* Part II.B.2.

incident to their provision of the communications service.¹³⁸ Such an exception is important because it would not serve to protect private communications if the systems facilitating them ended up decaying. Their normal maintenance might well involve administrators needing to listen in on some of the communications. However, there is a vast difference between occasional interceptions of conversations and constant monitoring. The latter falls outside of the language of the exception, which does not even allow for random monitoring except so far as it ensures “quality control.”¹³⁹ Indeed, all such monitoring must be in furtherance of the maintenance of the network.¹⁴⁰ Monitoring by network operators for any other purpose is impermissible.¹⁴¹

With Internet network administration, because of its nature, it may not be as easy to delineate between interceptions made while actively maintaining the network and interceptions made in a passive, prophylactic way.¹⁴² Threats to the network are pervasive, and some administrators believe the best course of action to protect the network is to act as though it is always under attack.¹⁴³

¹³⁸ See 18 U.S.C. § 2511(2)(a)(i) (“It shall not be unlawful under this chapter [18 USCS §§ 2510 et seq.] for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.”).

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ See, e.g., *State v. Dwyer*, 120 Ariz. 291, 294-95 (Ariz. Ct. App. 1978). Here, an operator connected a call and, pursuant to company policy, listened in for a minute to make sure the call went through. Subsequently she reconnected to the call and listened for 15 more minutes, eventually hearing what sounded like a murder plot. The operator called the police to report this. After the police found the victim, the prosecution tried to introduce the call into evidence, but the court rebuked the attempt. The court found that the presence on the line had exceeded the scope of the operator’s duties and therefore had been in violation of the Wiretap Act.

¹⁴² See, e.g., SANS Institute, *The Top 10 Most Critical Internet Security Threats*, June 25, 2001, at <http://www.sans.org/top20/2000/> (recommending to “actively monitor” content passing through the network firewall, despite having already taken precautions to secure it against unauthorized access).

¹⁴³ See, e.g., SANS Institute, *Windows XP: Surviving the First Day*, Nov. 23, 2003, at http://www.sans.org/reading_room/whitepapers/windows/1298.php (“Since its release, a number of severe security vulnerabilities have been discovered in Windows XP. These vulnerabilities are used by worms and viruses, making it impossible to connect an unsecured, unpatched system to the Internet for any amount of time without risking exposure and infection.”); University of California at Berkeley, *Minimum Standards for Networked Devices*, Jan. 2004, at <http://security.berkeley.edu/MinStds/> (“The University of California, Berkeley encourages the use of its electronic communications network in support

For that reason, the maintenance justification in having a tool that records all traffic may be reasonable under this exception, even if it involves recording all traffic that passes through it and monitoring it at the content level.¹⁴⁴ The very operation of the network, in fact, may depend on intercepting each packet of data in order to prevent any packet that would be damaging to the network.¹⁴⁵ Without the maintenance exemption to Wiretap Act's admonitions against interception and recording, such efforts and their enabling technologies would seem to be illegal. Yet such a result would essentially break the Internet because it would strip administrators of some of their most effective protective defenses.¹⁴⁶ The maintenance exemption permits a more nuanced approach by balancing privacy interests with the operation of the network.

Since a router handles an entire data packet, technically it has access to the information at any layer.¹⁴⁷ It only needs the addressing information to direct the packet around the network, however.¹⁴⁸ Intercepting the content layer, where the communication itself lies, is merely incidental and nothing is done with that data except that it is forwarded along with the rest of the address information.¹⁴⁹ This type of interception therefore should in no way compromise any of the privacy interests protected by the Wiretap Act. Therefore, to the extent that network maintenance involves facilitating the ordinary functioning of the network, this type of interception should easily fit the exception.

Routing technology, however, has grown more sophisticated as the traffic it handles has become more harmful to the network's integrity.¹⁵⁰ The tools

of education, research, and public service. However, this resource is limited and vulnerable to attack.”).

¹⁴⁴ Argus is a network tool that also monitors packets as they pass through the network, even at the content level. Because of the problem of packets masquerading as more benign content, Argus is helpful because it examines the packet to make sure it's contents reflect that it is what it purports to be. However, because it automatically intercepts, records, and examines network traffic, it might be just as impermissible under the Wiretap Act as CopySense, unless there is some way to differentiate their purposeful use. For more information about Argus, see Argus Web site, available at <http://www.qosient.com/argus/> (last visited Aug. 31, 2006).

