VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SUMMER 2011 UNIVERSITY OF VIRGINIA VOL. 16, NO. 02

What the Cops Can't Do, Internet Service Providers Can: *Preserving Privacy in Email Contents*

STEVEN R. MORRISON†

ABSTRACT

Legal rules have emerged that limit the State's right to search the contents of emails as they exist on Internet Service Providers' networks. Much attention has been paid to these rules, and they will continue to develop. What the State can't do, however, Internet Service Providers can. As private actors with incentives to search their users' email contents, ISPs can legally search some of the most personal online communication we engage in.

ISPs ought to be limited in their right to search email contents. In this article, I discuss the problem of ISP searches and possible solutions. I present three ways to address this problem: through statutory law, through constitutional judicial rulings, and through subconstitutional judicial rulings, specifically in tort. I conclude that a hybrid approach including statutory law and common law (either constitutional or otherwise) is the best way to ensure people's privacy interests and keep the law current. The last section of this article presents a model for a judicial ruling or statute that would protect users' email contents from being searched by ISPs.

Of all possible solutions, the most legally tenuous one is to issue a constitutional judicial ruling that holds that ISPs are state actors. I take on this particular challenge in detail, arguing that the public function,

† Steven R. Morrison teaches at the University of North Dakota School of Law. Thanks to the many people who provided invaluable comments for this article: Helen Norton, Alexander Tsesis, James Grimmelmann, Jelani Jefferson Exum, Robin R. Runge, Caylan van Larsen, Jan Stone, and Amanda Marie Lee.

entwinement, and assumption of risk doctrines all enable courts to conclude that the Fourth Amendment should limit ISPs.

ISPs currently search the contents of users' emails, have incentives to increase this practice, and work closely with law enforcement during these searches. With some exceptions, which I discuss, ISPs should not be able to invade users' privacy in this way.

The issue presented in this article is a small part of a large paradigm shift that is taking place in criminal procedure law today. This paradigm shift has been brought about by the advent of computers and the Internet, and it is doubtful that the law is keeping pace with new technologies. Whenever possible, therefore, courts ought to begin to make precedent-setting rulings in this field. Although courts and statutes have addressed the right of government agents to search email contents, this article is the first to propose that ISPs be treated as state actors for that purpose.

TABLE OF CONTENTS

I. INTRODUCTION

Billions of emails are sent each day. They include love letters, job inquiries, medical information, legal advice, and much more. Many of these emails contain sensitive information that the senders and recipients would prefer to keep private. Where we once sent physical letters through the post, email has become omnipresent, and is occupying the function that once belonged to the United States Postal Service.1 Our purpose in corresponding hasn't changed with technological developments, but our privacy under the law has. We have less privacy now that our personal letters have gone digital.

This development is largely an unintended consequence of technological innovation. But it is not completely undirected. Google, for example, has partnered with the Swedish Postal Service to provide advertising services to small businesses, and is planning to import the model to the United States.2 Governments are also forging closer ties to Internet Service Providers (ISPs) to facilitate criminal investigations.3 Internet Service Providers, as conduits through which our emails are sent (and sometimes as providers of email accounts), are increasingly acting as national postal services do. As a result, governments are asking ISPs to cooperate in criminal investigations. Even if governments didn't plan this decreased privacy in the digital age, they are taking advantage of it.

Although people understand that privacy in the digital age is in question, users aren't completely ready to abandon our expectation of privacy. If we don't think our Facebook accounts or forum postings are private, we generally believe that our emails are or should be private. After all, we use email to keep up with friends, send love letters, vent about our employer, discuss medical and legal issues, and so much more. And we know that our emails won't normally be viewed by anyone except the recipient.

The law ought to secure the privacy interest we have in the contents of our email.

---

[1] Brian Kane & Brett T. Delange, *A Tale of Two Internets: Web 2.0 Slices, Dices, and is Privacy Resistant*, 45 IDAHO L. REV. 317, 347 n.4 (2009); Kara A. Schiermeyer, *The Artful Dodger: Responding Parties' Ability to Avoid Electronic Discovery Costs Under 26(b)(2)(B) and 26(b)(2)(C) and the Preservation Obligation*, 42 CREIGHTON L. REV. 227, 227 (2009) ("…[T]he United States Postal Service anticipated delivery of 212 billion pieces of mail in 2006, while computer users were expected to send roughly sixty-two billion e-mail messages every day in 2006.").

[2] Bosse Andersson, *Google in new partnership with the Post*, EKOMONI, Oct. 20, 2010, http://www.dn.se/ekonomi/google-i-nytt-samarbete-med-posten-1.1192536 (last visited Dec. 8, 2010).

[3] Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES, Sept. 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=1 (last visited Dec. 8, 2010); Chris Williams, *ISPs to 'strengthen ties' with UK government*, THE REGISTER, Apr. 25, 2007, http://www.theregister.co.uk/2007/04/25/ispa_law_enforcement/ (last visited Dec. 8, 2010).

It is doing so against governmental searches, and a large body of scholarship has addressed the developing law in this area.[4] It should also do so as against searches performed by ISPs. This article explores the reasons why and ways that the law can and should address this emerging privacy concern. I want to focus narrowly on email contents that may be searched or seized by an ISP after the email has left the sender's computer but before it has arrived at the recipient's computer. The question is largely settled as to email existing solely in the sender's or recipient's computer. ISPs cannot reach these emails, and governmental searches are governed for the most part by traditional Fourth Amendment law.[5] The open question is what happens in between, while the email is being handled by ISPs. While being handled, how might the email contents be legally protected against searches by ISPs?

There are at least three ways that the law can address a particular circumstance. Courts can issue constitutional rulings (based, in the case of ISP searches, on the Fourth Amendment); courts can issue subconstitutional rulings (for example, developing tort law); and legislatures can enact statutes. A fourth solution, to let the market resolve problems, isn't a legal solution but bears mentioning.

In addition to these three primary ways to solve problems, hybrid approaches can be adopted. A legislature could pass a statute, and courts could interpret it (through either constitutional or subconstitutional opinions). Conversely, courts could advance the common law and legislatures could respond to it by passing legislation that reinforces, expands upon, or supersedes the new common law. In this article, I discuss all of these approaches.

I conclude that email users can be most protected from ISP searches of their email contents through a hybrid approach that combines statutory law and judicial action. I base this conclusion on the work of others who have explored the effectiveness of these various solution methodologies. The question of whether the judicial action involved

---

[4] *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. CHI. LEGAL F. 121 (2008); Marc Jonathan Blitz, *Stanley in Cyberspace: Why the Privacy Protection of the First Amendment Should be More Like That of the Fourth*, 62 HASTINGS L.J. 357 (2010); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007); Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700 (2010); Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 MICH. L. REV. 951 (2009); Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?* (Vand. Law. Sch. Pub. Law & Legal Theory Working Paper No. 10-64); CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (The Univ. of Chicago Press 2007).

[5] If the email remains on my computer and I haven't hit "send," then the Fourth Amendment protects that email from governmental searches and seizures just as it protects any letter in my home. United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers . . ."). If the email arrives into the recipient's computer, then I assume the risk that the recipient will disclose the contents of the email to law enforcement agents or anyone else. I no longer have any expectation of privacy in the email. United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) ("once the transmissions are received by another person, the transmitter no longer controls its destiny.").

should consist of constitutional (based on the Fourth Amendment) or subconstitutional (based on tort privacy law) rulings is a more difficult question. As we will see below, the answer to that question depends in part upon whether our goal is efficiency[6] (in which case we want to develop tort law) or justice (in which case we want to develop Fourth Amendment law). Efficiency and justice are not here mutually inclusive and, by pursuing one, we sacrifice part of the other. Of course, if we decide that a constitutional approach is preferable, we need to apply some exception to the state action requirement to bring ISPs, who are private actors, under the limitations of the Fourth Amendment.

As we shall see, although subconstitutional tort law may provide the judicial action half of the hybrid equation that best ensures email users' privacy, I explore heavily the application of constitutional Fourth Amendment law for three reasons. First, we have a fundamental privacy interest in our email contents that creates a question of justice rather than mere efficiency. Second, ISP activities in searching users' data, cooperation between ISPs and government agencies to uncover incriminating data, and the state action doctrine and associated law all suggest that ISPs can and should be limited by the Fourth Amendment. Third, among applying statutory law, tort law, and Fourth Amendment law to ISP searches of email contents, the most difficult one to argue for is Fourth Amendment law. The other two require only social impetus; the constitutional approach requires us to overcome the state action doctrine, which is neither uncontroversial nor easy.

And so I argue that for the purpose of the Fourth Amendment's application to email contents, ISPs can be treated as state actors. This proposal is based on the fact that ISPs, as handlers of email, are performing a traditionally governmental function.[7] It is also based on the fact that ISPs and governments are increasingly cooperating to perform criminal investigations. Their activities are becoming entwined,[8] and it appears that the future will see increased entwinement.[9]

---

[6] "Efficiency" as discussed in the pertinent literature is an economics term, and so may be difficult to apply literally to the question of ensuring privacy. I discuss this term below.

[7] *See* PruneYard Shopping Ctr. v. Robins, 447 U.S. 74 (1980); Marsh v. Alabama, 326 U.S. 501, 506 (1946); Smith v. Allwright, 321 U.S. 649, 664-65 (1944). ISPs are to be contrasted with companies like UPS and Fed Ex, who are not limited by the Fourth Amendment in their ability to search packages. *See* United States v. Robinson, 390 F.3d 853, 872 (6th Cir. 2004); United States v. Parker, 32 F.3d 395, 398 (8th Cir. 1994). The comparison between ISPs and UPS or Fed Ex is inapposite. The better comparison is between ISPs and the U.S. Postal Service. Both ISPs and the Postal Service are intended to provide basic access to means of communication. If you want to send a letter or email, you generally go to the post office or your ISP. UPS and Fed Ex provide "add-on" or enhanced services that are designed to go beyond services provided by the U.S. Postal Service. Their service hasn't pushed the Postal Service out of the market. ISPs, however, through the provision and/or facilitation of email, have done just that.

[8] Brentwood Academy v. Tennessee Secondary School Athletic Ass'n, 531 U.S. 288, 291 (2001).

[9] I acknowledge that the public function doctrine and the entwinement doctrine are problematic in many ways. The Supreme Court has, for example, said that "cases deciding when private action might be deemed that of the state have not been a model of consistency." Edmonson v. Leesville Concrete Co., 500 U.S. 614, 632 (1991). Others have called this area of

My proposal fits nicely with the approaches already taken by courts and commentators to limit government access to email contents. These approaches inquire into the proper legal and constitutional way that government actors can obtain email contents. They do not address the impact of ISPs—who are private actors—performing searches on their own and delivering evidence to government actors on a silver platter.[10] The blind spot is ISPs that can search users' email contents without restriction and are becoming key players in performing important governmental functions. ISP-initiated searches should be addressed because ISPs have incentives to perform independent searches of email contents.[11] They need to be limited in their right to perform such searches so that individuals' expectations of privacy in email contents can be protected. Individuals' email privacy does not need to be protected so that people may trade child pornography or use email to further a criminal conspiracy. Rather, email privacy needs to be protected because individuals use email to communicate personal, medical, legal, financial, and all sorts of other non-criminal, yet very sensitive, information. The reasons that we all enjoy privacy under the Fourth Amendment are the same reasons we should enjoy privacy in our email contents.

My proposal is limited to ISPs' searches of email contents. It leaves for another day the question of whether ISPs should have the right freely to search and seize instant messages, postings on websites and forums, text messages, and the many other forms of electronic communication existing today. These different forms of online communication are "public" and "private" to greater or lesser degrees, which would likely alter the analysis. Regarding electronic communications, there are, as one court argued, "complex, difficult, and 'far reaching' legal issues that we should be cautious about resolving too broadly."[12] Furthermore, the form and impact of many types of electronic communications are in constant flux and unknown, so we should hesitate to make precedent-setting law in such a dynamic environment.[13] Unlike these evolving forms of communication, email is relatively simple and stable. We can, therefore, declare what the law is concerning it.

---

law a "conceptual disaster area." Charles L. Black, Jr., *Foreword: "State Action," Equal Protection, and California's Proposition 14*, 81 HARV. L. REV. 69, 95 (1967). I discuss this problem below.

[10] *See* Elkins v. United States, 364 U.S. 206, 208 (1960) (rejecting the silver platter doctrine when the original search was illegal and performed by a governmental agency, but not when performed by a private actor).

[11] ISPs may wish to avoid liability for copyright infringement, *see* Josh Halliday, *LimeWire shut down by federal court*, THE GUARDIAN, Oct. 27, 2010, http://www.guardian.co.uk/technology/2010/oct/27/limewire-shut-down (last visited Dec. 8, 2010), or for facilitating the transmission of child pornography, Julia Scheeres, *ISP Guilty in Child Porn Case*, WIRED, Feb. 16, 2001, http://www.wired.com/culture/lifestyle/news/2001/02/41878 (last visited Dec. 8, 2010).

[12] Rehberg v. Paulk, 611 F.3d 828, 846 (11th Cir. 2010).

