

PHONE: 713.231.2315
FAX: 512.692.2522

W. SCOTT MCCOLLOUGH
ATTORNEY AT LAW
1250 CAPITAL OF TEXAS HIGHWAY SOUTH
BUILDING TWO, SUITE 235
AUSTIN, TX 78746

Email: wsmc@smccollough.com
Web: www.smccollough.com

October 15, 2007

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street SW
Room CY-B402
Washington, D.C. 20554

RE: Docket 07-52, *In the Matter of Broadband Industry Practices*
Notice of *Ex Parte* Meeting

Dear Ms. Dortch:

On behalf of Data Foundry, Inc., I hereby submit this notice of *ex parte* meetings held in the above-captioned proceeding, on the dates and involving the persons below indicated. At each meeting the Data Foundry representatives distributed the attached document, which served as the basis for discussion. All discussions that occurred were consistent with Data Foundry's prior-filed comments on this proceeding, with particular emphasis on but not limited to the legal ramifications of "tiered" broadband internet service and Deep Packet Inspection systems. The Data Foundry representatives in each meeting were Ron Yokubaitis, Founder and Chairman, Andy MacFarlane, Director of Governmental Affairs, and Scott McCollough, General Counsel.

October 10, 2007:

Presentation to Chris Moore, Legal Advisor to Commissioner Tate
Presentation to Scott Bergmann, Legal Advisor to Commissioner Adelstein
Presentation to Marcus Maher, Nick Alexander, Christi Shewman, Jeremy Miller, and Heather Hendrickson of the Wireline Competition Bureau

October 11, 2007:

Presentation to Scott Deutchman, Legal Advisor to Commissioner Copps
Presentation to Kevin Martin, Chairman, and Aaron Goldberger, Legal Advisor to Chairman Martin

October 12, 2007:

Presentation to John Hunter, Senior Legal Advisor for Commissioner McDowell
Presentation to Mary Beth Murphy, Alison Neplokh, John Norton, Jeffrey Neumann, Holly Saurer, John Wong, and Michael Lance of the Media Bureau

Sincerely,

W. Scott McCollough
Counsel for Data Foundry, Inc.

Note

Tiered Internet Service Threatens the Privileged and Confidential Nature of Online Communications

by Matthew A. Henry

I. Introduction

The comment period for the FCC's Notice of Inquiry into broadband industry practices recently closed with a remarkable 27,000-plus comments submitted by interested parties.¹ The Notice of Inquiry was in response to an outcry against the planned implementation of a "tiered" Internet service by several major Internet access providers (IAPs).² Internet content hosts, users, consumers, and others fear that such an IAP service would be used to monitor Internet traffic and degrade access to information not sponsored or approved by the IAPs. The tiered service dispute has now taken center stage within the wider "Net Neutrality" debate.³

In the media, the dispute has been framed as pitting wealthy and influential special interest groups against each other. On one side are content hosts like Google and Microsoft, and on the other side are the access providers, such as AT&T and Time Warner. The positions of the opponents have been reported as philosophical and economic arguments over the nature of the

¹ See ECFS Comment Search, http://fjallfoss.fcc.gov/cgi-bin/websql/prod/ecfs/comsrch_v2.hts?ws_mode=retrieve_list&id_proceeding=07-52 (last visited August 8, 2007).

² Verizon and Verizon Wireless Comments at 40. *In the Matter of Broadband Industry Practices* (WC Docket 07-52). Available at http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_Document=6519529411 (last visited August 8, 2007).

³ Net Neutrality is an amorphous political term without a consensus definition. The Congressional Research Service described Net Neutrality as the principle that "owners of the networks that compose and provide access to the Internet should not control how consumers lawfully use that network; and should not be able to discriminate against content provider access to that network" (See CRS Report for Congress, *Net Neutrality: Background and Issues*. Available at <http://www.fas.org/sgp/crs/misc/RS22444.pdf> (last visited August 27, 2008)). The political Net Neutrality debate centers on the question of whether federal regulation or a free market is the better mechanism for realizing this principle. While this note uses the phrase, the author notes that from a customer or user perspective the issue is really about the extent to which broadband users will continue to have a wide range of choices with regard to the applications and services they can employ and the devices they can attach and use in association with broadband. This note, however, addresses an issue of even far greater importance: whether tiered service will directly eliminate customers' right to privacy and eviscerate all privileges over information that is transmitted and/or received over broadband.