¹⁴⁵ See discussion *supra* Part II.B.2.

¹⁴⁶ Given the fact that harmful traffic is constantly seeking access to the network, and given the fact that basic fortifications (e.g., passwords, firewalls, etc.) are still limited in their protective ability, without the ability to audit the traffic and ensure that nothing nefarious has gained access it shouldn't have, network administrators would be forced to simply hope for the best that nothing harmful has accessed the network. Given the pervasiveness of the threat, that hopefulness would seem misplaced, and as each local network is inevitably compromised, eventually so would be the Internet in general.

¹⁴⁷ CHRIS LEWIS, CISCO TCP/IP ROUTING PROFESSIONAL REFERENCE, at 18 (1991).

¹⁴⁸ *Id.* at 18-19.

¹⁴⁹ *Id.* at 19.

¹⁵⁰ See discussion *supra* note 144.

necessary to fend off this harm may likely require intercepting, potentially recording, and then reacting to all the information in a data packet, including information on its content layer. Since packets may not necessarily be what they claim in their exterior address packaging,¹⁵¹ administrators will need networking tools to take a more detailed look into their cargo before determining what action to take. Actions include either forwarding the packets on, or prioritizing them, or rejecting them outright if they pose a threat to the network. Thus, continuous network traffic interception, even at the content layer, may very well fall under the maintenance exception, if it is the kind of activity that is necessary to ensure proper network operation.

CopySense, however, goes a step further than the other networking tools in its ability to identify the traffic's true content.¹⁵² It not only determines if it is P2P traffic, but it further identifies the specific payload of that P2P traffic.¹⁵³ While other content-layer tools look to make sure the packets do not reflect the signature of certain data (like viruses) which, if let through, could negatively affect the functionality of the network, CopySense looks for the content signature of data which, if transmitted, would not harm the physical operation of the network at all.¹⁵⁴ This difference is not negligible: the maintenance exception strictly applies to ensuring the network's operability.¹⁵⁵ Since the data intercepted has no bearing on the operability of the network, capturing this content cannot fit under the maintenance exception.

Universities may claim that P2P traffic harms the network in terms of its throughput capacity. A university network administrator, for instance, might prefer to prioritize traffic to make sure that its academic-related email has priority on the available bandwidth. Administrators might then, once determining the traffic is P2P, want to lower its priority or simply reject it. Nevertheless, even under the most liberal reading of the maintenance exception, rejection of all P2P traffic outright raises serious concerns – a phone company could not refuse to transmit faxes, for instance. As long as administrators make routing decisions based entirely on the traffic's general profile and not on specifically what is in the content layer, such administration might still be considered a legitimate exercise of network maintenance covered by the exception. CopySense's purpose, however, is not to deal with the data generally, but rather to take action based entirely on the content of each packet specifically.¹⁵⁶ In fact, it does not just look at the content to understand better what type of traffic it is (e.g., P2P), but also what application is sending it and

¹⁵¹ See discussion *supra* note 46.

¹⁵² WHITE PAPER, *supra* note 13, at 4.

¹⁵³ *Id.* at 2.

¹⁵⁴ P2P traffic does indeed consume bandwidth, but all Internet communication consumes bandwidth. Moreover, a song is not like a virus – its transmission will not damage or destroy the network or any data on its nodes.

¹⁵⁵ 18 U.S.C. § 2511(2)(a)(i).

¹⁵⁶ WHITE PAPER, *supra* note 13, at 4.

the very thing that it is sending.¹⁵⁷ It enables the administrator to know exactly what material a user is transmitting, and to take action according to that information.¹⁵⁸ However, since no copyrighted song will cause the network to cease to operate – as a virus or a security hack might – this type of inquisitorial content analysis should fall well outside the scope and purpose of the maintenance exception.

Furthermore, given that the traffic's payload poses no risk to the network, there can be no compelling maintenance reason for any of the other actions the CopySense tool facilitates, such as IP logging and full reporting of the contents found. Such disclosure of a non-risk can have no affect on the network's operation and therefore cannot be justified as maintenance.