[13] What doesn't seem to be in flux is the ability of ISPs and the government to trace every electronic communication to a single computer based on its IP address. This uniform ability to track communications suggests the need to explore people's right to privacy and the stability of circumstances required to declare what the law is.

This article proceeds as follows: Part II describes the structure of the Internet as it relates to emails and ISPs. It also discusses the issues raised by this structure—in other words, why this article matters. Part III describes the existing law that addresses privacy protections in e-mail contents. This includes case law on the matter, the Stored Communications Act,[14] and the Wiretap Act.[15] This section suggests that judicial opinions haven't consistently addressed privacy concerns in email contents and that current statutory law is antiquated and thus unresponsive to actual needs. Neither case law nor statutory law suggests the possibility of ISPs being considered state actors when it comes to ISP searches of email contents. One recent Fourth Circuit case, *United States v. Richardson*,[16] comes close, but still falls short. This case and its rationale are described in detail below.

Part IV explores the use of statutory law, subconstitutional case law, and constitutional case law to address problems. It also suggests that a hybrid approach to ISPs searches of email contents is the ideal solution. I base this conclusion on the work of others who have found that where circumstances are changing rapidly (as forms of online communication are doing), a combination of statutory and case law is most likely to lead to an optimal legal regime. Part IV also discusses the relative merits of using constitutional (Fourth Amendment) and subconstitutional (tort) case law.

Part V discusses how ISPs can be considered state actors. I base my argument on the public function doctrine and, to a lesser extent, the entwinement doctrine. Part V also addresses the common retort to assertions of privacy protection in email contents: that e-mail senders assume the risk that ISPs will search the contents of the emails. It addresses additional counterarguments as well. Part VI presents a model judicial approach that can be used to address the problem of ISP searches of email contents. The conclusion places this Article's thesis in the broader context of the paradigm shift that criminal procedure law is currently undergoing. This paradigm shift has been brought about by quickly-changing social realities, central to which is the development of computers, cyberspace, and the digital communication that these technologies enable.

II. THE STRUCTURE OF THE INTERNET AS IT RELATES TO EMAIL; THE FOURTH AMENDMENT AND ISPS; DEFINING A "SEARCH"

A. The Structure of the Internet As It Relates to Email

Functionally, the Internet aims to provide "universal communication services."[17] Quite simply, it is a tool by which we can communicate just as easily with someone continents away as with a person one cubicle over from us. The time it takes to communicate a message is usually nearly identical in both cases and is amazingly short.

[14] 18 U.S.C.A. § 2701 *et seq.* (2010).
[15] 18 U.S.C.A. § 2510 *et seq.* (2010).
[16] 607 F.3d 357, 363-67 (4th Cir. 2010).
[17] BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION 83 (MIT Press 2010).

Structurally, the Internet "connects different physical networks."[18] These physical networks themselves provide connectivity among computers at companies, universities, or local areas.[19]

The Internet is a staggeringly large network to which individual computers like yours and mine are attached.[20] It has been referred to as a "super network connecting millions of" individual networks.[21] Our individual computers are not thought to be a literal part of the Internet.[22] Instead, the Internet is depicted visually in common culture by individual computers attached to the Internet—often itself depicted as a cloud—which is then connected to other individual computers.[23] The chain of communication over the Internet is generally illustrated as going from computer to Internet to computer.

Email is one of the many ways that digital messages are transferred from one individual computer (the sender), via the Internet, and carried by a number of ISPs, to another individual computer (the recipient).[24] Originally, emails were sent directly from the sender computer to the recipient computer. Both computers had to be online at the same time to complete the transfer.[25] Now, emails are sent using a "store-and-forward" model, in which emails are sent to an intermediary, such as an ISP, and sent on to the recipient when the transfer can be made.[26] The email message consists of the message header and message body.[27] The header contains control information such as the sender's and recipient's email addresses. The header has been analogized to a physical letter's envelope, which contains the mailing address of the sender and recipient of the letter.[28] The message body is like the letter itself.[29]

The process of sending an email can be broken down into five stages: (1) drafting

---

[18] *Id.* at 84.

[19] *Id.* at 83.

[20] Lockheed Martin Corp. v. Network Solutions, Inc., 141 F. Supp. 2d 648, 650 (N.D. Tex. 2001); VAN SCHEWICK, *supra* note 17, at 83; VINTON G. CERF, COMPUTER NETWORKING: GLOBAL INFRASTRUCTURE FOR THE 21ST CENTURY (1997), http://www.cs.washington.edu/homes/lazowska/cra/networks.html (last visited Jan. 25, 2011).

[21] *Lockheed Martin Corp.*, 141 F. Supp. 2d at 650.

[22] Lately, however, the increased communicative functionality of the Internet has allowed individual computers to become part of larger networks. The Search for Extraterrestrial Intelligence (SETI) Institute, for example, provides individuals with the opportunity to "loan" their computers' computing power to analyze radio waves received from outer space. The process is automated, and so individuals' computers can be said to be part of a network of computers dedicated to a massive amount of data analysis. SETI@home, http://setiathome.berkeley.edu (last visited Dec. 9, 2010).

[23] Wikipedia, *Internet*, http://en.wikipedia.org/wiki/Internet (last visited Dec. 9, 2010).

[24] VAN SCHEWICK, *supra* note 17, at 109.

[25] Wikipedia, *Email*, http://en.wikipedia.org/wiki/E-mail (last visited Dec. 9, 2010).

[26] VAN SCHEWICK, *supra* note 17, at 109.

[27] United States v. Vaghari, 2009 WL 2245097, at *8 (E.D. Pa. 2009).

[28] Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 905 (9th Cir. 2008); United States v. Hart, 2009 WL 2552347, at *22 (W.D. Ky. 2009).

[29] Courts have uniformly held that the email header is not subject to Fourth Amendment protection. *Id.* The email body, or content, is the subject is this article.

the email, (2) sending the email, (3) the transfer of the email over the Internet, (4) the receipt of the email, and (5) the ultimate disposition of the email. Imagine that you want to write an email to your partner who is on a business trip in another country. You go to your home computer, write your email, and hit "send." You know that the email is now travelling across the Internet to find its way to your partner's inbox. In a few moments, your partner receives notice, via an "unread email" entry in her email account's web page, that your email awaits her. She hits "read," and your email appears. Simple?

In reality, when it comes to privacy rules, this process is not so simple. Let's take the five steps in sequence:

(1) Drafting the email. It is settled that police must abide by the Fourth Amendment if they wish to obtain a file or email from someone's computer.[30] This rule is easily applied if, for example, you type your email in Microsoft Word, save it, and plan to cut and paste it into your email window at a later time. If you write your email in the email window, however, the question gets complex. The location of that email draft will vary based on the type of email you use. If you use Post Office Protocol (POP) email, and you save a draft of the email without hitting "send," that email will remain solely on your computer.[31] If you use Web-based email, such as Gmail, then that draft will be saved not on your computer, but on Google's servers.[32] If you use Interactive Message Access Protocol (IMAP) email, then your email draft will usually be saved on both your computer and on an external server.[33] Although it appears that state actors would have to abide by the Fourth Amendment to access your email draft if it exists on your computer, their ability to obtain it from ISPs, if it is stored on an ISP's server, is an open question.[34] ISPs are currently free to access that email on their own and turn it over to law enforcement. Privacy laws and the Fourth Amendment would not thereby be implicated.

(2) Sending the email. When you hit "send," your email will generally first be sent to your ISP's mail transfer agent (MTA).[35] This MTA will look at the email's

[30] United States v. Potts, 586 F.3d 823, 833 (10th Cir. 2009) ("the particularity requirement of the Fourth Amendment demands that '[o]fficers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant.'"); United States v. Forrester, 495 F.3d 1041, 1049-50 (9th Cir. 2007) (privacy interests in emails and letters are identical); United States v. Lifshitz, 369 F.3d at 190 ("Individuals generally possess a reasonable expectation of privacy in their home computers.").

[31] ITS Documentation, *How to Tell If You are Using IMAP or POP for Your E-Mail*, http://www.itd.umich.edu/itcsdocs/s4322/#what (last visited Feb. 12, 2011).

[32] Hon. M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth*, 85 N.Y.U. L. REV. 905, 922 (2010).

[33] Craig D. Ball, *E-Discovery: Right . . . From the Start*, SS006 ALI-ABA 247 (2010); Rob Pegoraro, *Internet Providers Should Find Their Way to IMAP*, WASH. POST, Mar. 21, 2004, http://www.washingtonpost.com/wp-dyn/articles/A10089-2004Mar20.html (last visited Feb. 12, 2011).

[34] *Lifshitz*, 369 F.3d at 190 ("Individuals generally possess a reasonable expectation of privacy in their home computers. . . . They may not, however, enjoy such an expectation of privacy in transmissions over the Internet . . .").

[35] United States v. Councilman, 418 F.3d 67, 69 (1st Cir. 2005).

destination address and access a domain name system (DNS) to determine where to send the email.[36] Using Simple Mail Transfer Protocol (SMTP), the MTA will send the email via other MTAs on its way to the recipient. Once you hit "send," however, this process does not automatically begin. You may, for example, order your email service to delay delivery of emails to the ISP for processing. In Outlook, this means that the email will be stored in your outbox for a specified time after you hit "send."[37] Between hitting send and the email actually being sent, the email remains on your computer. Presumably, this email would be subject to regular Fourth Amendment protection. Once the email is sent, it leaves your computer, enters the Internet, and may therefore not be protected.

(3) Transfer of the email over the Internet. To transmit data, including emails, Internet service providers use packet switching[38] and routing.[39] Packet switching involves breaking up larger packets of data (files, images, emails, etc.) into smaller ones to facilitate the transmission.[40] Routing involves determining the best route for these packets to take from the source computer to the destination computer.[41]

In a network that uses packet switching to transfer data, the sent email is first broken up into smaller pieces of data, called packets.[42] Each packet is labeled with its origin, destination, and sequential place in the original file.[43] The packets then begin their journey from the sender's computer to the recipient's computer.[44] There are millions of routes that packets can take to get from one computer to another computer.[45] Millions of routers on the Internet intercept packets, and determine where the packets should go to arrive at their destination as efficiently as possible.[46] Each packet will travel along a route different from its companions.[47] When the packets arrive at the recipient computer, the computer uses the packet information to reassemble the packets in the

---

[36] Jonathan Weinberg, *Site Finder and Internet Governance*, 1 U. OTTAWA L. & TECH. J. 345, 348 (2003-2004).

[37] Heather K. Kelly, *E-mail Disclaimers, Inadvertent Disclosures, and the Attorney—Client Privilege*, 39-MAY COLO. LAW. 97, 98 (2010); Microsoft Office, *Delay or Schedule Sending a Message*, http://office.microsoft.com/en-us/outlook-help/delay-or-schedule-sending-a-message-HP005242790.aspx (last visited Dec. 9, 2010).

[38] United States v. Szymuszkiewicz, 622 F.3d 701, 704 (7th Cir. 2010).

[39] VAN SCHEWICK, *supra* note 17, at 50-51, 85-86.

[40] *Szymuszkiewicz*, 622 F.3d at 704.

[41] VAN SCHEWICK, *supra* note 17, at 50-51, 85-86.

[42] PBS produced a simple but effective illustration of packet switching, found at *Packet Switching Demo*, http://www.pbs.org/opb/nerds2.0.1/geek_glossary/packet_switching_flash.html (last visited Dec. 9, 2010).

[43] *Id.*

[44] *Id.*

[45] Onion routing networks like Tor take advantage of these millions of paths to ensure users' privacy while transmitting data over the Internet. They prevent people from monitoring a user's Internet activity by routing her use in circuitous paths around the Internet. *See* Tor Home Page, http://www.torproject.org/index.html.en (last visited Feb. 12, 2011).

[46] *See* Widevine Technologies, Inc. v. Verimatrix, Inc., 2009 WL 3734106, at *1, 5 (E.D. Tex. 2009).

[47] *See generally* PBS, *Packet Switching Demo*, *supra* note 42.

correct order.[48]

When you send an email or other data over the Internet, you send it first to the ISP with which you have service. In large metropolitan areas, you probably have a wide choice of ISPs (Comcast, RCN, Qwest, etc.). Smaller cities or rural areas may be served by only one ISP.[49] That ISP doesn't cover the entire Internet. Instead, after you send your email to that ISP, it will forward your email to higher tier ISPs that cover more of the Internet.[50] Those ISPs may transfer the email to still higher tier ISPs, which will send the email on. At some point, higher tier ISPs will begin to send the email to lower tier ISPs until the email reaches its recipient from the ISP with whom the recipient has service.[51] With the exception of the ISP with whom we individually contract for service, we have absolutely no choice as to which ISPs handle our emails. Routers will determine the most efficient path for our emails, and will not discriminate based on ISP.