Internet, whether it should be “regulated,”⁴ and to what extent. The advocates of Net Neutrality oppose tiered service, arguing that it would stifle the open nature of the Internet and grant the IAPs too much control over content, services, applications, and the devices used to attach to broadband Internet. The advocates of tiered service hail packet prioritization as the next step in the evolution of the Internet, a step that will efficiently manage the increasing use of bandwidth on a network infrastructure that is becoming overloaded.

What is largely missing from the debate is an analysis of the legal implications for the users and customers, should the IAPs establish tiered Internet service. This note will examine those ramifications, specifically focusing on how tiered service would affect the expectations of privacy in one’s use of the Internet. This note will argue that the IAP collection, inspection, and prioritization of all network traffic will lead to the waiver of all customer privacy expectations and transform legally privileged and confidential communications into access provider business records. As such, these records would be potentially subject to release at will, or available from the IAP through a third party civil or criminal subpoena upon a showing of mere relevance.

II. The Tiered Internet Service Debate

The growing dispute over tiered Internet service has emerged in response to the plans of several IAPs to charge content hosts for prioritized delivery. Former AT&T Chief Executive Officer Edward Whitacre made this intention clear in an interview with BusinessWeek Magazine. In responding to a question about competition from content hosts, Whitacre said:

Now what they would like to do is use my pipes free, but I ain’t going to let them do that because we have spent this capital and we have to have a return on it. So there’s going to have to be some mechanism for these people who use these pipes to pay for the portion they’re using. Why should they be allowed to use my pipes?

⁴ Those in favor of some regulation are not actually attempting to regulate *the Internet*. The contemplated regulation would apply to those who control the gateway to the Internet because they own the physical infrastructure (for the most part the local distribution or “last mile” portion) that is used to access the Internet.

The Internet can't be free in that sense, because we and the cable companies have made an investment and for Google or Yahoo! or Vonage or anybody to expect to use these pipes [for] free is nuts!⁵

What Whitacre is proposing is a novel way to interpret the relationship between access providers and content hosts. Traditionally the two have been considered to be in a somewhat symbiotic business relationship that brings the Internet to the public. Each offers a product that depends on the other, which the users and customers access simultaneously. Instead, Whitacre is asserting that content hosts are essentially free riders using IAP bandwidth, and that there should be "some mechanism" in place to charge the content hosts as customers. That mechanism would be a tiered Internet. The access providers' current justification for tiered service, however, is notably different than Whitacre's.

According to the IAPs, traffic prioritization has become necessary to prevent the growing bandwidth demands of today's Internet users from outstripping the underlying infrastructure.⁶ The providers claim that their networks are running at 75% of capacity and rising,⁷ and that this traffic overload is responsible for the slowdowns that users see.⁸ Compounding the problem, according to the access providers, is that simply building more network facilities to keep pace with bandwidth usage would be so costly that Internet service would become prohibitively

⁵ Patricia O'Connell, At SBC It's All About "Scale and Scope", BusinessWeek.com, November 7, 2005, http://www.businessweek.com/@@n34h*IUQu7KtOwgA/magazine/content/05_45/b3958092.htm (last visited August 9, 2007).

⁶ AT&T Comments at 5. In the Matter of Broadband Industry Practices (WC Docket 07-52). Available at http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6519529324 (last visited August 8, 2007).

⁷ AT&T Reply Comments at 43. In the Matter of Broadband Industry Practices (WC Docket 07-52). Available at http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6519558101 (last visited August 8, 2007).

⁸ Traffic slowdowns may also be caused by one or any number of other unrelated problems, including slow local networks or problems within network servers.

expensive for most users.⁹ To remedy this imminent bandwidth shortage the IAPs plan to introduce a tiered Internet service and charge content hosts for prioritized delivery.

The content hosts counter that these claims of bandwidth saturation are an ISP-manufactured crisis, used as a pretext for double charging traffic and curtailing infrastructure investment.¹⁰ According to the content hosts, the service provider research substantiating their contentions is biased and self serving.¹¹ Content hosts argue that the IAPs have deliberately oversold their networks and the proper remedy would be network expansion and prorated user billing, rather than charging nonsubscribed content hosts.¹²

Again, what is missing in all these arguments is what it means to the users that the access providers are trying to lock up. The users subscribe to broadband to access the Internet and to send and receive information. They may be Mr. Whitacre's pipes, but the information presently belongs to the users or entities other than the IAPs. Mr. Whitacre was implicitly assuming that he owns the pipes *and* the information. To the extent he did not realize at the time that he had yet to obtain some ownership interest in the content, his goal appears to be to ultimately obtain ownership and control. The result would be a complete loss of privacy for all broadband users.

III. The Mechanics of Packet Prioritization

⁹ AT&T Comments at 33.