3. The Extension Telephone Exception

Congress recognizes another exception permitting interception: the extension telephone exception.¹⁵⁹ Part of the rationale for this exception stems from the location of the extension – the area of one of the parties – and might suggest either a lack of a reasonable expectation of privacy or implicit consent to the interception.¹⁶⁰ Another important reason Congress included this exception is that it has typically been impossible to pick up an extension without there being a tell-tale “click” informing the parties that someone else was listening in.¹⁶¹ In instances where individuals used recording devices that did not similarly provide an indication that the call was being intercepted, courts have found the recording impermissible.¹⁶² CopySense advertises how it sits “transparently” on the network,¹⁶³ without users knowing about it, which would seem to make it a device similar to those judged impermissible.

The extension exception also implies that another person is actively monitoring the call.¹⁶⁴ It is unlikely that a person would listen in to all calls on an extension every hour of every day. The extension exception incorporates the implicit requirement that the interception be limited in duration.¹⁶⁵ The CopySense product, however, as an automatic device, lacks the need for human intervention that would prevent full-time monitoring, and in fact is fully capable of monitoring continuously.¹⁶⁶ As such, it cannot be justified under

¹⁵⁷ *Id.*

¹⁵⁸ *Id.*

¹⁵⁹ 18 U.S.C. § 2510(5)(a)(i).

¹⁶⁰ See *infra* Parts III.C and III.D.1.

¹⁶¹ *Deal*, 980 F.2d at 1157.

¹⁶² See, e.g., *id.*

¹⁶³ See *Audible Magic*, *supra* note 1.

¹⁶⁴ *U.S. v. Jones*, 542 F.2d 661, 673 n.24 (6th Cir. 1976) (“... there is a vast difference between overhearing someone on an extension and installing an electronic listening device to monitor all incoming and outgoing telephone calls”).

¹⁶⁵ *Id.*

¹⁶⁶ Administrators can set CopySense only to operate at certain times of the day.

this exception.

4. How No Other Applicable Exceptions Could Be Inferred

Aside from the enumerated statutory exceptions, courts have been reluctant to infer any additional judicial exceptions for occasions when intercepting communications would be permissible.¹⁶⁷ For example, although earlier decisions suggested there might be an inter-spousal exception implicit in the Wiretap Act,¹⁶⁸ recent decisions have moved away from that analysis, finding that there is not enough unity of interest between spouses to find such interceptions consistent with the protections of the act.¹⁶⁹ Congress knew when it drafted the law that most interceptions within a home would result from domestic disputes, with one party trying to get evidence of the other's wrongdoing, and had it thought this kind of interception to be a valid use of wiretapping it could have exempted it.¹⁷⁰ Yet it did not, and courts are reluctant to do what Congress had opted against doing.¹⁷¹

Although Congress in 1968 could not have anticipated the Internet as it is today, the deference courts show to Congress to maintain the protections of the Wiretap Act and not judicially carve out additional exceptions should extend here. This is especially true because, to analogize with inter-spousal communications (which the Wiretap Act does protect from interception) in the case of universities, there is presumably even less of a common unity of interest between university and student than between spouses. The relationship between users of the network and the university does not permit the inference that one party automatically has the best interests of the other in mind, as one might presume from a familial relationship. This is particularly true when, by using tools such as CopySense, one party – the university – is clearly trying to get evidence of the other's wrongdoing. Moreover, while both Congress and

However, unless individuals are there, actively monitoring the appliance as if they themselves had picked up the phone exception, this scheduling capability does not redeem the interception. WHITE PAPER, *supra* note 13, at 3.

¹⁶⁷ See, e.g., *Pritchard v. Pritchard*, 732 F.2d 372, 374 (4th Cir. 1984) (finding that Title III “prohibits all wiretapping activities unless specifically excepted”); *Jones*, 542 F.2d at 667-68 (concluding that the intention of Title III was to guard against the tremendous incursions into privacy that modern technology now permitted, except in rare but clearly articulated situations).

¹⁶⁸ See, e.g., *Simpson v. Simpson*, 490 F.2d 803 (5th Cir. 1974); *Anonymous v. Anonymous*, 558 F.2d 677 (E.D.N.Y. 1974).

¹⁶⁹ See, e.g., *Glazner v. Glazner*, 347 F.3d 1212, 1215 (11th Cir. 2003); *Heggy v. Heggy*, 944 F.2d 1537, 1540 (10th Cir. 1991); *Kempf v. Kempf*, 868 F.2d 970, 972-73 (8th Cir. 1989); *Pritchard*, 732 F.2d at 374 (4th Cir. 1984); *Jones*, 542 F.2d 661, 667 (6th Cir. 1976).