(4) Receipt of the email. The variations in email handling between POP, IMAP, and Web based email programs apply to the receipt of emails as well as the sending of them. Once an email is "received," a message will likely appear in the recipient's inbox ("you've got mail," "unread mail," etc.). The email may also not appear until the recipient actually attempts to download the message. At this point, it remains stored on a server outside of the recipient's computer.[52] Once the recipient hits "read," POP, IMAP, and Web based email programs will treat the email differently. In general, POP programs will download the email to the recipient's computer and delete it from any external server.[53] IMAP programs will save email on an external server, but may also download it to the recipient's computer.[54] Web based programs will, as their name suggests, store the emails on an external server.[55]

(5) Ultimate disposition of the email. Once the recipient hits "read," that email is either downloaded to her computer and deleted from an external server (POP email), downloaded and remains on the external server (IMAP email), or merely read on her screen and stored solely on an external server (Web based email). The recipient can print the email out and give it to law enforcement authorities, or show it to authorities on her computer screen. It is also possible that the recipient's screen shot will be cached on her

---

[48] *Id.*

[49] In 2010, 78% of Americans could choose between only one of two local ISPs and 13% had only one option. Rob Pegoraro, *Fast Forward: For now, there's little to do about a bad Internet provider*, WASH. POST, Apr. 18, 2010, at http://www.washingtonpost.com/wp-dyn/content/article/2010/04/16/AR2010041601316.html (last visited Feb. 12, 2011).

[50] *See* Brett Frischmann, *Privatization and Commercialization of the Internet Infrastructure*, 2 COLUM. SCI. & TECH. L. REV. 1, 37-38 (2001).

[51] *Id.*

[52] Ball, *supra* note 33, at 351; Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as Emails Get Dusty*, 88 B.U. L. REV. 1043, 1052-53 (2008).

[53] Alexander Díaz Morgan, *A Broadened View of Privacy as a Check Against Government Access to E-mail in the United States and the United Kingdom*, 40 N.Y.U. J. INT'L L. & POL. 803, 852 n.5 (2008).

[54] Craig Ball, *A Practical Guide to E-mail Discovery*, TRIAL, Oct. 2005, at 29, 31 (2005).

[55] Ball, *supra* note 33, at 367, 372.

computer without her knowledge or intent.[56] This screen shot will include anything on the recipient's screen, including the email content itself, the banner that says "Yahoo," "Gmail," "Outlook," etc., and, if the screen shot includes the recipient's address list or new mail inbox, this information will also be displayed.[57] Just as the law is settled regarding email contents existing on the sender's computer, the law seems clear that the sender loses her Fourth Amendment protection in email contents she has sent to a recipient and that exist on the recipient's computer.[58]

B. The Fourth Amendment and ISPs

During the last few years, around fifty billion non-spam emails were sent per *day*.[59] These emails travel over countless ISP networks, and their senders have no choice as to which ISPs handle them. Nevertheless, email users send love letters, medical information, business advice (including legal advice[60]), and more, and expect that this information will not be broadcast to law enforcement or the world.[61] Statutory and case

---

[56] United States v. Kuchinski, 469 F.3d 853, 863 (9th Cir. 2006); Ian C. Ballon, *IP and Internet Litigation: Law and Developing Trends*, 798 PLI/PAT 357, 386 (2004).

[57] *See* United States v. Fullmer, 584 F.3d 132, 154 (3d Cir. 2009); Mellon Investor Services, LLC v. Longwood Country Garden Centers, Inc., 263 F.App'x 277, 279 (4th Cir. 2008).

[58] *Lifshitz*, 369 F.3d at 190 (Senders "may not . . . enjoy . . . an expectation of privacy in . . . e-mail that [has] already arrived at the recipient."); United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) ("once the transmissions are received by another person, the transmitter no longer controls its destiny"). This email may simultaneously remain on an ISP's servers. I argue that even if an email exists on the recipient's computer, the sender has lost her expectation of privacy in that email, but retains her expectation of privacy in copies of that email that remain on an ISP's servers.

[59] Covad Commc'ns. Co. v. Revonet, Inc., 254 F.R.D. 147, 150 n.2 (D.D.C. 2008); *Internet 2009 in Numbers*, ROYAL PINGDOM, http://royal.pingdom.com/2010/01/22/internet-2009-in-numbers/ (last visited Dec. 10, 2010).

[60] Stengart v. Loving Care Agency, Inc., 973 A.2d 390, 402 (N.J. Super. Ct. App. Div. 2009) (emails exchanged by an employee and her attorney through her personal, password-protected, web-based email account were protected by the attorney-client privilege even though the emails were sent via the employer's computer and a version of the employer's handbook purported to transform the private emails into company property).

[61] If we don't believe we actually *have* privacy, the proliferation of email encryption services such as Pretty Good Privacy, http://www.pgp.com/ (last visited Dec. 19, 2010), the hubbub over the 2008 hacking of Sarah Palin's emails, Wikipedia, *Sarah Palin email hack*, http://en.wikipedia.org/wiki/Sarah_Palin_email_hack (last visited Dec. 10, 2010), and the persistent question of whether employers may access the emails of employees, Jared D. Beeson, *Cyberprivacy on the Corporate Intranet: Does the Law Allow Private-Sector Employers to Read Their Employees' E-mail?*, 20 U. HAW. L. REV. 165 (1998); Nicole Lindquist, *You Can Send This but Not That: Creating and Enforcing Employer Email Policies Under Sections 7 and 8 of the National Labor Relations Act After Register Guard*, 5 SHIDLER J.L. COM. & TECH. 15 (2009); Louis J. Papa & Stuart L. Bass, *How Employers Can Protect Themselves from Liability for Employees' Misuse of Computer, Internet, and E-mail Systems in the Workplace*, 10 B.U. J. SCI. & TECH. L. 110 (2004); Benjamin F. Sidbury, *You've Got Mail . . . And Your Boss Knows It: Rethinking the Scope of the Employer E-mail Monitoring Exceptions to the Electronic*

law address the extent to which law enforcement can obtain our email contents, but nothing is said about whether ISPs can do the same. The Internet today is not a space in which speech is constitutionally protected in the way we may think it is. Government actors cannot generally restrict our online speech, but the fact is that virtually the entire online universe is owned by private entities. These private entities can restrict speech and other online behavior with near impunity. Clay Shirky describes cyberspace as "a corporate sphere that tolerates public speech."[62] Internet intermediaries like Facebook, Twitter, and PayPal may be shutting down speech that they don't like,[63] and ISPs could conceivably follow. And they have every incentive to search emails for content they don't like.

For starters, although ISPs in the U.S. enjoy extensive freedom from liability for the actions of third parties who use their networks,[64] this may not be the case in other countries.[65] The issue is not necessarily settled in the U.S., with commentators calling for increased ISP liability when they fail to filter undesirable material.[66]

Political pressure may also be exerted on ISPs to filter certain content that is illegal. In some instances, there is even pressure to filter content that is legal but controversial. The recent Wikileaks saga saw governmental and private actors put pressure on companies such as PayPal, Amazon, MasterCard, and Visa to drop their services to Wikileaks.[67] As technology advances, ISPs may find it possible to search the contents of billions of emails sent over their networks and prevent their transmission.[68] If ISPs are not limited in their ability to monitor the content of their network traffic, there is

---

Communications Privacy Act, 2001 UCLA J.L. & TECH. 5 (2001), indicates that we think we *should* have privacy in the contents of our emails.

[62] Ashlee Vance & Miguel Helft, *Hackers Give Web Companies a Test of Free Speech*, N.Y. TIMES, Dec. 9, 2010, at B1, *available at* http://www.nytimes.com/2010/12/09/technology/09net.html?_r=1.

[63] *Id.*

[64] Broder Kleinschmidt, *An International Comparison of ISPs' Liabilities for Unlawful Third Party Content*, 18 INT'L J.L. & INFO. TECH. 332, 348 (2010).

[65] *Id.* at 338-41.

[66] *See* Matthew G. Jeweler, *The Communications Decency Act of 1996: Why § 230 is Outdated and Publisher Liability for Defamation Should be Reinstated Against Internet Service Providers*, 8 U. PITT. J. TECH. L. & POL'Y 3 (2007); Mark A. Lemley, *Digital Rights Management: Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 115-18 (2007); Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 222-25 (2006).

[67] Vance & Helft, *supra* note 62, at B1.

[68] This technology already largely exists. Sniffer programs can detect hash values associated with known images of child pornography, and can also be set to detect hash values of terms such as "Comcast sucks!" or "ten kilos of white for 20." United States v. Marchand, 308 F. Supp. 2d 498, 500 n.2 (D.N.J. 2004) ("A sniffer is a device that monitors internet traffic across a firewall and generates alerts based on packets of information or key words that cross the firewall."); State of New York, Office of the Attorney General, *Attorney General Cuomo Announces Expansion of Groundbreaking Initiative to Eliminate Sharing of Thousands of Images of Child Pornography on Social Networking Websites*, http://www.ag.ny.gov/media_center/2010/june/june21a_10.html (last visited Dec. 10, 2010).

a likelihood that emails that criticize ISPs, promote a controversial or unpopular political agenda, or otherwise threaten the ISP's bottom line may be restricted.[69] Currently, the law does not limit this ability.

It should. The architecture of the Internet today is built on an Open Systems Interconnection Model (OSI), which is comprised of seven different layers, each of which perform a certain task in transmitting data.[70] The bottom layer is the "physical layer," and consists of the hardware that makes up the Internet: modems, wires, copper cables, and so forth.[71] Internet backbone providers generally occupy the network and transport layers, which reside above the bottom physical layer.[72] The topmost layer is the application layer, which includes protocols, methods, and programs that consumers use to enable computer-to-computer communication.[73] Google's Gmail service operates at the application layer.[74] Google routinely scans email contents sent or received in Gmail in

---

[69] Comcast has, for example, monitored users' blogs in search of users' (negative) opinions about Comcast, ostensibly to provide better customer service. Iain Thomson, *Comcast Communicated by Blog*, PC & TECH AUTHORITY (July 26, 2008), http://www.pcauthority.com.au/News/117924,comcast-communicated-by-blog.aspx (last visited Jan. 15, 2011). Comcast's Privacy Policy suggests that it reserves the right to search email contents. *Web Services Privacy Policy: November 18, 2010*, COMCAST.NET, http://www.comcast.net/privacy/2010-11/ (last visited Jan. 15, 2011) (Comcast may access "content and data feeds from non-Comcast social networks or services that [the user] choose[s]"). Another ISP, Qwest, has a more explicit policy:

> **Network management**. We collect and use information generated on our networks to manage them and to keep our services running efficiently. For example, we monitor data to check for viruses, to control spam, to prevent attacks that might disable our services, to ensure that your traffic does not violate our Qwest High-Speed Internet Subscriber Agreement or our Acceptable Use Policy, and to guard against other inappropriate or illegal activity. This involves looking at the characteristics of our network traffic, such as traffic volumes, beginning and ending points of transmissions, and the types of applications being used to send traffic across our network. Sometimes we need to look into the content of the data (such as the specific websites being visited, files being transmitted, or application being used) for the purposes described above, in circumstances when we are concerned about fraud or harassment, to repair a problem we detect or that a customer contacts us about, or when we are providing the content of broadband traffic to law enforcement which we only do as authorized by law."

Qwest's Privacy Policy, QWEST, http://www.qwest.com/privacy/#collect (last visited Jan. 15, 2011).

[70] Padcom, Inc. v. NetMotion Wireless, Inc., 418 F. Supp. 2d 589, 592 (D. Del. 2006).

[71] *Padcom*, 418 F. Supp. 2d at 592; *See* Daniel L. Brenner, *Creating Effective Broadband Network Regulation*, 993 PLI/PAT 69, 93 (2010); James Grimmelmann, *The Internet is a Semicommons*, 78 FORDHAM L. REV. 2799, 2824 (2010).

[72] *See* J. Scott Marcus, *Evolving Core Capabilities of the Internet*, 3 J. TELECOMM. & HIGH TECH. L. 121, 132 (2004); Mark G. Milone, *Hacktivism: Securing the National Infrastructure*, 58 BUS. LAW. 383, 394 (2002).

[73] William F. Kroener, III, *Select Banking Topics of Current Importance: The FDIC Perspective*, SC78 ALI-ABA 1, 118 (1998); Christopher S. Yoo, *Beyond Network Neutrality*, 19 HARV. J.L. & TECH. 1, 14 (2005).

[74] *See* Grimmelmann, *supra* note 71, at 2823.

order to provide "customized content and advertising."[75] It does so at the application layer, [76] and it owns the application in which it performs these searches.