¹⁰ Google Comments. In the Matter of Broadband Industry Practices (WC Docket 07-52). Available at http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6519529458 (last visited September 10, 2007).

¹¹ The research studies referenced by the IAPs to show that bandwidth usage is increasing at a rate too fast for network construction were either conducted by or were in some way funded by the IAPs themselves. See, AT&T Comments at note 84 (Referencing a publication from the Phoenix Center for Advanced Legal & Economic Public Policy Studies, an organization funded in part by AT&T and the Bells; a publication by Richard N. Clarke, AT&T's Director of Economic Analysis; and a publication by Steven Pociask, the former Chief Economist for Bell Atlantic (now Verizon)); AT&T Reply Comments at note 139 (Referencing two publications each composed by the same five authors, three of which are AT&T employees and a fourth that is a recipient of research funding from AT&T).

¹² Google Comments at 24.

A tiered Internet can be analogized to a tollway. The first tier is a fast lane and the second tier is a slow lane.¹³ The traffic from content hosts that pay the toll will receive priority and access to the fast lane, and traffic from those that do not will be relegated to the slow lane. The predicament content hosts face with prioritization is that bandwidth availability is a zero sum game. As some content hosts purchase unequal portions of bandwidth, those that are unwilling or unable to pay will lose their share at the same rate. This decrease in bandwidth may cause increased latency and packet loss, resulting in the user experiencing degraded service when accessing non-prioritized content, applications, or services. Many content hosts would have to decide between being forced to the slow lane and losing bandwidth or purchasing priority access and remaining competitive.

To perform packet prioritization, the IAPs must necessarily examine all traffic before selecting either the fast or slow lane. To do so, the IAPs will implement Deep Packet Inspection (DPI) in association with systems such as IP Multimedia Subsystems. DPI and associated programs work as a filter, scrutinizing and recording the contents of each packet of information and applying IAP-supplied criteria to determine the assigned priority. All Internet traffic that travels the access provider network, from low bandwidth applications such as email to bandwidth intensive applications like video downloading, will go through this procedure.

The DPI process is critically important for privacy interests because the access providers would no longer be blindly passing traffic across their networks on a first come, first served (“best efforts”) basis. Instead, the IAPs would, in the standard course of operations, be accessing customer traffic and making real-time network resource allocation decisions based upon the

¹³ This is an admittedly simplistic analogy. Content would be prioritized based on several criteria (including application, destination/origination, and content host status) and allocated a predetermined amount of bandwidth. The end result, however, is that like traffic will be segregated into two categories: prioritized (fast lane) and non-prioritized (slow lane).

content that is being conveyed. This would mark a fundamental change in the relationship between the access providers and their customers.

IV. The Effect of Third Party Access Upon Expectations of Privacy

The IAPs have always had some ability to view and access the user information that traverses their network. Information is placed in the possession of the access provider and entrusted for delivery to the intended destination. The IAPs have generally not unilaterally accessed this information, however, because they have had few business related reasons to do so, until now.

Internet privacy considerations are significantly complicated by the potential for third party access by the IAP. As a general legal rule, knowledge of third party access waives any expectations of privacy in one's personal information.¹⁴ Two criteria are centrally important in determining whether the rule applies; the *purpose* for which one provides access to the third party and the access *practices* of the third party.

A. The Third Party Doctrine

The general third party rule, which forecloses any privacy interests in information available to a third party, originated from a pair of Supreme Court decisions from the late 1970's dealing with business records, *United States v. Miller*¹⁵ and *Smith v. Maryland*.¹⁶ The *Miller*

¹⁴ See Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & Tech. 1 (2007) ("The third party doctrine provides that information 'knowingly exposed' to a third party is not subject to Fourth Amendment protection because one 'assumes the risk' that the third party will disclose that information to the government. Under this test, constitutional privacy interests in information are both bright and binary. It does not matter if the information is exposed for a limited purpose, or in confidence; it matters only whether the individual should know the information was made available to another party.").

¹⁵ *United States v. Miller*, 425 U.S. 435 (1976).

¹⁶ *Smith v. Maryland*, 442 U.S. 735 (1979).

Court ruled there can be no expectations of privacy in one's bank records,¹⁷ while in *Smith*, the same was held for dialed telephone numbers.¹⁸ The Court reasoned that one who provides information for "legitimate business purposes,"¹⁹ which is acted upon in "the ordinary course of business,"²⁰ assumes the risk of disclosure by the third party. This risk applies "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."²¹ If Internet traffic were to be held to this standard, one could not expect the contents of one's communications to remain private. There is, however, an exception to this doctrine, which protects a great deal of private communications.