¹⁷⁰ *Jones*, 542 F.2d at 668 (citing Hearings on Invasions of Privacy Before the Subcomm. on Administrative Practice & Procedure of the Senate Comm. on the Judiciary, 89th Cong. 1st Sess. (1965-66)).

¹⁷¹ *Heggy*, 944 F.2d at 1540; *Jones*, 542 F.2d at 669; *Pritchard*, 732 F.2d 373-74; *Kratz v. Kratz*, 477 F. Supp. 463, 470 (E.D. Penn. 1979).

the courts have allowed parents to eavesdrop on their children's conversations to ensure that their teenagers are not getting into trouble,¹⁷² the university-student relationship is not an analogously custodial one. Students are generally older than eighteen – the legal age of adulthood – and rather than trying to keep them out of trouble, using the CopySense tool seems instead to be done with the purpose of actually getting the students *in* to trouble.¹⁷³

C. *How University Students Have a Reasonable Expectation of Privacy Warranting Wiretap Act Protection*

The hazard of lumping all Internet communications into the single category “electronic communications” is that Internet communications vary widely in form and function, sometimes connecting one person to many people – sometimes even many strangers – or one person to a few people, or one person to one person, or even one person to no other person.¹⁷⁴ While a person posting to a public Web site might not have a reasonable expectation of privacy – the user knows that an untold number of strangers could be privy to the communication – in other situations, the user may realistically believe that a particular, finite, and intended audience will receive the communication exclusively. This belief is certainly present when users engage in contemporaneous Internet communications like IM and P2P, which make closed connections between a limited number of parties.¹⁷⁵

¹⁷² *Anonymous*, 558 F.2d at 679 (citing testimony of Professor Herman Schwartz during hearings for the original Wiretap Act: “I take it nobody wants to make it a crime for a father to listen in on his teenage daughter or some such related problem.” Hearings on the Anti-Crime Program Before Subcomm. No. 5 of the House Judiciary Comm., 90th Cong., 1st Sess. 901 (1967)).

¹⁷³ Arguably a university could claim that by identifying the contents of the students' communications it could keep them out of trouble, by either advising them – or forcing them – to stop communicating the objectionable material. However, if it were permissible for the university to make these interceptions, they would be under no compunction to act so benevolently. Knowing the contents of students' communications could result in subjecting the students to any sort of negative consequence, disciplinary or legal. The only way for the students to avoid any such consequences would be for the university not to be able to know the contents of their communications at all.

¹⁷⁴ For example, individuals could IM a single person, have a chat session with a group of people, or transmit data to their own account on another machine that would not involve communicating with another person.

¹⁷⁵ For IM the contents of the communication are exchanged between a limited number of parties. See *Instant Messaging*, WIKIPEDIA, at http://en.wikipedia.org/wiki/Instant_messaging (last visited Sept. 20, 2006). For P2P, although in some architectures an intermediate node may broker the connection, the actual exchange of content is made exclusively between a finite number of peers on the network. Unlike a public Web site where the contents of the communication are offered to an unlimited audience, on a P2P network the contents of the communication are contained within a limited number of parties connected to the exchange. See generally Nigel Wong, *How P2P Works*, at

Many courts have instead determined whether users have a reasonable expectation of privacy based on whether or not the communications were interceptable.¹⁷⁶ In other words, these courts have decided that because a service provider *could* read emails, that users did not have any expectation of privacy.¹⁷⁷ This approach is inconsistent with telephone wiretapping jurisprudence.¹⁷⁸ After all, phone calls are inherently interceptable.¹⁷⁹ If they were not, there would have been no need for the Wiretap Act's prohibition against it.

A better way to evaluate the potential existence of a reasonable expectation of privacy is to connect it to how people *use* communications technology. In *Katz*, the Court found that the defendant, who placed a phone call at a public pay phone, still made the phone call with a reasonable expectation of privacy.¹⁸⁰ It follows that individuals who make telephone calls today from the privacy of their home, but transported via Internet technology, would still make those calls with the same expectation of privacy.¹⁸¹ Therefore, if phone calls can be made with a reasonable expectation of privacy, then so should any other contemporaneous Internet communication, even one that is data, rather than voice.¹⁸²

Furthermore, Internet users' behavior itself suggests that users believe that

[http://ezinearticles.com/?How-Peer-to-Peer-\(P2P\)-Works&id=60126](http://ezinearticles.com/?How-Peer-to-Peer-(P2P)-Works&id=60126) (last visited Sept. 20, 2006).