The process of deep-packet inspection[77] is similar in effect to what Google does, but enables ISPs (as opposed to Google, which is not, strictly speaking, an ISP) to look closely into a computer user's Internet activity, including email content. ISPs perform deep-packet inspection at different layers because they perform different functions than Google does. The effect, however, is the same. Deep-packet inspection is now being used to push user-specific advertisement.[78] To stop the accessing of pornography by employees in the workplace and kids at home, ISPs are able to detect such images, which are transmitted in part in emails.[79] Richard Clarke, the counterterrorism czar under Presidents Clinton and George W. Bush, suggested that ISPs could be compelled to look at the "digital format" of emails to stop cyberattacks.[80] The FBI has asked ISPs to search for illegal content on websites.[81] The British government has asked ISPs to track all emails passing over their networks.[82]

All of these searches would be acceptable if private entities never disclosed private, but legal, information to third parties; and if government actors never mistakenly or with malicious intent proceeded criminally against someone based on such information. The result would be that ISPs would disclose to law enforcement authorities only evidence of actual criminal activity, and the government would file charges only against people who actually committed the crimes charged. We do not live in this perfect system, so the Fourth Amendment and other law protects our privacy.[83] ISPs can, and

---

[75] *Online Profiling: DPI's Bad, Data Mining's Worse. What to Make of Google's E-mail Scanning*, NETWORK WORLD, Aug. 20, 2008, http://www.networkworld.com/columnists /2008/082008johnson.html.

[76] *See* VAN SCHEWICK, *supra* note 17, at 50.

[77] Deep packet inspection is an act that takes place somewhere between the sender's computer and the recipient's computer and can examine the content of an email for some predefined data set. VAN SCHEWICK, *supra* note 17, at 287, 371-72.

[78] Jeff Smith, *Deeply Personal New Marketing Model Can Track Web Activity, Profile User*, DENV. ROCKY MTN. NEWS, Sept. 22, 2008, *available at* 2008 WLNR 17994302.

[79] Vijay Thakur, *Image Analyzer for Porn-safe Surf*, STATESMAN (India), Oct. 2, 2006, available on Westlaw.

[80] *Richard Clarke: On the Growing 'Cyber War' Threat*, Interview with Terry Gross, National Public Radio (Apr. 19, 2010), *available at* 2010 WLNR 8680690.

[81] *Combatting Child Exploitation Globally*, US FEDERAL NEWS, Aug. 11, 2008, at 2008 WLNR 24460410.

[82] Dominic Casciani, *Plan to monitor all internet use*, BBC NEWS, Apr. 27, 2009, http://news.bbc.co.uk/2/hi/8020039.stm (last visited Jan. 15, 2011).

[83] For example, every image file has a particular hash value associated with it. Government agencies have databases of the hash values of known images of child pornography. ISPs can install programs to detect such hash values on their networks. This seems like a good idea. ISPs can also, however, use the same programs to detect the hash values of, say, iconic images of the World Trade Center as it burned on 9/11. ISPs could conceivably notice that these images were being sent from and received by a particular computer at a relatively high rate. The ISP could disclose this information to law enforcement, which might then initiate a terrorism investigation against the computer user. That user might have a legitimate reason for the prevalence of the

do, search the contents of emails. Often, they are cooperating closely with law enforcement to perform network searches.[84] The law, whether by statute, constitutional case law, or subconstitutional case law, should limit ISPs' right to do so.

It can. Courts have stated that whether someone has a reasonable expectation of privacy in the content of her email entails "complex, difficult, and 'far-reaching' legal issues that [courts] should be cautious about resolving too broadly."[85] This hesitancy is not based on whether people actually expect their email contents to remain private, but on the belief that email's role in society hasn't yet become clear.[86] Email's role *has* become clear and people *do* expect privacy in their email contents.[87] As for the technology of email, it has remained relatively stable since the advent of its widespread use in the late 1990s.[88]

Legislatures and courts can, and should, protect email contents while they exist on ISPs' networks. At the border between a sender's computer and the Internet, and a recipient's computer and the Internet, things get a little blurry.[89] For example, web-based email remains stored on ISPs' networks even after the recipient reads it. By contrast, POP email is generally downloaded onto the recipient's computer and disappears from the ISP's network. At this border, both types of email have different exposure to searches. For the government to search the POP email, it must get a warrant to search the user's computer. To search the web-based email, the government can proceed through the ISP based on less stringent rules. The problem with such differentiation is that email recipients generally don't consider web-based and POP emails as different from each other in any way, including in the level of privacy accorded to each.

---

image file, but may have to undergo an investigation, indictment, or even trial. Although an acquittal may follow, by undergoing the criminal process the computer user will have effectively been punished for possessing perfectly legal image files.

[84] *See* U.S. v. Richardson, 607 F.3d 357 (4th Cir. 2010), discussed below.

[85] Rehberg v. Paulk, 611 F.3d 828, 846 (11th Cir. 2010).

[86] *Id.*

[87] Ginger Gibson & J.L. Miller, *Sunlight bill faces likely amendments*, THE NEWS JOURNAL, Mar. 11, 2009, at 2009 WLNR 18259230 ("…[C]onstituents expect some measure of privacy in their e-mails to legislators."); Eric Goldman, *ABA Antitrust Section Consumer Protection Conference Recap*, TECHNOLOGY AND MARKETING LAW BLOG, July 7, 2009, at 2009 WLNR 12933598 ("consumers may expect greater privacy in email."); Vineetha Menon, *Self-destructing emails now a reality*, ARABIANBUSINESS.COM, Aug. 24, 2009, at 2009 WLNR 16459171 ("people [expect] the same privacy for e-mail and the Web that they expect for a phone conversation."); Patricia Smith & Kristin LaRosa, *Factors to Take Into Consideration When Drafting Electronic Communications Policies*, 201 N.J.L.J. 899 (2010); *Google is a friend in need for Yahoo!*, CYBER INDIA ONLINE LIMITED, Apr. 14, 2010, at 2010 WLNR 7886104 ("Society expects and relies on the privacy of e-mail messages just as it relies on the privacy of the telephone system.").

[88] Michael J. DeMaria, *Messaging & Collaboration – Look for stable communications technologies such as e-mail and videoconferencing to converge on the network with new collaboration media like blogs and podcasts*, NETWORK COMPUTING, Dec. 18, 2005, at 32, at 2005 WLNR 25480223.

[89] As, for example, the difference between POP, IMAP, and Web based email systems.

The law deals with blurry margins all the time. As for the issue at hand, a blanket rule that limits ISPs' right to search email contents while they exist on ISPs' networks is reasonable. Initially, as applied to POP and web-based emails, this rule would lead to some inconsistent results (received POP email would be treated differently than received web-based email, for example). Evolving common law would make these results consistent over time by clarifying and distinguishing the broad ruling limiting ISPs' right to search email contents.

A distinction ought to be made at this point between ISP searches of emails and searches by web-based email providers such as Gmail or Hotmail. ISPs provide access to networks and facilitate the transmission of all sorts of information. At their neutral best, they give access to "stupid networks" that don't discriminate based on data type.[90] ISPs are therefore seen in part as neutral conduits of information.[91] Web-based email providers like Gmail run applications over ISPs' networks. Each web-based email provider offers one small way for users to communicate over ISPs' networks. This changes the privacy analysis when it comes to ISPs or web-based email providers searching emails.

First, ISPs have an important role to play in structuring the Internet so that we all can effectively communicate. ISPs are, therefore, akin to common carriers, and their actions affect public speech, policy issues, and, ultimately, democracy itself. This is especially so because most people have very few choices when it comes to selecting ISPs. Web-based email providers, on the other hand, compete with innumerable other web-based email providers. If a user doesn't like that Gmail searches email contents to facilitate advertisements, she can use Hotmail. If she doesn't like Microsoft, and wants a more secure web-based email account, she can use Hushmail.[92]

ISPs are therefore like the U.S. Postal Service, and web-based email providers are like FedEx or UPS. The former play an important role in the dissemination of ideas, something the First Amendment was intended to promote. The latter provide "extra" services, tailored to users' specific needs. Because these are "extra" services, and because there is true competition in the web-based email arena, this article doesn't apply to searches performed by web-based email providers.

C. Defining a "Search"

A "search" of email contents can have many different definitions. For the purposes of this article, a search of email contents is defined as "any action taken whose function is to discern the body of an email and/or the substantive content of any

[90] David Isenberg, *Rise of the Stupid Network*, J. HYPERLINKED ORG., June 1997, http://www.hyperorg.com/misc/stupidnet.html.

[91] They are seen simultaneously as content producers, and obtain the benefits of both classifications. Rob Freiden, *Invoking and Avoiding the First Amendment: How Internet Service Providers Leverage Their Status as Both Content Creators and Neutral Conduits*, 12 U. PA. J. CONST. L. 1279, (2010).

[92] HUSHMAIL.COM, http://www.hushmail.com (last visited Feb. 18, 2010).

attachment to an email."

This definition includes searches by either actual people or computers.[93] It includes actions that discern the text in an email. It also includes actions that reveal the hash values of attached images, because the hash value can reveal the content of the image.

This definition does not include actions that reveal the source or destination of the email, the time or date it was sent or received, or the identity of the sender or recipient.

Despite these limitations, this definition of a search is broad. It covers, for example, searches that are specifically designed and limited to discerning *only* known images of child pornography—something one would, presumably, want to permit. Because this definition is so broad, this article envisions the possibility of writing exceptions into any law that would prohibit ISPs' right to search email contents.

III. CASE LAW; STORED COMMUNICATIONS ACT; *UNITED STATES V. RICHARDSON*

Courts have generally held that ISPs are private actors that are not subject to constitutional restrictions.[94] They have not foreclosed the possibility of applying tort privacy law to ISPs, and legislatures could also act to protect email contents. As for searches of email contents, courts have largely restricted themselves to considering whether and how law enforcement agencies—not ISPs—can get access to email contents. Courts have staked out three positions in this regard. One position is that people have *no* expectation of privacy in email transmissions over the Internet.[95] A second position is that privacy interests in email are protected just as strongly as are letters.[96] A third and seemingly dominant position leaves the issue unresolved for the time being.[97]

---

[93] It is possible, for example, for individuals at ISPs to focus on particular data transmissions or to set computer programs that flag certain keywords. These are just two ways that China manages Internet content within its borders. Philip Sohmen, *Taming the Dragon: China's Efforts to Regulate the Internet*, 1 STAN. J. E. ASIAN AFF. 17, 21 (2001).

[94] United States v. Richardson, 607 F.3d 357, 364 (4th Cir. 2010) (concluding that an internet service provider acted in a private capacity not subject to Fourth Amendment limitations); Green v. Am. Online (AOL), 318 F.3d 465, 472 (3d Cir. 2003) (stating that an internet service provider was not subject to the First Amendment's free speech guarantees because it was a private company and not a government entity); Noah v. AOL Time Warner, Inc., 261 F. Supp. 2d 532, 546 (E.D. Va. 2003) (stating there is no evidence that an internet service provider was a state actor).

[95] United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004).

[96] United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996); *See* United States v. Forrester, 495 F.3d 1041, 1049-50 (9th Cir. 2007).

[97] *See* Rehberg v. Paulk, 611 F.3d 828, 843 (11th Cir. 2010); Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 904 (9th Cir. 2008) ("The extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question."); Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007) ("individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP."), *vacated by* Warshak v. United States, 532 F.3d 521, 526-27 (6th

Statutory law also addresses law enforcement's ability to obtain email contents. The Stored Communications Act[98] and the Wiretap Act[99] are antiquated laws, and although there have been amendments and calls for additional amendments,[100] there is no indication that ISPs will be limited in their right to access email contents. Recently, the Fourth Circuit made a ruling that came close, but didn't quite touch upon the right of ISPs to search email contents. It will be helpful to detail this case.

A. United States v. Richardson

The defendant, Thomas Richardson, possessed and transferred to others images of child pornography via the Internet.[101] On appeal, he argued that AOL, an ISP with whom Richardson had an email account, discovered the images on behalf of the government, and thereby violated the Fourth Amendment.[102] The court rejected his claim and affirmed his conviction.[103]

AOL created a program, called an Image Detection and Filtering Process (IDFP), specifically for the purpose of detecting when subscribers use email to transfer images of child pornography.[104] The IDFP searches for hash values associated with images of

---

Cir. 2008) (issue of whether Warshak had a reasonable expectation of privacy in his email vacated as unripe. "The answer to that question will turn in part on the expectations of privacy that computer users have in their e-mails—an inquiry that may well shift over time, that assuredly shifts from internet-service agreement to internet-service agreement and that requires considerable knowledge about ever-evolving technologies.").

[98] 18 U.S.C.A. § 2701 *et seq.* (2010).

[99] 18 U.S.C.A. § 2510 *et seq.* (2010).

[100] Daniel B. Garrie et al., *Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?*, 29 SEATTLE U. L. REV. 97, 138 n.205 (2005); Jane E. Kirtley, *Privacy Protection, Safety, and Security*, 1027 PLI/PAT 15, 95 (2010); Scott Ness, *The Anonymous Poster: How to Protect Internet Users' Privacy and Prevent Abuse*, 2010 DUKE L. & TECH. REV. 8, 15 (2010).

[101] *Richardson*, 607 F.3d at 360.

[102] *Id.* (Richardson also claimed that the district court erred in granting AOL's motion to quash Richardson's subpoena seeking documents that would establish an agency relationship with the government with regard to the detection of AOL subscribers involved in child pornography.).

[103] *Id.* at 360, 371.