B. Content-Envelope Distinction

Privacy expectations in communications facilitated by third parties are often determined under the content-envelope exception to the third party rule.²² This exception makes a distinction between information that is openly viewable and information that is hidden from the third party. As the name suggests, information analogized to that on the outside of a mailed envelope is held to a different standard than the contents.²³ The envelope information receives no privacy

¹⁷ *Miller*, 425 U.S. at 443 ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities...").

¹⁸ *Smith*, 442 U.S. at 743 ("Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.")

¹⁹ *Smith*, at 744.

²⁰ *Miller*, at 442; *Smith*, at 744.

²¹ *Miller*, at 443.

²² See Lawless, *supra* note 11.

²³ Those participating in the debate over so-called "Net Neutrality" rarely define what they mean by "content." The meaning of the term can vary depending on the specific topic under debate. Usually they mean merely the "payload" information that is the purpose of the communication, and not other information including the

protection because it is within the plain view of the postal service and is necessarily inspected and acted upon to ensure the delivery the sender intended. The contents within the sealed envelope, on the other hand, are not generally viewed in the regular course of business and are wholly unrelated to the delivery process. The sender can reasonably expect the contents to remain private and free from viewing throughout delivery.²⁴ It is essential here that the third party has no legitimate purpose in viewing the contents of the communication and, by practice, would generally not do so.

V. Privacy Expectations in Internet Communications

In applying the content-envelope distinction to electronic communications, the courts have analogized several modern technologies to the information on or within an envelope. The Supreme Court originally did so by determining that dialed telephone numbers are envelope information,²⁵ while audio constitutes protected content information.²⁶ Carrying the analogy over

“headers” in packets. The Electronic Communications Privacy Act defines “content” as “any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8). This statutory definition clearly goes beyond just the actual communication itself. “Content” can mean other information besides just the payload if that information allows one to gain an understanding of the information that is in the payload, because it bears on the “substance, purport or meaning.” The Communications Act uses the terms “content” in many places, but has no express definition. See §§ 153(43), 220(c), 223(e)(1) and (h)(3), 225(d)(1)(F), 230(c) and (e), 274(h)(2), 275(d), 303(w), 396(g)(1)(D), 398(c), 611(c)(2), 613(e)(2), 614(b)(3), 615(g)(1), 624(f)(1), 640(b), 641(c) and 705(a). The author notes that the words in § 705(a) are strikingly similar to the ECPA definition of “content.”

²⁴ See *United States v. Choate*, 576 F.2d 165, 174 (9th Cir. 1978) (“[I]t is settled that the Fourth Amendment’s protection against ‘unreasonable searches and seizures’ protects a citizen against the warrantless opening of sealed letters and packages addressed to him in order to examine the contents.”) (Quoting *Ex parte Jackson* 96 U.S. 727, 733 (1877)); *Lustiger v. United States*, 386 F.2d 132, 139 (9th Cir. 1967) (“[F]irst class mail cannot be seized and retained, nor opened and searched, without the authority of a search warrant.”); *United States v. Jacobsen*, 466 U.S. 109 (1984); *United States v. Van Leeuwen*, 397 U.S. 249 (1970); see also *United States v. Boyd*, 2006 U.S. Dist. LEXIS 4795 (D. Mass. 2006) (An expectation of privacy in one’s mail also applies to private delivery companies, such as Federal Express).

²⁵ See *Smith*, 442 U.S. at 743.

²⁶ See *Katz v. United States*, 389 U.S. 347, 352 (1967) (“One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.”); *Zaffuto v. City of Hammond*, 308 F.3d 485, 489 (5th Cir. 2002) (“[T]he right to privacy in personal phone calls has long been established.”); *United States v. Sullivan*, 42 M.J. 360 (C.A.A.F 1995); *United States v. Sturdivant*, 13 M.J. 323 (C.M.A. 1982).

to Internet communications, e-mail information has been split much the same way.²⁷ The text and subject line of e-mail messages have been recognized as reasonably private content information,²⁸ while the to/from addresses and subscriber information are deemed unprotected envelope information.²⁹ Private communications on social networking websites have been similarly accepted as reasonably private content in nature and thus protected against discovery.³⁰ Additionally, IAP-stored search and URL records have likewise been held to constitute protected content information because they reveal the “‘substance’ and ‘meaning’ of the communication,” rather than just a destination.³¹ It is important to note that each of these determinations

²⁷ See *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) (“In a sense, e-mail is like a letter. It is sent and lies sealed in the computer until the recipient opens his or her computer and retrieves the transmission. The sender enjoys a reasonable expectation that the initial transmission will not be intercepted by the police.”); *United States v. Charbonneau*, 979 F.Supp. 1177, 1184 (D. Ohio 1997) (“E-Mail is almost equivalent to sending a letter via the mails.”); *Com. v. Proetto*, 771 A.2d 823 (Pa. Super. Ct. 2001). Of note, all of these cases recognized that disclosure of the contents of the communication by the recipient will effectively waive an expectation of privacy. This is consistent with the standard applied to letters and telephone conversations.