¹⁷⁶ Freiwald, *supra* note 20, at 66-67.

¹⁷⁷ *Id.* (citing *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001); *U.S. v. Kenney*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000), *U.S. v. Hambrick*, 55 F. Supp. 2d 504, 506-09 (W.D. Va. 1999), *U.S. v. Maxwell*, 45 M.J. 406, 417 (C.A.A.F. 1996)).

¹⁷⁸ Freiwald, *supra* note 20, at 67.

¹⁷⁹ *Id.*

¹⁸⁰ *Id.* at 38 (citing *Katz*, 389 U.S. at 352, 361).

¹⁸¹ *See, e.g., id.* at 78 (referring to Peter P. Swire, *Katz is Dead, Long Live Katz*, 102 MICH. L. REV. 904 (2004) and his prediction that "there will be no practical difference between wiretapping and stored records searching when telephone calls take place over the Internet").

¹⁸² Phone calls themselves are often data-based. For instance, Telecommunications Device for the Deaf ("TDD") machines allow deaf callers to type their conversations. 47 U.S.C. § 225 (2000). The data-voice distinction for Internet communications should also be of little importance as developers of Internet resources more and more create them to be understood by users with handicaps. While it is a "best-practice" for all Internet resources, the law requires that developers of Internet resources for the United States government make sure that all information provided by them is available for all users. For instance, a site that uses audible information would also need to provide descriptive text or a means for an adaptive device to translate the content. U.S. § 508, Pub. L. 105-220, 1998 H.R. 1385; Pub. L. 105-220, enacted Aug. 7, 1998, 112 Stat. 936; codified as: Section 504 of the Rehabilitation Act, 29 U.S.C. § 794d. See <http://www.usability.gov/accessibility/> for general guidelines on constructing Internet sites for Section 508 compliance. In other words, the format of the information is of less importance than the information itself.

their communications will remain private.¹⁸³ Accounts protected by passwords, messages often sent under anonymous or semi-anonymous aliases, transmissions made in the privacy of one's home or personal workspace – these are all factors indicating that Internet users do in fact have a common expectation of privacy.¹⁸⁴ If this expectation is somehow unreasonable, then there are many, many people clinging to this privacy myth.¹⁸⁵

Moreover, these factors suggest that Internet users are even more vulnerable to interceptions than users of conventional telephone technology.¹⁸⁶ Because Internet communications feel private, they inspire richer communication than telephone lines normally carry.¹⁸⁷ Communications often consist of pictures and video and long documents, which often reveal much more about communicators than mere phone calls would.¹⁸⁸ Numerous individuals would likely not be so candid if they did not have a reasonable belief in those communications remaining private.

There might be certain instances where the appearance of privacy is illusory. Chat rooms might be one such context where the sense of speaking privately is false, because the forum is otherwise open for others to observe silently. Still, users should reasonably be able to consider some connections private, including those made exclusively with another individual, or even a few individuals,¹⁸⁹ and certainly with no other individuals.¹⁹⁰

The university environment offers nothing that should change this assessment. Logically, students using university-provided Internet access within their dormitories, for instance, should not be entitled to less protection than a student living in an off-campus apartment with a third-party provider. This is particularly true when the university network connection is the only one available.¹⁹¹ Until the mass availability of the cell phone, the university was

¹⁸³ Freiwald, *supra* note 20, at 77.

¹⁸⁴ *Id.*

¹⁸⁵ *Id.*

¹⁸⁶ *Id.*

¹⁸⁷ *Id.* at 77.

¹⁸⁸ *Id.*

¹⁸⁹ Some instant message clients can also provide a conference call feature, connecting more than one user, but telephones can also connect through this arrangement. A handful of private users all engaged in the same conversation is a considerably more private communication than one made in a chat room. *See, e.g., Yahoo!, Yahoo! Messenger Features,* at http://messenger.yahoo.com/features.php?_ylt=AnyB2NejPqnt25rMWcXBW9VwMMIF (last visited May 20, 2006).

¹⁹⁰ Some Internet technologies allow remote access to other machines, for instance. *See* discussion *supra* note 42. In these cases, the user may be logging into his own account, sending his own data from his own possession in one place to his own possession in another. Certainly, there can be nothing more private than communicating with oneself.