[104] Brief of Amicus Curiae Aol LLC in Support of Appellee United States of America for Affirmance at 1, United States v. Richardson, 607 F.3d 357, 360, No. 09-4072 (4th Cir. Oct. 26, 2009). This technology, designed specifically to detect relatively clear criminal activity, seems like a good idea. The Fourth Amendment, however, preserves every citizen's privacy by being a means-oriented, and not an ends-oriented, rule. The Fourth Amendment is not concerned so much with whether a search uncovers evidence of legal or illegal conduct, but rather with whether the search itself was done according to principles that ensure privacy for criminals and law-abiding people alike. This is why the Supreme Court held that the use of a thermal imaging device that, in effect, detected only marijuana growing operations in a home, violated the Fourth Amendment. Kyllo v. United States, 533 U.S. 27 (2001). This is also why the exclusionary rule is a remedy for Fourth Amendment violations—if the means of finding evidence of criminal activity violated constitutional principles, that evidence will be suppressed. This is also why we

apparent child pornography that AOL had previously found on its network.[105] A "match" indicates that an AOL user is attempting to send an email that contains an image of apparent child pornography.[106]

Once an image was found, the law at the pertinent time in *Richardson* required AOL to notify the government.[107] Once the IDFP made a match, the program automatically generated the required report and sent it to the appropriate government agency, along with a copy of the image.[108] AOL developed and implemented this program in order to "fulfill its legal obligation to report the transmission . . . of child pornography on its systems,"[109] and to prevent its networks from being used for criminal purposes.[110] It has "openly and as a matter of public record, joined in efforts among government" and other groups "to help suppress the possession, distribution, and exchange of child pornography."[111]

The United States argued that AOL's search did not violate the Fourth Amendment because AOL is a private actor, but that if the search did implicate the Fourth Amendment, it was reasonable because the search for the hash values of images of child pornography was not a search of "the actual content of the e-mail or attachments of its users."[112] The search

> merely screened the e-mail traffic for matches to numerical values of files "associated with known threats to its system," including contraband such as child pornography. If that screening process revealed a match to the hash values, or the "fingerprint," of a known child pornography image, the report of apparent child pornography was transmitted to NCMEC [the National Center for Missing and Exploited Children]. The intrusion into a user's privacy caused by this screening, then, is *de minimus*: in screening its e-mail traffic for contraband, AOL does not learn any personal

---

ought to be concerned that ISPs are searching the contents of our emails. By doing so, they will discover child pornography. They may also discover that one user is HIV positive, another user is about to sue her employer, and yet another user lost all his money to a gambling addiction.

[105] Brief of Amicus Curiae Aol LLC in Support of Appellee United States of America for Affirmance at 6, United States v. Richardson, No. 09-4072 (4th Cir. Oct. 26, 2009).

[106] *Id.*

[107] *Richardson*, 607 F.3d at 363.

[108] Brief of Amicus Curiae Aol LLC in Support of Appellee United States of America for Affirmance at 6, United States v. Richardson, 607 F.3d 357, 360, No. 09-4072 (4th Cir. Oct. 26, 2009).

[109] *Richardson*, 607 F.3d at 363 (internal quotations omitted).

[110] Brief of Amicus Curiae Aol LLC in Support of Appellee United States of America for Affirmance at 18, United States v. Richardson, 607 F.3d 357, 360, No. 09-4072 (4th Cir. Oct. 26, 2009).

[111] *Id.* at 20.

[112] Brief for the United States at 30, United States v. Richardson, No. 09-407 (4th Cir. Oct. 15, 2009).

> information about the user. Rather, at most, AOL learns that a given e-mail contained child pornography.[113]

In determining that AOL was not a state actor for purposes of the Fourth Amendment, the Fourth Circuit applied the test set forth in *United States v. Jarrett*.[114] In that case, the Fourth Circuit held that the key factors to determine whether a private actor engages in a government search are (1) "whether the government knew of and acquiesced in the private search," and (2) "whether the private individual intended to assist law enforcement or had some other independent motivation."[115] The court did not address the first, but found that there was "little evidence . . . to suggest that AOL intended to assist the Government in its case against Richardson."[116]

Richardson's petition for certiorari to the U.S. Supreme Court was denied.[117]

B. Analysis of *United States v. Richardson*

There are a number of questionable aspects of this opinion. First is the unfounded declaration by the United States that a search for hash values associated with images of child pornography is not a search of the contents of an email. Images contained in the text of the email or as attachments certainly are not part of the email *header*. However harmful and illegal these images are, they are patently part of the email *body*, or contents. A search for such hash values is not unlike a search for drugs by a drug dog (which is not a Fourth Amendment search)[118] or a search for a marijuana growing operation in a home by use of a thermal imager (which is a Fourth Amendment search).[119] By assuming that AOL's actions did not constitute a search of Richardson's email contents, the Fourth Circuit punted on an important and timely issue.

Furthermore, under the *Jarrett* analysis, it is possible that AOL *was* engaging in what constituted a government search. The Fourth Circuit didn't answer *Jarrett*'s first prong—whether the government knew of and acquiesced to AOL's search program—probably because it was obvious that the government did know of it and did acquiesce to it. The question, therefore, is whether AOL intended to assist law enforcement, or whether it had its own motivation for inventing and implementing the IDFP.

The United States claimed that AOL created and implemented the IDFP in order "to protect its network from contraband."[120] An AOL representative stated that AOL "simply 'screens the email traffic using numerical values associated with known threats

---

[113] *Id.*
[114] United States v. Jarrett, 338 F.3d 339, 344 (4th Cir. 2003).
[115] *Id.*
[116] United States v. Richardson, 607 F.3d 357, 365 (4th Cir. 2010).
[117] Richardson v. United States, 131 S. Ct. 427 (2010).
[118] United States v. Place, 462 U.S. 696, 707 (1983).
[119] Kyllo v. United States, 533 U.S. 27, 34-40 (2001).
[120] Brief for the United States at 19, United States v. Richardson, No. 09-407, 607 F.3d 357, (4th Cir. Oct. 15, 2009).

to its system, including computer viruses, worms, bots and contraband,' taking appropriate measures to remove the identified threats from its system."[121]

It is difficult to see why the transmission of images of child pornography is a threat to AOL's network in the way that viruses, worms, and bots are a threat.[122] The latter may actually harm AOL's network, while images of child porn present an external harm to society that governmental agencies have traditionally been tasked with detecting and preventing. In short, images of child porn—however unacceptable and harmful they are—are as insignificant a threat to AOL's network as are images of your friend's latest birthday party or pictures of a bicycle that you hope to sell online.

There is no doubt that AOL has an interest in preventing the trade in child porn via its network. However, the interest is in law enforcement and moral housekeeping, not in network security. If illegal pornography files frequently contained viruses that could damage the network, then ISPs could claim that they needed to search for such images to ensure network security. Digitally speaking, illegal images are no different than images of your summer trip to France.[123] If child porn were legalized tomorrow, it's a safe bet that AOL would cease use of its IDFP.[124]

The practical result of *Richardson* is that (1) we still have no judicial opinion on the right of ISPs to search the contents of emails existing on the ISPs' networks, and (2) it appears that courts are unwilling to limit ISPs' right to search. Moreover, courts will tend to find that ISPs are private actors, despite the fact that they work closely with law enforcement and often engage in activities traditionally dedicated to governmental agencies. The fact that ISPs perform such work over a network that facilitates the 21st century's main form of communication is further support for saddling ISPs with Fourth Amendment, or at least tort or statutory, restrictions. Although courts have not been willing to find that ISPs are state actors, the argument is there to be made. A limit on

[121] *Id.* at 8.

[122] Arguably, if AOL allowed child pornography to be transmitted over its network, people would be hesitant to use AOL for fear that they would inadvertently view this material. This probably isn't an actual concern, however. Child pornography is illegal, and people who trade in it have an interest in maintaining secrecy. It seems, therefore, that it would be extraordinarily difficult to accidentally stumble upon such illegal images.

[123] Such images are certainly more morally reprehensible than legal images. ISPs could legitimately argue that they seek to detect illegal images and disclose them to law enforcement because they are illegal *and* morally wrong. In the case of child pornography, few would probably fault ISPs for taking such a moral stance. In Richardson, however, the government did not claim that AOL used IDFP out of moral conviction.

[124] This is not to say that I am against the use of programs that detect the hash values of known images of child porn. We all have a great interest in stopping this harmful criminal activity, and targeted searches for these images may be a boon. It may be, furthermore, that if ISPs were limited in some way in their ability to search email contents, the searches performed by AOL's IDFP program would be excepted or deemed reasonable. Like the use of drug dogs, they may not be deemed Fourth Amendment searches at all. When ISPs do perform such searches, however, the Fourth Amendment, tort law, or legislation should have something to say about them.

ISPs' right to search email content is needed and is a reasonable step to take.

C. The Persistent Legacy of IDFP?

Despite my criticism of the Fourth Circuit's failure to inquire into whether AOL's IDFP program conducted a "search" of Richardson's email, I don't necessarily believe that IDFP did, in fact, perform a search that would be prohibited under my proposal.

As noted above, any prohibition on ISPs' right to search email contents may, and probably should, include exceptions. Because IDFP detected *only* known images of child pornography, it and similar technologies should be able to continue to operate.

Such exceptions should be carefully and narrowly crafted. IDFP is an easy exception because it detects only (1) clearly illegal activity that (2) is exceptionally harmful to the victims. When either of these two factors is absent, the law should tend toward protecting individual privacy.

For example, it should not be legal to set a program like IDFP to detect the phrase "bin Laden is awesome." There is nothing inherently illegal in this phrase, and it's likely to be written in a wholly innocent context.

As another example, an IDFP-type program should not be set to detect video files, the transfer of which comprises a copyright violation. The low level of harm doesn't justify the invasion of privacy.

Finally, the disclosure law at issue in *Richardson* would remain legal. It doesn't compel ISPs to perform any type of search. Furthermore, if ISPs were limited in their right to search email contents, and appropriate exceptions were in force, then the negative downstream effects (government investigations or indictments born from unacceptable privacy violations) would be eliminated.

IV. THE MERITS OF STATUTORY LAW, CONSTITUTIONAL CASE LAW, AND SUBCONSTITUTIONAL CASE LAW

There are a number of reasons why statutory law, constitutional case law, and subconstitutional case law each have relative advantages. These reasons are helpful to mention, but a deeper analysis is ultimately needed to arrive at the best mechanism for addressing the issue at hand. Economics work on the subject by Giacomo A. M. Ponzetto and Patricio A. Fernandez[125] provides good guidance, as does the more traditional legal work by Adrian Vermeule.[126] Let's pursue these two subjects in order.

Statutory law is said to have the following positive attributes: it anticipates future

[125] Giacomo A. M. Ponzetto & Patricio A. Fernandez, *Case Law Versus Statute Law: An Evolutionary Comparison*, 37 J. LEGAL STUD. 379 (2008).

[126] Adrian Vermeule, *Common Law Constitutionalism and the Limits of Reason*, 107 COLUM. L. REV. 1482 (2007).

conditions rather than responds to past controversies;[127] it can apply a broader swath of information and material that is often denied to a judge;[128] it can enjoy the benefits of consultation, negotiation, mediation, amendment, and improvement in ways that judicial opinions cannot;[129] it is clear, universal, comprehensive, and stable;[130] it is uniform;[131] it can provide for more rights than courts can provide;[132] and it is predictable.[133] Two drawbacks to statutory law are that statutory law may be inefficient due to the involvement of interest groups,[134] and that any change to legislation would need to be brought about by further legislation.[135]

Judicial action (leaving aside the difference between constitutional and subconstitutional action for a moment) is said to have the following positive attributes: it moves law toward efficiency by gradually evolving the law;[136] it prevents law from becoming an "antiquated straight jacket and then dead letter;"[137] it allows the law to be incremental, tentative, and thus experimental;[138] it promotes public confidence through the doctrine of stare decisis;[139] it can reflect local circumstances and values;[140] it responds to changing conditions and mores;[141] and it becomes part of people's common beliefs and

---

[127] Robert M. Ackerman, *Bringing Coherence to Defamation Law Through Uniform Legislation: The Search for an Elegant Solution*, 72 N. C. L. REV. 291, 329 (1994).

[128] Robert Sharpe, *Brian Dickson, the Supreme Court of Canada, and the Charter of Rights: A Biographical Sketch*, 21 WINDSOR Y. B. ACCESS TO JUST. 603, 623 (2002).

[129] *Id.*

[130] Hanoch Dagan, *The Craft of Property*, 91 CALIF. L. REV. 1517, 1565 (2003).

[131] Andrew J. Foti, *Contingency Fee Agreements: Remedying the Enormous Tax Burden of the AMT to Clients*, 1 BUS. L. BRIEF (AM. U.) 27, 30 (2004).

[132] Ira P. Robbins, *Lessons from Hurricane Katrina: Prison Emergency Preparedness as a Constitutional Imperative*, 42 U. MICH. J.L. REFORM 1, 65-66 (2008).

[133] Kyle C. Velte, *Towards Constitutional Recognition of the Lesbian-Parented Family*, 26 N.Y.U. REV. L. & SOC. CHANGE 245, 305 (2000-2001).