²⁸ See *Warshak v. United States*, 490 F.3d 455, 473 (6th Cir. 2007) (“[I]ndividuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial [IAP]. The content of e-mail is something that the user ‘seeks to preserve as private,’ and therefore ‘may be constitutionally protected.’”) (Quoting *Katz*, 389 U.S. at 351); *Maxwell*, at 418; *United States v. Long*, 64 M.J. 57, 62 (C.A.A.F. 2006); *Wilson v. Moreau*, 440 F.Supp.2d 81, 108 (D.R.I. 2006); 18 USCS §2510(8).

²⁹ See *United States v. Forrester*, 2007 U.S. App. LEXIS 16147 (9th Cir. 2007) (“[E]-mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communication. Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages...”); *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) (“Courts have applied [the content-envelope distinction] to computer searches and seizures to conclude that computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator.”).

³⁰ See *T.V. v. Union Township Board of Education*, 2007 ILRWeb (P&F) 1840 (N.J. Super. Ct. 2007) (Held plaintiff maintains a reasonable expectation of privacy in communications between private MySpace and Facebook user accounts.).

³¹ See *In re United States for an Order Authorizing the Use of a Pen Register & Trap*, 396 F.Supp.2d 45, 49 (D. Mass. 2005) (“A user may visit the Google site. Presumably the pen register would capture the IP address for that site. However, if the user then enters a search phrase, that search phrase would appear in the URL after the first forward slash. This would reveal content ... The ‘substance’ and ‘meaning’ of the communication is that the user is conducting a search for information on a particular topic.”).

recognizing user privacy expectations depends upon the private communications remaining free from regular IAP access and review.³²

In *Warshak v. United States*,³³ the U.S. Court of Appeals for the Sixth Circuit explained exactly how access provider actions could undermine the protection of the content-envelope distinction for Internet communications. The court noted that, in general, IAP terms of service only permit access in extraordinary circumstances outside the normal course of business.³⁴ This limited access justifies the users in believing their communications will remain private.³⁵ However, should the terms of service foreclose any user privacy interests or provide notice to the customer that his traffic will be subjected to “wholesale inspection, auditing, or monitoring”³⁶ during the regular course of business, any expectations of privacy against IAP access would be waived.³⁷ If there is no privacy with regard to the IAP, the court noted, the user cannot claim a privacy interest against a third party or government subpoena.³⁸ In other words, a user’s knowledge of the access provider’s comprehensive collection and inspection system will strip away *all* expectations of privacy and subject Internet communications to the application of the Third Party Doctrine, rather than the content-envelope distinction.

³² Internet communications that are public in nature, such as those on message boards, public chat rooms or blogs, will not maintain a reasonable expectation of privacy. See *Maxwell*, 45 M.J. at 419; *Charbonneau*, 979 F. Supp. at 1185; *Com. v. Proetto*, 771 A.2d at 831.

³³ 490 F.3d 455 (6th Cir. 2007).

³⁴ *Id.*, at 474 (Because the [IAPs] right to access e-mails under these user agreements is reserved for extraordinary circumstances, much like the university policy in *Heckenkamp*, it is similarly insufficient to undermine a user’s expectation of privacy. For now, the government has made no showing that e-mail content is regularly accessed by [IAPs], or that users are aware of such access of content.”)

³⁵ *Id.*, at 471 (“Like telephone conversations, simply because the phone company or the [IAP] could access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the [IAP] or the phone company will not do so as a matter of course.”).

³⁶ *Id.*, at 474.

³⁷ *Id.*, at 473 (“This factual determination tracks the language from *Miller* and *Phibbs* that suggests a privacy interest in records held by a third party is only undermined where the documents are accessed by the third party or its employees ‘in the ordinary course of business.’”) (Quoting *Miller*, at 442).

³⁸ *Id.* (“Where there is such an arrangement, compelled disclosure by means of an SCA order directed at the ISP would be akin to the third party subpoena directed at a bank as in *Miller* and *Jerry T. O’Brien*.”).