¹⁹¹ Arguably, a student in a dorm could use a dial-up account to a third-party provided service, but the speeds of such service will likely be significantly slower than a broadband connection onto the university's network.

often also the only provider of telephony for the students as well.¹⁹² Of course, even though the university may have provided the phone service, certainly the university had no claim to be able to listen in on its students' communications.¹⁹³ That students are now making many of these communications via Internet technologies should not affect their according expectation of privacy.

Nor should it ultimately matter whether the student used the Internet at home or somewhere on campus with a wireless connection. As *Katz* explained, it is people, not places, that are protected.¹⁹⁴ Calls from public phone booths, as long as done away from prying eyes and eavesdropping ears, were just as protected as calls made from the privacy of one's own home.¹⁹⁵ Thus, the law should protect Internet communications made under like conditions.

While CopySense currently addresses only P2P traffic, the discussion on other Internet communications is still important when considering users' expectation of privacy. Users can transmit files via many of these types of applications; P2P just happens to be particularly popular so that is what CopySense currently addresses.¹⁹⁶ CopySense's makers, however, could conceivably reprogram it to intercept any of these other types of communications, but with no more permissiveness. Furthermore, P2P communications themselves are most similar to phone calls, which the Wiretap Act most unquestionably considers private and protectable, because they depend on private connections between users as well.¹⁹⁷ Each connection constitutes a private communication that users establish without the facilitation of a central party.¹⁹⁸

¹⁹² Even today, many students must rely on the university as a provider for a dial tone in their dormitory rooms. *See, e.g.*, the policy for the dorms of the University of California at Berkeley, available at <http://rts.berkeley.edu> (last visited Sept. 1, 2006).

¹⁹³ Nor would it even if the students were using dial-up accounts to transmit copyrighted materials the university itself owned over the phone lines it provided.

¹⁹⁴ *Katz*, 389 U.S. at 351.

¹⁹⁵ *Id.* at 352.

¹⁹⁶ WHITE PAPER, *supra* note 13, at 6.

¹⁹⁷ *See e.g.*, Freiwald, *supra* note 20, at 14.

¹⁹⁸ Since the *Napster* decision, *A&M Records v. Napster*, 239 F.3d 1004, 1011-12 (9th Cir. 2001), P2P services have largely changed their architecture so that no central server brokers the connections between computers. *MGM Studios, Inc. v. Grokster Ltd.*, 380 F.3d 1154, 1161-62 (9th Cir. 2004), *cert. granted* 125 S. Ct. 686 (2005). Although users may end up in connections with people they do not already know, the connection is still a private one. In addition, the Wiretap Act does not have a requirement for familiarity with the other party in order for the Act to protect phone calls.

D. *How There Is No Valid Consent to Permit the Universities' Interception of Students' Communications*

1. There Is No Implied Consent

Just as the Wiretap Act carves out specific exceptions in the statute for things like maintenance, it also carves out an exception for consent.¹⁹⁹ It is permissible to intercept a communication “where one of the parties to the communication has given prior consent to such interception.”²⁰⁰ The idea of consent is also the implicit basis many of the exceptions rest upon. For instance, a user implicitly consents to the network operator intercepting the communication to the extent that it is necessary to transmit it.²⁰¹ Still, even these exceptions have limitations. The network operator does not have permission to eavesdrop on all communications – its interception is limited to that which is necessary for the operation of the network.²⁰² Furthermore, even in these cases, consent to interception does not also extend to consent to monitoring of those communications.²⁰³ On the occasions when courts have found there to be implied consent to the communications' interception, courts then had to “inquire into the dimensions of the consent and to ascertain whether the interception exceeded those boundaries.”²⁰⁴ Additionally, the consent must also have been actual, and not simply constructive.²⁰⁵

Universities might want to claim that users using the network have implicitly consented for administrators to intercept their communications. Students are at least to some degree aware that networks administrators have the capability to intercept communications, given administrators' acknowledged role in recovering passwords²⁰⁶ and restoring lost data from backups.²⁰⁷ Merely being aware, however, that the university has the ability to intercept communications is not the same thing as consenting to the university

¹⁹⁹ 18 USC § 2511(2)(d).

²⁰⁰ *Id.*

²⁰¹ 18 USC § 2511(2)(a)(i).