[134] Lyria Bennett Moses, *Understanding Legal Responses to Technological Change: The Example of In Vitro Fertilization*, 6 MINN. J.L. SCI. & TECH. 505, 561-62 (2005).

[135] Malcolm Sargeant, *New Transfer Regulations*, 31 INDUS. L.J. 35, 40 (2002) (claiming that this condition is actually an advantage of legislation).

[136] Richard Dagen, *Rambus, Innovation Efficiency, and Section 5 of the FTC Act*, 90 B.U. L. REV. 1479, 1530-31 (2010); Jonathan Klick & Francesco Parisi, *Wealth, Utility, and the Human Dimension*, 1 N.Y.U. J. L. & LIBERTY 590, 608 n.5 (2005); Aaron J. Rappaport, *Unprincipled Punishment: The U.S. Sentencing Commission's Troubling Silence About the Purposes of Punishment*, 6 BUFF. CRIM. L. REV. 1043, 1117 (2003).

[137] United States v. Standard Oil Co. of Cal., 332 U.S. 301, 313 (1947).

[138] Janet Cooper Alexander, *Do the Merits Matter? A Study of Settlements in Securities Class Actions*, 43 STAN. L. REV. 497, 586 (1991).

[139] Terry W. Frazier, *Protecting Ecological Integrity Within the Balancing Function of Property Law*, 28 ENVTL. L. 53, 66 (1998).

[140] James L. Huffman, *Beware of Greens in Praise of the Common Law*, 58 CASE W. RES. L. REV. 813, 828 (2008).

[141] Peter A. Alces & David Frisch, *On the UCC Revision Process: A Reply to Dean Scott*, 37 WM. & MARY L. REV. 1217, 1237 (1996); Cass R. Sunstein, *Law and Administration After Chevron*, 90 COLUM. L. REV. 2071, 2088 (1990).

is sanctioned by the people because of its "essential rightness."[142] Common law has been criticized as being reactive, not proactive.[143] In addition to the aforementioned drawbacks, any praise given to either a statutory or judicial solution implies an additional criticism of the other.

Less explored is the difference between constitutional and subconstitutional judicial action. Each has its own advantages and disadvantages. Constitutional common law rulings are said to safeguard individuals' fundamental rights against the vagaries of politics and administrative processes.[144] The relative permanence of constitutional rulings as compared with subconstitutional rulings may, however, be a drawback during times of rapid change. When the law intends to address such rapid change, relatively permanent rulings may hamstring subsequent courts from abrogating precedent in favor of more rights-protective solutions. It's easier to change tort law than it is to change Fourth Amendment law. There is, therefore, a trade-off. A Fourth Amendment ruling is protected from legislation and subsequent courts, but may limit lawmakers and courts from providing more or better privacy protection. A tort ruling isn't protected, but allows legislatures and subsequent courts to fashion better rules when new circumstances demand them.

This is not an absolute, non-negotiable trade-off: constitutional rulings can be distinguished or even overturned, and subconstitutional rulings, as precedent, enjoy respect and thus a degree of permanence. Therefore, the functional difference between the two types of judicial rule-making may be minimal.

What, then, is the best way to ensure individual privacy in email contents against ISPs' searches? The above lists of the advantages of legislation and common law don't help us very much. If we're predisposed to preferring legislation, then we find evidence that legislation is the best way to go. Similarly, if we're fans of judicial solutions, we'll find that courts are best suited to address the issue. A couple of studies have gone beyond a mere listing of relative advantages, offering insight that suggests a hybrid approach combining legislation and judicial action would work best.

A number of commentators have suggested that a hybrid approach to determining rights is generally most effective.[145] This approach may be especially effective when

---

[142] LON L. FULLER, LAW IN QUEST OF ITSELF 133-34 (1940).

[143] Sharpe, *supra* note 128, at 623.

[144] Abdullahi An-Na'im, *Challenging Liberalism on Its Own Rationale to Support an Affirmative Role for the State?*, 1 INT'L J. CONST. L. 741, 744 (2003) (reviewing MARTIN SCHIENIN, ED., WELFARE STATE AND CONSTITUTIONALISM: NORDIC PERSPECTIVES (2001); Michael T. Mullaly, *"'Til Death Do Them Part?": Assessing the Permanence of Goodrich*, 27 B.C. THIRD WORLD L.J. 499, 508 (2007).

[145] Neal Kumar Katyal, *Legislative Constitutional Interpretation*, 50 DUKE L.J. 1335, 1336 (2001) (claiming that the courts and the legislature have "comparative strengths," and so "[t]he institutional differences between the branches can be a source of richness, rather than a constitutional weakness."); Gerald Korngold, *For Unifying Servitudes and Defeasible Fees: Property Law's Functional Equivalents*, 66 TEX. L. REV. 533, 562-63 (1988).

dealing with "new and changing social contexts" like the Internet.[146] Giacomo A. M. Ponzetto and Patricio A. Fernandez present economic proof that this is the case, and Adrian Vermeule discusses the implications of the use of constitutional rulings compared with subconstitutional rulings.

Ponzetto and Fernandez argue that the common law in abstract is "a continuous, never-ending process of evolution of legal rules that is characterized by probabilistic convergence toward greater efficiency and predictability."[147] The problems with this abstraction are that Supreme Court decisions are shaped by ideology as much as by precedent,[148] and that precedent tends to hinder the common law's adaptation to changing circumstances.[149] One could add that where there is rapid social change, the common law will attempt to address a moving target, and thus never quite achieve efficiency.

The authors also observed that statutory law does not move the law toward greater efficiency, as case law does.[150] Although statutory law may provide "short-run certainty of the written law,"[151] "the convergence of case law [toward better rules] makes it, on average, more efficient than statute law after a surprisingly brief evolution."[152] For this reason, pure statutory law is never desirable.[153] Again, however, "in the face of social change stare decisis can be an intolerable burden on case law."[154]

In a system that is experiencing social change, the authors conclude that a mixed statutory/case law approach is preferable.[155] A mixed system becomes more desirable as the rate of social change increases.[156] This allows statutes to deal with changing underlying conditions and case law to interpret these statutes in accordance with precedent.[157] This system helps to address judicial bias[158] and frees law from the constraints of stare decisis in the face of changing circumstances.[159] It also depends upon an accountable legislature whose preferences are aligned with social welfare.[160] The cost associated with legislatures that aren't perfectly accountable or whose preferences aren't

---

[146] Thomas K. Richards, *The Internet and Decisional Institutions: The Structural Advantages of Online Common Law Regulation*, 10 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 731, 735-36 (2000) (stating that common law "presents a particular advantage [over legislation] when applied to the newest and most unregulated space of our time, the Internet," but also that common law can "increase the functionality of future legislation by slowly mapping out the legal terrain in this uncharted territory.").

[147] Ponzetto & Fernandez, *supra* note 125, at 381.

[148] *Id.* at 380.

[149] *Id.* at 404.

[150] *Id.* at 398.

[151] *Id.* at 382.

[152] *Id.* at 401.

[153] Ponzetto & Fernandez, *supra* note 125, at 405.

[154] *Id.*

[155] *Id.* at 406.

[156] *Id.* at 405.

[157] *Id.* at 382-83.

[158] *See id.* at 405.

[159] Ponzetto & Fernandez, *supra* note 125, at 405.

[160] *Id.*

perfectly in line with social welfare is acceptable when "social change is sufficiently intense."[161] A hybrid system, therefore, seems preferable, especially when dealing with new and changing technology such as online communication.

The question now becomes whether constitutional (Fourth Amendment) or subconstitutional (tort) judicial action is the preferable partner to statutory law. Adrian Vermeule provides some insight into this. He asserts, "arguments for the rationality or efficiency of [subconstitutional] common law . . . do not translate successfully into arguments for the comparative rationality or efficiency of the constitutional common law."[162] This is so because constitutional common law isn't "a repository of latent wisdom" upon which judges can build.[163] Constitutional common law is built upon both precedent *and* social traditions.[164] These social traditions can be perceived differently over time. In addition, constitutional common law applies "evolving standards of decency" and notions of what is "implicit in the concept of ordered liberty."[165] Only supporters of "the most stringently backward-looking forms of originalism" would presume that our notions of decency and liberty do not change over time, and most often radically.[166] Despite this fact, in many cases, "the principle target of common law constitutionalism is originalism,"[167] which retards the law's progress toward more efficient rules.

Furthermore, the very goal of efficiency is problematic when it comes to constitutional common law. Vermeule defines "efficiency" as "wealth maximization" and therefore asks whether constitutional law should even strive to be efficient.[168] The point of constitutional law is to achieve justice, not efficiency.[169] Even if we assume a broader definition of "efficiency" or apply some other framework such as Pareto efficiency or even a collective level of happiness (however determined), it's unclear that "justice" can be measured.[170] If it can't be measured, then we can't speak of constitutional law converging on a "better" legal system. Even if it could, Vermeule argues that constitutional law's binding nature would prevent it from evolving toward a better system, a problem that subconstitutional law doesn't have.[171]

If we can't speak of constitutional law converging on any better system, then the

---

[161] *Id.* at 406.
[162] Vermeule, *supra* note 126, at 1482.
[163] *Id.* at 1483.
[164] *Id.* at 1492.
[165] *Id.* at 1495.
[166] *Id.*
[167] *Id.* at 1502.
[168] Vermeule, *supra* note 126, at 1523.
[169] *Id.*
[170] When we speak of justice, we speak of values, not absolute truth. Vermeule argues that law can move toward a "right answer" only if (1) there is a factual component to a legal question; (2) there is a prescriptive or means-end judgment about which legal ruling will best conduce to achieving an agreed-upon goal; or (3) the legal question otherwise has a right answer somehow defined. *Id.* at 1491. In constitutional law, all of these criteria are often absent.
[171] Vermeule, *supra* note 126, at 1531-1532.

hybrid approach to lawmaking advanced by Ponzetto and Fernandez necessitates the use of subconstitutional common law. The ability to converge on a better system is what gives that half of Ponzetto and Fernandez' hybrid system its value.

Subconstitutional tort law may be better suited to partnering with statutory law to ensure people's privacy interests in ISP searches of their emails. Tort law ultimately deals with money settlements, which are amenable to being measured according to a traditional view of efficiency as wealth maximization. If ISPs conclude that searching users' email contents will harm their bottom line, ISPs will stop searching email contents. By establishing privacy tort law that is very supportive of email users, ISPs will tend not to search their email contents. The primary mechanism of enforcement will be financial, and the knock-on effect will be a certain amount of justice in the form of protecting users' privacy.

A hybrid approach to addressing changing social circumstances is ideal. In terms of pure effectiveness, statutory law should partner with subconstitutional tort law, and not constitutional Fourth Amendment law, to deal with the problem of ISP searches of users' email contents. This is so not only for the reasons stated in this section, but also because it would simply be easier to do so. ISPs are privately-owned entities, and given the Supreme Court's retreat from its liberal mid-twentieth century state action jurisprudence, it's unlikely that ISPs would be found to be state actors. The Fourth Amendment would therefore not limit them in their ability to search users' email contents.

I do, however, think the case is there to be made. The relationship between ISPs and the government suggests that ISPs could be considered state actors. I'm also not sure that users' interest in privacy should be assured only as a knock-on effect of a tort ruling that pushes toward economic efficiency. If that were the case, then our constitutional law landscape would look quite different and would likely ensure many fewer rights to vulnerable groups. Thus, let's take a look at how ISPs could be considered state actors.

V. HOW ISPS CAN BE CONSIDERED TO BE STATE ACTORS; AN EXPANDED THEORY OF THE FOURTH AMENDMENT; THE PUBLIC FUNCTION DOCTRINE; THE ENTWINEMENT DOCTRINE; ASSUMPTION OF RISK; ISPS' COUNTERVAILING INTERESTS; A MIDDLE GROUND

During the civil rights era of the twentieth century, the Supreme Court often addressed inequality by finding that private actors who discriminated based on race were state actors. Thus, the Constitution applied to their actions. Since the 1960s, the Court has been much more hesitant to make similar findings. Unlike limiting racial discrimination under the Commerce Clause or the Fourteenth Amendment, there has never been a substantial trend to saddle private actors with Fourth Amendment restrictions.

It may be time to explore the value and workability of such a trend. Our digital age has brought with it a new communications paradigm, and ISPs are working closely with the government, including law enforcement agencies, to police these new forms of communication. For a number of reasons, ISPs are performing a traditionally

governmental function and are entwined with the government such that they may be considered state actors for Fourth Amendment purposes.

In this section, I first describe an expanded theory of the Fourth Amendment that could apply in the digital age, at least as it pertains to ISPs' searches of email contents. I then discuss how the public function and entwinement doctrines could operate to make ISPs state actors. I then address the assumption of risk doctrine and other ISP-specific counterarguments to my thesis. Finally, I point us toward a middle ground that might satisfy individual privacy interests in a way that is palatable to ISPs.