VI. The Contractual Loss of Privacy in ISP Terms of Service

In order to implement Deep Packet Inspection and tiered service, IAPs will undoubtedly be changing their terms of service and privacy policies to appear much like the standard contemplated by the *Warshak* court. These changes will provide notice to customers that the access provider may and will collect and inspect all traffic. AT&T, for example, revised its Internet privacy policy in 2006 to declare user Internet records company property and to reject any user expectations of privacy as against the access provider. The policy states, “While your Account Information may be personal to you, these records constitute business records that are owned by AT&T. As such, AT&T may disclose such records to protect its legitimate business interests, safeguard others, or respond to legal process.”³⁹ By staking a claim to this information, AT&T is turning these records into something more like the bank records of *Miller*, than a letter in the mail. Use of Deep Packet Inspection under such terms of service would destroy all expectations of privacy and render any communication processed by the access provider completely unprotected.

The AT&T privacy policy speaks of another business use, beyond bandwidth tiering, for customer Internet records. The statement reads, “AT&T uses Usage Information to personalize your Services, to recommend content, and to select advertisements or other promotions for you based upon your interests.”⁴⁰ While targeted advertising is not new to the Internet, how the IAPs plans to implement it will be. Deep Packet Inspection-facilitated advertisements will be constructed from the contents of user URL and search histories, financial transactions, downloads, or private e-mails. Considering the particularly personal nature of Internet usage,

³⁹ AT&T Privacy Policy for AT&T Yahoo! and Video Services, For All Applications, All Operating Systems, and All Domains, <http://helpme.att.net/article.php?item=8620> (last visited Aug. 17, 2007).

⁴⁰ Id.

these advertisements could be alarmingly well tailored to each individual. Because their terms of service foreclose any right of privacy against the IAP, customers subjected to such advertising would have little recourse.

Any IAP reassurance that post-DPI privacy policies remain robust and vigilant should be of little comfort for users. The revised AT&T Privacy Policy begins with this declaration:

Conducting business ethically and ensuring privacy is critical to maintaining the public's trust and achieving success in a dynamic and competitive business climate. Privacy responsibility extends not only to protection of customer account information but to the privacy of conversations and to the flow of information in data form.

This type of pledge, however, is a hollow promise as IAPs will soon be inspecting traffic in order to facilitate prioritization and targeted advertising. Internet records will constitute business records owned by the ISP and the *Miller* court made clear that regardless of any agreement or privacy policy to the contrary, one cannot maintain a privacy interest in the business records of another party.⁴¹ DPI will place Internet traffic squarely under the application of the Third Party Doctrine and users will lose any expectation of privacy in their Internet communications that they once had, or still believe they have.

VII. Waiver of Privilege through Consensual Inspection

With the loss of privacy in one's Internet traffic as to the IAP, Internet users will no longer be able to assert a legal privilege in their Internet communications because all privileged communications, both common law and statutory, depend upon a showing of confidentiality.⁴²

⁴¹ See *supra* note 16.

⁴² See *In re Horowitz*, 482 F.2d 72, 81-82 (2d Cir. 1973) ("It must be emphasized that it is vital to a claim of privilege that the communications between [parties] were made in confidence and have been maintained in confidence."); *United States v. Schwimmer*, 892 F.2d 237, 244 (2d Cir. 1989); *Bogle v. McClure*, 332 F.3d 1347, 1358 (11th Cir. 2003); *United States v. Melvin*, 650 F.2d 641, 645 (5th Cir. 1981); *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 255 (Bankr. D.N.Y. 2005).

The law of privilege is well settled on the issue⁴³ and replete with examples of waiver by voluntary disclosure to a third party and a consequent loss of confidentiality.⁴⁴

Most, if not all, privileged relationships have progressed to using the Internet for confidential communications. E-mail has become the preferred form of communication for many lawyers and their clients. Employees transmit company trade secrets to data storage facilities via the Internet. Physicians communicate with and diagnose patients by e-mail.⁴⁵ Psychologists and counselors also provide their services by chat and e-mail.⁴⁶ Priests and pastors are turning to the Internet to communicate in confidence with their church members.⁴⁷ Spouses, journalists, government officials, and others who typically maintain privileged relationships are all incorporating the Internet into their confidential communications under the assumption that no one will be reading, using, and reserving the right to disclose the contents.

⁴³ See Jennifer A. Hardgrove, *Scope of Waiver of Attorney-Client Privilege: Articulating a Standard That Will Afford Guidance to Courts*, 1998 U. Ill. L. Rev. 643, 653 (1998) (“Voluntary disclosure of a privileged communication constitutes a waiver in nearly all situations, even where the disclosure was nontruthful or misstated, where the disclosed information could have been obtained elsewhere, and where the third party receiving the disclosed information agreed not to further disclose it.”) (Emphasis added).