²⁰² *Id.*

²⁰³ Peter Murphy, *An Examination of the United States Department of Justice's Attempt to Conduct Warrantless Monitoring of Computer Networks Through the Consent Exception to the Wiretap Act*, 34 CONN. L. REV. 1317, 1339-40 (2002) (describing the question raised in *Gilady v. Dubois*, 124 F.3d 277, 297 (1st Cir. 1997), and suggesting there was implied consent for networks be able to make backups of electronic communications as long as they are not actually monitored).

²⁰⁴ *Griggs-Ryan v. Smith*, 904 F.2d 112, 119 (1st Cir. 1990).

²⁰⁵ *Blumofe v. Pharmatrak, Inc. (In re Pharmatrak Privacy Litig.)*, 329 F.3d 9, 19 (1st Cir. 2003) (citing *William v. Poulos*, 11 F.2d 271, 281 (1st Cir. 1993)).

²⁰⁶ *See, e.g.*, Boston University Front Office, available at <http://www.bu.edu/it/frontoffice/> (last visited Sept. 1, 2006).

²⁰⁷ *See, e.g.*, Boston University Operations, available at <http://www.bu.edu/it/operations/> (last visited Sept. 1, 2006).

to do so.²⁰⁸ As the D.C. Circuit noted, “consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception.”²⁰⁹ A network tool that sits “transparently”²¹⁰ on the network, automatically recording and analyzing every bit of content of every communication without users aware it was actually doing so, would not seem to satisfy the implied consent requirement even if students theoretically knew that such monitoring was possible. In fact, the transparency aspect makes it seem that the goal is to keep students from knowing this interception is even happening, which would directly defy both the letter and spirit of the consent exception.

2. Universities Should Not Be Able to Extract Express Consent to Justify Their Interceptions of All Student Internet Communications

In order to satisfy the consent exception, universities might try to install terms of service, whereby students, in order to use the campus network, expressly consent upfront to the interception of all their communications. It would need to be actual consent, and likely very specific.²¹¹ Click-through or adhesion agreements would probably not suffice either.²¹² Universities would likely need to put students on notice for the actual interception that would occur, and not just the general policy of interception.

However, even with the most explicitly worded agreement leaving no doubt as to the satisfaction of the requirements of the consent exception, public policy should not permit this kind of agreement. The liberty at stake is a fundamental Fourth Amendment protection. Requiring students to sign away all their communications privacy in order to use the campus infrastructure makes those communications extremely expensive. While making a long distance call on the telephone might cost a few pennies, trying to communicate on the Internet would potentially cost the sacrifice of a civil liberty.

The problem is not just that universities would be privy to the content of the

²⁰⁸ *Blumofe*, 329 F.3d at 20 (quoting *Watkins v. LM Berry & Co.*, 704 F.2d 577, 581 (11th Cir. 1983)).

²⁰⁹ *Id.* at 20 (quoting *Berry v. Funk*, 146 F.3d 1003, 1011 (D.C. Cir. 1998)).

²¹⁰ *Audible Magic*, *supra* note 1.

²¹¹ *Murphy*, *supra* note 203, at 1336 (“[T]he *Jandak* court shows that it will take a very high degree of actual consent by a person whose communications are being intercepted before they will be considered to have ‘knowingly agreed to the surveillance.’” (citing *Jandak v. Village of Brookfield*, 520 F. Supp. 815, 818 (N.D. Ill. 1981) and quoting *U.S. v. Amen*, 831 F.2d 378, 379 (2d Cir. 1987))).

²¹² *See* *Murphy*, *supra* note 203, at 1330-35, regarding network banners and their limited ability in yielding truly informed consent. Network banners were found to be sufficient to construe consent in a military context, *U.S. v. Monroe*, 50 M.J. 550 (1999), but *Murphy* argues, reasonably, that the result should not directly apply to the private sector. *Id.* at 1333. In the military, if personnel divulge too much in their communications, they may jeopardize national security. *Id.* If students happen to share copyrighted information, however, they are unlikely to undermine national security.

communications. The problem is also one of disclosure. Not only would students potentially face the universities' disciplinary system, but universities could also divulge information gleaned from the intercepted communications to copyright holders to fuel their lawsuits. For students to consent to being monitored in this way opens themselves up to significant consequences they might not necessarily have had to face had their communications remained private. Moreover, even if there were no possible legal consequences to having universities identify and disclose the contents of students' communications,²¹³ there still could be other, non-legal consequences. That there might be wrongful content in a communication is immaterial to whether universities can intercept it. Both the innocent and the guilty are still entitled to the Fourth Amendment protections that the Wiretap Act recognizes.²¹⁴