A. An Expanded Theory of the Fourth Amendment

We don't necessarily need a *new* theory of the Fourth Amendment for the digital age. Rather, we need to expand current theory and rethink secondary constitutional doctrines from which the Court has generally retreated or which it has left undeveloped or inconsistent. This approach can be criticized as rejecting the notion that the Constitution has some recognized substantive content. The charge is, in other words, that my approach alters the law simply because the outcome would be better. I do not think this charge is justified. The approach I propose hews quite closely to traditional Fourth Amendment law. Where it departs from precedent, it doesn't alter the law, but expands upon it. This evolution in law is commonplace, and has resulted in Fourth Amendment decisions such as *Katz* and *Kyllo* that address new technologies. One might justifiably argue that I apply the public function doctrine too freely. That is certainly part and parcel to my approach of expanding the use of existing law; it is not, however, creating new law.

At its base, the Fourth Amendment restricts the right that government actors have to search or seize things in which people have a subjective and reasonable expectation of privacy.[172] Correspondence among citizens is at the heart of what the Court considers to be private and protected by the Fourth Amendment.[173] It is so protected not only in order to preserve the integrity and dignity of the individual, but also to enable ideas to circulate freely, which is thought to ensure a dynamic yet enduring democracy.[174] This is one reason that the Constitution established the U.S. Postal Service, and why the Postal Service cannot open our mail with impunity.[175]

---

[172] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J. concurring).

[173] Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 558-59 (2007).

[174] Sandra Braman, *Where Has Media Policy Gone? Defining the Field in the Twenty-First Century*, 9 COMM. L. & POL'Y 153, 182 n.4 (2004) ("the postal provision of the Constitution established a postal service in order to provide universal access to the kind of distributed communication system considered critically necessary for the functioning of a democracy."); Susan Landau, *National Security on the Line*, 4 J. TELECOMM. & HIGH TECH. L. 409, 445 (2006) ("the U.S. Post Office was seen as a facilitator of democracy and was one of the few strong federal institutions established in the nascent United States.").

[175] Landau, *supra* note 174, at 445.

As a governmental agency, the Fourth Amendment limits the Postal Service.[176] This means that individuals retain all of the Fourth Amendment rights to their letters in the post that they would have if those letters were in their home.[177] "No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail."[178] There are, of course, some exceptions to this privacy right that apply broadly in Fourth Amendment jurisprudence. For example, a suspicious package or letter may be held for a reasonable time[179] and the use of narcotics dogs at postal facilities isn't considered a Fourth Amendment search.[180]

The purpose of providing such robust privacy rights in our mailed correspondence is to ensure free speech and all of the benefits to democracy that that right enables. "[T]he use of the mails is almost as much a part of free speech as the right to use our tongues."[181] In the post office, therefore, we see one of the best examples of how and why the Fourth Amendment protects First Amendment interests.[182] Anuj C. Desai has discussed the relationship between communications freedom and the Fourth Amendment[183] and the Fourth Amendment's more straightforward application to the post office.[184] Despite the obvious implications of the First Amendment in the post office context, this article focuses on the Fourth Amendment in that context and the comparison between letters sent through the post and email sent over ISPs' networks.

The dilemma we face today is that as our communication goes online, we are sending fewer and fewer letters in favor of more and more emails, chats, instant messages, and so forth. The content of physical letters and emails is often the same, but the privacy protections are quite different. No longer does a government agency handle the bulk of our private correspondence; private actors—ISPs—now perform this function. Just as it allows prisons to be run and toll roads maintained by private companies, the government may feel that this new arrangement is to its benefit. If "[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be,"[185] then our electronic correspondence ought to be protected. If ISPs have taken over the role of the Postal Service, they should be limited by the same constitutional rules that limit the Postal Service, which include the Fourth Amendment.

---

[176] Ex Parte Jackson, 96 U.S. 727, 732-33 (1877).

[177] United States v. Van Leeuwen, 397 U.S. 249, 251 (1970).

[178] *Ex Parte Jackson*, 96 U.S. at 733.

[179] *Van Leeuwen*, 397 U.S. at 252.

[180] United States v. Place, 462 U.S. 696, 709 (1983); United States v. Dennis, 115 F.3d 524, 532 n.3 (7th Cir. 1997).

[181] *Van Leeuwen*, 397 U.S. at 251 (quoting U.S. ex rel. Milwaukee Social Democratic Pub. Co. v. Burleson, 255 U.S. 407, 437 (1921) (Holmes, J., dissenting)).

[182] See Blitz, *supra* note 4.

[183] Desai, *supra* note 173.

[184] Anuj C. Desai, *Can The President Read Your Mail? A Legal Analysis*, 59 CATH. U. L. REV. 315 (2010).

[185] *Ex Parte Jackson*, 96 U.S. at 733.

In going online to write our letters, we have left behind the privacy protections associated with the post office and protected by law. We have entered a field in which our privacy is protected by large corporations and smaller ISPs and only at their whim. They are interested in earning a profit and protecting their names, not in protecting their users' privacy. If the postal service and the privacy protections inherent in mailings through it are meant to ensure free speech and the progress of our democracy, then this new digital arrangement threatens these very values. Whatever benefits may accrue, the costs of going online without privacy may be too much to bear.

In this new era of communication, we need to reconsider the extent to which the Constitution can and should apply to private actors. We need to invoke extant constitutional doctrine to guide us to the appropriate boundaries, and we also need to use this doctrine to get us there. Just as the 1940s, 50s, and 60s saw the expanded use of the Commerce Clause and Fourteenth Amendment to reach private action, the extension of the Fourth Amendment to ISPs must now be explored.

The theory of the Fourth Amendment that I propose here is not new, but is rather reconsidered, and pushes toward the expanded use of the Fourth Amendment to reach private actors. It should reach private actors where these actors are engaged in a traditionally public function or where they are entwined with the government. Using these doctrines provides us with opportunities to ensure individuals' privacy, define the scope of Internet users' rights, and develop what the public function and entwinement doctrines actually mean.

B. Public Function Doctrine

Along with other exceptions to the state action doctrine, the Supreme Court has admitted that the "cases deciding when private action might be deemed that of the state have not been a model of consistency."[186] Others have called this area of law a "conceptual disaster area."[187] What results, therefore, is that facts are more likely to drive the legal analysis. The approach used might be a balancing test that tries to favor the party with more fundamental interests,[188] an inquiry into whether the activity in question has traditionally and exclusively been performed by the government,[189] or whether there is "a sufficiently close nexus between the State and the challenged action of the regulated entity."[190] At best, the Court will do what it thinks is in the country's best interests; at worst, base political orientation will drive judicial rulemaking.

When it comes to ISP searches of users' email contents, there are obvious

[186] Edmonson v. Leesville Concrete Co., 500 U.S. 614, 632 (1991).

[187] Black, *supra* note 9, at 95.

[188] Marsh v. Alabama, 326 U.S. 501, 509 (1946) ("When we balance the Constitutional rights of owners of property against those of the people to enjoy freedom of press and religion, as we must here, we remain mindful of the fact that the latter occupy a preferred position.").

[189] Lugar v. Edmondson Oil Co., Inc., 457 U.S. 922, 937 (1982).

[190] Jackson v. Metro. Edison Co., 419 U.S. 345, 351 (1974) (citing Moose Lodge No. 7 v. Irvis, 407 U.S. 163, 176 (1965)).

competing interests that implicate issues of politics and democracy. For those who favor rules that allow ISPs to control their networks as they see fit, principles of limited government, judicial conservatism, private property, and freedom of contract will be compelling factors. For those who want to promote individuals' rights to keep their emails private, principles of individual sovereignty, integrity, and privacy as fundamental interests will drive decision-making.

This article promotes the individual privacy orientation, but also recognizes the legitimacy of the opposite viewpoint. The question I want to approach here is whether the public function doctrine can be used to conclude that ISPs are state actors. They may be considered state actors because they are acting as a postal service, and have in fact largely usurped the role of the U.S. Postal Service. They may, therefore, be performing a task that is traditionally the exclusive prerogative of the government.[191]

Under one interpretation of the public function test, a private actor will be deemed to be a state actor if the function performed is traditionally the exclusive prerogative of the state.[192] The public function must be "traditionally exclusively reserved to the State."[193] There may be no function more traditionally exclusively reserved to the government than that of running a postal service. The Constitution provides Congress with the power to "establish post offices and post roads,"[194] from which it has been inferred that Congress also has the power to carry mail along the post road.[195] It has been recognized that Congress' power in this regard is exclusive—it has, in other words, a monopoly on carrying letters.[196]

This monopoly has been supported by the Private Express Statutes (PES),[197] which were passed as a broad revenue protection measure for the Postal Service vis-à-vis private competitors.[198] Section 1694 of the PES states, for example,

---

[191] A balancing of interests could conceivably favor individual privacy interests over ISP interests, and therefore determine that ISPs are state actors. This balancing test, however, relies on political and factual inquiries. Because I take an opinionated stance in this article based on these inquiries (individual right to privacy should prevail when it comes to ISP searches of users' emails), I will not try to analyze the application of the balancing test as a legal principle.

[192] *Lugar*, 457 U.S. at 937.

[193] *Jackson*, 419 U.S. at 352.

[194] U.S. CONST. ART. 1, § 8, CL. 7.

[195] United States v. Comstock, 130 S. Ct. 1949, 1963 (2010) (citing McCulloch v. Maryland, 17 U.S. 316, 385 (1819)).

[196] Regents of Univ. of Cal. v. Pub. Emp't Relations Bd., 485 U.S. 589, 593-94 (1988). As mentioned above, UPS and Fed Ex are not considered to be engaging in a public function, perhaps because their service is an "add-on" or extra that complements, but doesn't replace, the Postal Service. Email, however, has taken a large bite out of the Postal Service's market share, replacing it to a great extent.

[197] 18 U.S.C. §§ 1693-1699 (2010); 39 U.S.C. §§ 601-606 (2010).

[198] Air Courier Conference of Am. v. Am. Postal Workers Union AFL-CIO, 498 U.S. 517, 519 (1991).

> Whoever, having charge or control of any conveyance operating by land, air, or water, which regularly performs trips at stated periods on any post route, or from one place to another between which the mail is regularly carried, carries, otherwise than in the mail, any letters or packets, except such as relate to some part of the cargo of such conveyance, or to the current business of the carrier, or to some article carried at the same time by the same conveyance, shall, except as otherwise provided by law, be fined under this title.[199]

By providing email accounts and facilitating their transmission, ISPs are engaging in activity that has historically been done by a government monopoly. As a result of this shift from letters to email, the U.S. Postal Service has gone from being profitable in the 1990s[200] to being reliant on handouts from the U.S. Treasury.[201] Not only are ISPs engaging in a traditionally exclusive governmental function, but they are also undermining the very purpose of the monopoly: to protect revenue streams against private competitors. This arrangement means that under the public function doctrine, ISPs can be considered to be state actors.

ISPs ought not to be analogized to companies like Fed Ex and UPS, which are *not* government actors and are *not* limited by the Fourth Amendment.[202] These private courier companies do not serve the same purposes as the U.S. Postal Service. The USPS' goal is to ensure the free flow of ideas in accord with democratic ideals of free speech, privacy, and social progress. Private courier companies serve a much narrower band of society, and are explicitly business-oriented.

Fed Ex, for example, prides itself on its innovation and specialized services to help build businesses around the world.[203] It targets various "market segment[s]" to provide the best service possible.[204] It does this in order to keep itself "in front of the marketplace."[205] One of its long-range goals is to increase revenue. UPS is similarly

---

[199] 18 U.S.C. § 1694 (2010).

[200] Robert A. F. Reisner, *When a Turnaround Stalls*, HARV. BUS. REV., Feb. 2002, at 45-52 http://hbr.org/2002/02/when-a-turnaround-stalls/ar/1.

[201] Angela Greiling Keane, *A Bailout for the U.S. Postal Service?*, BLOOMBERG BUSINESSWEEK, Dec. 9, 2010, http://www.businessweek.com/magazine/content/10_51/b4208033645172.htm?campaign_id=rss_topStories (last visited Dec. 19, 2010).

[202] Shortz v. United Parcel Service, 179 F.App'x 644, 645 (11th Cir. 2006); United States v. Souza, 223 F.3d 1197, 1200 (10th Cir. 2000).

[203] *Our Company*, FED EX, http://about.fedex.designcdt.com/our_company (last visited Feb. 2, 2011).

[204] *Company Information*, FED EX, http://about.fedex.designcdt.com/our_company/company_information/mission_statement (last visited Feb. 2, 2011).

[205] *Fed Ex Innovation*, FED EX, http://about.fedex.designcdt.com/our_company/fedex_innovation (last visited Feb. 2, 2011).

focused on efficiency, price competitiveness, and customer service.[206] It has gone beyond simply transporting packages; it now manages a "streamlined organization that provides logistics, global freight, financial, and mail services to enhance customers' business performance and improve their global supply chains."[207] It claims that "[o]ver the past 100 years, UPS has become an expert in transformation, growing from a small messenger company to a leading provider of air, ocean, ground, and electronic services."[208]

ISPs, as providers or couriers of email, do not currently discriminate based on whether an email is personal or business-related. Like letters through the post, one email looks like any other to an ISP. The purpose of emails is similarly to convey all sorts of information, about individuals' personal and professional lives, medical and legal issues, the arts, and so forth. Discussion of all of these topics amounts to speech that ought to be protected in order to ensure the progress of democracy.[209] This is what the postal service has historically protected, and this is the type of information currently traded via email.