⁴⁴ See, e.g., *Wolfe v. United States*, 291 U.S. 7, 12 (1934) (Marital privilege waived through the use of a stenographer to transcribe a letter from husband to wife); *Westinghouse Elec. Corp. v. Republic of Phil.*, 951 F.2d 1414, 1427 (3d Cir. 1991) (Attorney-client privilege waived when confidential information was provided to a government investigation); *In re Grand Jury Investigation*, 918 F.2d 374, 386 (3d Cir. 1990) (Statements in the presence of a third party will generally waive the priest-penitent privilege. The exception being group confession); *Redding v. Virginia Mason Med. Ctr.*, 878 P.2d 483 (Wash. Ct. App. 1994) (Third party presence will waive the psychotherapist-patient privilege); *People v. Covington*, 19 P.3d 15, 20 (Colo. 2001) (Third party presence will waive the physician-patient privilege); *United States v. Lowe*, 948 F.Supp. 97, 100 (D. Mass. 1996) (Disclosure to a third party will waive the counselor-victim privilege).

⁴⁵ See, e.g., SxCheck website, <https://www.sxcheck.com/> (last visited August 22, 2007) (Website sells STI testing panels by mail and patient receives lab results by e-mail in order to provide a confidential process); AccurateMD website <http://www accuratemd.com/index.php> (last visited August 22, 2007) (Website prescribes medication through diagnoses by e-mail).

⁴⁶ See, e.g., Rape, Abuse & Incest National Network, National Sexual Assault Online Hotline, <https://online.rainn.org/index.aspx> (last visited August 22, 2007) (Website provides counseling to victims of sexual assault through a chat application); PsychologyCare.com, Online Psychology and Counseling Centre homepage, <http://www.psychologycare.com/index.html> (last visited August 22, 2007) (Website offers professional counseling through e-mail and chat communications).

⁴⁷ See, e.g., Christian Advice website, <http://www.myInternetpastor.com/> (last visited August 22, 2007).

The case law considering the privileged nature of Internet communications is not extensive but it is clear. Various courts have consistently held that e-mail is sufficiently confidential to maintain an assertion of privilege.⁴⁸ Necessarily, privileged e-mails are strictly confidential and without third party access. Had the holder of the privilege deliberately provided the e-mail to his access provider after actual or imputed notice that the content would be freely available for inspection; the case law would be much different. The communication would be considered knowingly disclosed and the privilege vitiated. When e-mail has lost its privileged nature, it will be subject to subpoena on a showing of mere relevance.⁴⁹

Deep Packet Inspection presents the prospect that lawyers conducting discovery in litigation will be within their rights, in light of their opponent's IAP terms of service, to compel production of all seemingly relevant Internet communications, regardless of any traditionally recognized privilege.⁵⁰ The target party or witness who knew that his traffic would be collected, inspected, acted upon, and claimed as service provider business records could not reasonably argue that his communications were confidential and undisclosed.

A discovery process that operates in this manner would have substantial ramifications for the many professional fields that depend upon the protection of a privilege. Doctors, attorneys, counselors, and priests would have to return to their pre-Internet communication practices to

⁴⁸ See *In re Asian Global Crossing, Ltd.*, 322 B.R. 247, 256 (Bankr. D.N.Y. 2005) (“[T]he transmission of a privileged communication through unencrypted e-mail does not, without more, destroy the privilege”); *City of Reno v. Reno Police Protective Ass’n.*, 59 P.3d 1212, 1218 (Nev. 2002) (“[A] document transmitted by e-mail is protected by the attorney-client privilege as long as the requirements of the privilege are met”); *Nat’l Employment Service Corp. v. Liberty Mutual Insurance Co.*, 1994 WL 878920 (Mass. Super. Ct. 1994); *Mold-Masters Ltd. v. Husky Injection Molding Systems*, 2001 WL 1558303 (N.D. Ill. 2001); *Curto v. Med. World Communs., Inc.*, 2007 U.S. Dist. LEXIS 35464 (D.N.Y. 2007); *Johnson v. Sea-Land Service*, 2001 WL 897185 (D.N.Y. 2001).

⁴⁹ See *U.S. v. Keystone Sanitation Co., Inc.*, 903 F.Supp. 803 (M.D. Pa. 1995).