Furthermore, it does not serve any public interest to give universities enforcement powers over their students' communications. Ostensibly, universities are places of learning and progress. Policing Internet communications may only serve to drive students back to more antiquated – but protected – telephone technology. This result may prevent the Internet from being an effective tool for further education and information exchange. In addition, since universities are often incubators for future technology usage habits,²¹⁵ which can carry forth after graduation, dissuading students from using the Internet during their studies will potentially negatively affect their likelihood of using it later on. In many ways, the Internet's usefulness and value is largely contingent on how many people it connects. If people in large numbers stop using it, there will be little reason for anyone else to continue to, and any benefit it might offer to further innovation or civic participation may be lost.

E. How the Goals and Purpose of the Wiretap Act Are Extensible to the Interception of Internet Communications

Although courts are reluctant to limit coverage of the Wiretap Act by inferring exceptions,²¹⁶ they are less reluctant to expand its coverage to areas not explicitly considered in its drafting. One such example where courts extended the Wiretap Act's protection is in the area of video surveillance.²¹⁷

²¹³ See discussion *supra* Part III.B.1.

²¹⁴ See, e.g., the plaintiff in *Deal v. Spears*, who was caught violating store policy yet still able to recover for the wrongful interception. 980 F.2d 1153 (8th Cir. 1992).

²¹⁵ See Cathy Gellis, *Berkeley.edu: Diffusion of the Internet among University Undergraduates* (1996), available at http://www.csua.berkeley.edu/~cathyg/infotech_writing/thesis/intro.html (last visited Sept. 4, 2006).

²¹⁶ See discussion *infra* III.D.4.

²¹⁷ *Freiwald*, *supra* note 20 (citing *U.S. v. Torres*, 751 F.2d 875, 882-84 (7th Cir. 1984)); *U.S. v. Koyomejian*, 946 F.2d 1450, 1457 (9th Cir. 1992); *U.S. v. Taketa*, 923 F.2d 665, 677 (9th Cir. 1991) (finding warrantless government video surveillance to be “exceptionally intrusive” and that “the silent, unblinking lens of the camera was intrusive in a way that no

Congress did not address video surveillance in 1968, likely because video surveillance did not resemble wiretapping enough to share its dangers.²¹⁸ Wiretapping is dangerous to privacy interests because it is “intrusive, continuous, indiscriminate, and hidden.”²¹⁹ Of course, in 1968 cameras were too large to pose a similar danger.²²⁰ However, once the technology advanced to the point where it could be equally dangerous to privacy interests, courts have applied the rationale and rules of the Wiretap Act, and *Katz* before it, to limit this kind of non-aural surveillance.²²¹ Similarly, courts should be willing to apply the rationale and rules of the Wiretap Act to the kind of technological surveillance effectuated by a tool like CopySense, which is also intrusive, continuous, indiscriminate, and hidden, and presents the same dangers to privacy.

IV. CONCLUSION

The very purpose of a tool like CopySense is to intercept and monitor communications. The very purpose of the Wiretap Act is to prevent the interception and monitoring of communications. Thus, by its very design, CopySense seems to conflict with the language and intent of the statute.

Of course, the Wiretap Act’s prohibition is not absolute. It carves out exceptions for when interception would be permissible. It is laden with antiquated language better suited for older communications technologies in defining its applicability. If deployment of CopySense could fit an exception, or avoid the Wiretap Act’s reach by definition, then its use could proceed with impunity.

However, it cannot. No statutory exception is available to cover the wholesale monitoring of private communications’ content that Audible Magic designed CopySense to intercept. Nor is CopySense immune from the Wiretap Act’s purview. That CopySense intercepts Internet communications, as opposed to telephone communications, does not, and should not, exempt it from the Act’s coverage. Private communications are private communications, and the Wiretap Act – as well as its underlying Constitutional precepts – forbids applications, such as CopySense, from violating that privacy through the type of monitoring CopySense facilitates.

temporary search . . . could have been”).

²¹⁸ Freiwald, *supra* note 20.

²¹⁹ *Id.*

²²⁰ *Id.*

²²¹ *Id.*; *See also* United States v. Taketa, 923 F.2d 665, 675-77 (9th Cir. 1991).