⁵⁰ See Fed. Rules Civ. Proc. R. 26(b)(1) (“Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.”)(Emphasis added).

ensure confidentiality and encourage full disclosure by their patients, clients, or parishioners.⁵¹ In order to safeguard trade secrets, businesses would be forced to make sweeping changes to the ways that secret data is stored and communicated amongst employees. Should any of these practices fail to keep confidential information from service provider networks, waiver of privilege would be automatic. A situation such as this would very plainly mark a significant change to the law of evidence and a tremendous step backwards for Internet privacy.

VIII. Recognition of Public Policy Against Inspection of Confidential Communications Necessary for Judicial Recourse

Internet access provider contracts that authorize Deep Packet Inspection and waive customer privacy rights may well be considered inequitable and offensive. Customers may seek to challenge their terms of service on public policy grounds under state contract law.⁵² Such challenges would be difficult to maintain because current legislation has not yet recognized a public policy against enforcement of contracts that permit access provider inspection of communications.⁵³ Without relevant legislation or a FCC declaratory ruling establishing such a public policy, attempts to void these contracts as against public policy will likely fail.

⁵¹ The use of encryption applications could arguably provide a certain amount of protection against access provider inspection of confidential communications. There are several important problems with encryption that make it an unrealistic solution. First, there is no alternative infrastructure in place to securely distribute and authenticate public keys. Passing the key by mail or in person would often prove impractical and inefficient. Second, encryption is sparsely used within the general Internet using population because it has proved overly burdensome for the casual user. There is no universal standard and encryption applications are generally not included in software bundles. These obstacles, which have kept e-mail encryption from already gaining popularity, would prove troublesome in the context of privileged communications and make consistent use unlikely. Third, access providers have a material interest in penetrating user encryption. Because encryption would frustrate packet prioritization and targeted advertising, IAPs may choose to attempt decryption or ultimately prohibit user encryption in the terms of service and drop or degrade traffic that cannot be inspected.

⁵² Forum selection clauses within Internet service contracts usually mandate that claims and disputes to be litigated in one state where the access provider maintains facilities or offices. For example, AT&T terms of service require all claims to be filed in California.

⁵³ See, Restatement (Second) of Contracts §178 (1981) (Providing that a contract or term is unenforceable on public policy grounds when legislation provides that it is unenforceable or when the public policy against enforcement clearly outweighs the interest in enforcement).

The Notice of Inquiry into broadband industry practices presents an opportunity for the FCC to recognize and declare that IAP contract terms allowing the provider to examine content violates public policy and are not enforceable. Such a declaratory ruling would be consistent with the expectations and practices of the Internet using population. Should the FCC decline this opportunity, however, all individual Internet activities may well be considered public in nature and without any expectation of privacy.

The FCC cannot create privileges. Only Congress or the courts have that power. The FCC cannot overrule the judicial precedent and declare that notwithstanding DPI the privilege remains. It can, however, declare IAP contract terms to be contrary to public policy and unenforceable because they eliminate the public's present reasonable expectation of privacy. It can hold that DPI would decrease efficiency and harm the economy, in that privileged or confidential communications could not longer be transmitted over the Internet and maintain confidentiality.

IX. Conclusion

Access providers like to analogize packet prioritization to express mail.⁵⁴ When senders want expedited delivery, they can purchase priority treatment. This comparison is misleadingly benign and simplistic. A more accurate postal comparison would be a flat rate delivery service that opens each parcel, reads and records the contents for later advertising, and then assigns priority service only if the recipient or sender has purchased preferential treatment. Few would expect to maintain the confidentiality of their communications through such an intrusive process.

To the IAPs, the legal ramifications of packet prioritization are of minor consequence. For them, tiered service is an opportunity to increase revenues and cut costs with minimal

⁵⁴ See Verizon Comments at 42; AT&T Comments at 73.

investment. With few competitors and no federal regulation, the IAPs can implement this strategy, which is fundamentally inconsistent with the public interest, with little fear of customer backlash or government reprisal, while at the same time extolling the virtues of a free market.

The unintended consequences of packet prioritization will remain largely unnoticed as the tiered service debate is dominated by special interests. Wholesale Deep Packet Inspection threatens to quietly alter the landscape of the laws of privilege and evidence. Discovery will become a fishing expedition where lawyers can subpoena IAPs for the entirety of their targets' Internet records and communications, so long as they can show that production may lead to the finding of admissible evidence.⁵⁵ And with the watchful eye of the access providers reading and recording everything customers say and do, doctors, lawyers, spouses, government officials, and many others who depend upon their privileged relationships will be forced to find another means for communicating in confidence.

⁵⁵ See Fed. Rules Civ. Proc. R. 26(b)(1) *supra* note 45.