Fed Ex and UPS do not serve this lofty purpose. Their organizations pursue innovation that serves businesses around the world, and therefore increases their own profit margin. There is a much lower expectation of privacy in letters sent via Fed Ex and UPS than via the postal service. Justice Holmes said, "the use of the mails is almost as much a part of free speech as the right to use our tongues."[210] The use of Fed Ex and UPS could be said to be almost as much a part of doing business as opening a brick-and-mortar store.

These differing interests mean that individuals using each service enjoy relatively greater or lesser privacy rights. Because ISPs have largely replaced letters sent through USPS, because ISPs carry all emails equally, and because people use emails for all of the purposes for which they traditionally used the USPS, ISPs should be limited in their right to search emails much as the USPS is limited in its right to search letters and packages that it carries.

Another interpretation of the public function doctrine is the proposition that "[t]he more an owner, for his advantage, opens up his property for use by the public in general, the more do his rights become circumscribed by the statutory and constitutional rights of those who use it."[211] When facilities "are built and operated primarily to benefit the public and since their operation is essentially a public function, [they are] subject to state

---

[206] *1991-1999*, UPS, http://www.ups.com/content/us/en/about/history/1999.html (last visited Feb. 2, 2011).

[207] *2000-2007*, UPS, http://www.ups.com/content/us/en/about/history/2007.html (last visited Feb. 2, 2011).

[208] *Id.*

[209] *See* Alexander Meiklejohn, *The First Amendment is an Absolute*, 1961 SUP. CT. REV. 245, 255-57 (1961).

[210] *Van Leeuwen*, 397 U.S. at 251 (quoting U.S. *ex rel.* Milwaukee Social Democratic Pub. Co. v. Burleson, 255 U.S. 407, 437 (1921) (Holmes, J., dissenting)).

[211] *Marsh*, 326 U.S. at 506.

regulation."[212] Although ISPs are clearly in the business to earn money, and not to provide for the public good, that argument misses the point. All private actors seek first to earn a profit,[213] and only then, and then incidentally, to serve the public good. Where their actions, done for whatever purpose, entail a public function, the public function doctrine may apply. A shopping mall owner, for example, doesn't run a mall in order to provide a forum for speech. Nonetheless, because the shopping mall is the place where people congregate, an expansive view of the public function doctrine would result in the First Amendment limiting shopping mall owners in some ways.[214] Just as shopping malls have replaced public sidewalks and squares, ISPs have replaced the U.S. Postal Service. Just as the public function doctrine might limit shopping mall owners, so should it operate to place Fourth Amendment restrictions on ISPs' ability to search the contents of email existing on their networks.

There may also be developing a nexus between the state and ISPs that would conclude with ISPs being considered state actors. Whether such a nexus exists depends, in part, on whether the State "has exercised coercive power or has provided such significant encouragement, either overt or covert, that the choice must in law be deemed to be that of the State."[215] Given the Court's refusal in *Jackson v. Metropolitan Edison Co.* to find state action under the nexus doctrine,[216] it's difficult to see how ISPs could be treated as state actors under it.

Nevertheless, courts willing to expand the public function doctrine may rest on the fact that ISPs and law enforcement often work together, the government is actively encouraging ISPs to take steps to facilitate law enforcement investigations in cyberspace, and ISPs have taken steps specifically in response to statutory law. Although the government isn't compelling ISPs to do any of these things, such compulsion isn't a necessary condition. Public function opinions, rather, leave a large area open for ad hoc, totality-of-the-circumstances analyses that look more to perceived equities than strict legal rules.

C. Entwinement Doctrine

The Supreme Court introduced the entwinement doctrine in 2001 in *Brentwood Academy v. Tennessee Secondary School Athletic Ass'n.*[217] The Court held

---

[212] *Id.*

[213] Indeed, "increasing [ISPs'] ability to monitor and control applications and content on their networks increases their profits. . . . [ISPs] increasingly deploy devices for deep packet inspection in their networks that let them monitor and control the applications on their network. These devices can be used to slow down or exclude specific applications and content. . . ." VAN SCHEWICK, *supra* note 17, at 371.

[214] *See* PruneYard Shopping Ctr. v. Robins, 447 U.S. 74 (1980); *but see* Hudgens v. Nat'l Labor Relations Bd., 424 U.S. 507 (1976); Lloyd Corp. v. Tanner, 407 U.S. 551 (1972); Amalgamated Food Emps, Union Local 590 v. Logan Valley Plaza, Inc., 391 U.S. 308 (1968).

[215] American Mfrs. Mut. Ins. Co. v. Sullivan, 526 U.S. 40, 52 (1999).

[216] Jackson v. Metro. Edison Co., 419 U.S. 345, 358 (1974) (no nexus exists where the private actor was heavily regulated, privately owned, had a partial monopoly, and relied on state law).

[217] Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288 (2001).

that "[w]hen . . . the relevant facts show pervasive entwinement to the point of largely overlapping identity" between a state and a private actor, then the private actor is said to be engaged in state action.[218] The Court seemed to apply the nexus test,[219] and further acknowledged that the analysis "is a matter of normative judgment, and the criteria lack rigid simplicity."[220] Therefore, "no one fact can function as a necessary condition across the board for finding state action; nor is any set of circumstances absolutely sufficient, for there may be some countervailing reason against attributing activity to the government."[221]

Brentwood presents a number of inconsistencies and vagaries. Is entwinement like the entanglement doctrine, which is another exception to the state action doctrine?[222] Based on its reference to the nexus doctrine, is it like the public functions doctrine? If it is like either of these, does it differ in enough ways to be its own doctrine? If not, then are these three exceptions to the state action doctrine simply legal fictions, and does the Court make its decisions based on other factors? The *Brentwood* Court acknowledged that its analysis was a "matter of normative judgment." Does this mean that its decisions are merely political or based on subjective values about which rights should prevail in a conflict? Finally, even if the legal analysis (whatever that may be) is performed, can "some countervailing reason" change the outcome? Is this countervailing reason the implication of some fundamental right? Does that mean that due process is implicated?

Despite the vagaries, let's take a look at how the entwinement doctrine as we understand it might apply to ISP searches of email contents. According to the entwinement doctrine, a private actor may be treated as a state actor "when it is 'entwined with governmental policies' or when government is 'entwined in [its] management or control.'"[223] Entwinement may exist when neither the government nor the private entity controls a given sphere of activity, but both are so intimately involved in that activity that the actions of the private actor in that sphere are "fairly attributable" to the state.[224]

United States v. Richardson, discussed above, is a pretty good example of ISP/government entwinement (even though it is doubtful that a court would think so). Although AOL was not *required* to search for images of child pornography, it is clear that it was responding to a statutory mandate to report such images if and when they were discovered. In order to protect itself from liability, AOL may have decided simply to actively search for child pornography, rather than defend itself against claims of negligence.

In order to root out child pornography, the government needs to be entwined with

---

[218] *Id.* at 303.
[219] *Id.* at 295.
[220] *Id.*
[221] *Id.* at 295-96.
[222] *See* Edmonson v. Leesville Concrete Co., 500 U.S. 614 (1991); Lugar v. Edmondson Oil Co., 457 U.S. 922 (1982); Shelley v. Kraemer, 334 U.S. 1 (1948).
[223] *Brentwood Acad.*, 531 U.S. at 296.
[224] Evans v. Newton, 382 U.S. 296, 298 (1966).

ISPs.[225] ISPs own the software and hardware network over which legal and illegal data alike travel. Law enforcement agents cannot simply tap into ISPs' private networks. If they cannot tap into the network, they often cannot discover illegal conduct occurring on the network, which could provide the basis for a warrant to search the network. Since child pornography is all but impossible to obtain through non-electronic means,[226] law enforcement usually cannot obtain evidence from a source external to the Internet to obtain probable cause to search a network.[227] Despite claims that there is no privacy in the digital era, in the case of child pornography, the Internet provides decent insulation for traders of images.[228] To address this trade, law enforcement needs, and receives, the help of ISPs like AOL. Statutes support and encourage this assistance. Because ISPs and state actors are entwined—and may become increasingly entwined in the near future[229]—ISPs should be considered state actors and thus limited by the Fourth Amendment.[230]

This isn't to say that the Court *will* find that ISPs and the government are entwined. Given the current makeup of the Supreme Court, the state action doctrine will probably be applied rather traditionally, and its exceptions not given much effect. What will be needed to invoke the exceptions is recognition that we are in a paradigm shift when it comes to communication and that our online communication needs to be protected. A set of factual events (such as a string of revelations of disturbing ISP searches of email content) that vividly highlights this article's concern may also be needed to spur the Court to acknowledge the paradigm shift. Although this hasn't yet taken place, the state action doctrine and its exceptions do provide a way for the Court to provide email users with constitutional protections. What are the counterarguments to this?

---

[225] Under the Commerce Clause, the government could require ISPs to install programs such as IDFP. This would, of course, not address email users' interest in privacy. Rather, it would further the argument that ISPs are state actors, and are thus limited by the Fourth Amendment.

[226] PHILIP JENKINS, BEYOND TOLERANCE: CHILD PORNOGRAPHY ON THE INTERNET 3, 9 (2001).

[227] Law enforcement can, however, troll chat rooms and forums to look for illegal behavior. Based on that, they can obtain warrants. The Stored Communications Act and Wiretap Act also provide law enforcement with some entrée into networks. The laws' provisions, however, as mentioned above, are inconsistent and anachronistic.

[228] MAX TAYLOR & ETHEL QUAYLE, CHILD PORNOGRAPHY: AN INTERNET CRIME 159-63 (2003) (noting the relative ease and anonymity of assembling large collections of child pornography over the Internet as compared to pre-Internet distribution channels).

[229] *See Feds Seek Broader Internet Eavesdropping Rights*, CBSNEWS.COM, Sept. 27, 2010, http://www.cbsnews.com/stories/2010/09/27/tech/main6903887.shtml (last visited Dec. 12, 2010).

[230] This does not necessarily mean that programs such as AOL's IDFP will be unconstitutional. A program designed to detect known images of child pornography may not constitute a search, or may constitute a reasonable search that satisfies the Fourth Amendment. Although I am in favor of saddling ISPs with legal limitations, constitutional or otherwise, I am also in favor of providing ISPs and state actors with the ability to detect the trade in child pornography. We should be confident that a regime that does both is eminently possible.

D. Assumption of Risk

Courts have suggested that if people have a reasonable expectation of privacy in the contents of their emails (as against searches by government agencies or ISPs), they do not lose their Fourth Amendment protection because they assume the risk that the ISP will disclose the emails.[231] A New York District Court wrote:

> It is true . . . that by sharing communications with someone else, the speaker or writer assumes the risk that it could be revealed to the government by that person, or obtained through a subpoena directed to that person . . . . However, "[t]he same does not necessarily apply ... to an intermediary that merely has the ability to access the information sought by the government." . . . Indeed, the "assumption of risk" so trumpeted by the Government, is far from absolute. "Otherwise phone conversations would never be protected, merely because the telephone company can access them; letters would never be protected, by virtue of the Postal Service's ability to access them; the contents of shared safe deposit boxes or storage lockers would never be protected, by virtue of the bank or storage company's ability to access them." . . . These consequences of an extension of the assumption of risk doctrine are not acceptable under the Fourth Amendment. A caller "'is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,' and therefore cannot be said to have forfeited his privacy right in the conversation."[232]

Assumption of risk is a good doctrine in contexts that allow someone a choice to engage a particular risk or to avoid it. In general, when someone conveys information to a third party (as when an email sender sends the email to an ISP for forwarding onto the ultimate recipient), she has assumed the risk that the third party will disclose the information to the government.[233] The Supreme Court, however, qualified the doctrine's applicability, writing that

> [I]mplicit in the concept of assumption of risk is some notion of choice. At least in the third-party consensual surveillance cases, which first incorporated risk analysis into Fourth Amendment doctrine, the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications . . . unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance . . . It is idle to speak of

[231] Warshak v. United States, 490 F.3d 455, 469 (6th Cir. 2007).

[232] *In re U.S. for Orders*, 515 F. Supp. 2d at 337-38 (citing Warshak v. United States, 490 F.3d 455, 470 (6th Cir. 2007)).

[233] Smith v. Maryland, 442 U.S. 735, 749 (1979).

> "assuming" risks in contexts where, as a practical matter, individuals have no realistic alternative.[234]

Email today is a professional, if not a personal, necessity. Imagine your boss's reaction when, in response to her request to email her a document, you proclaim, "sorry, I don't use email."

We virtually cannot avoid using email. When we do, we can only hope to be able to choose the initial ISP who will provide us with Internet access. We can "choose," then, to send our emails to that ISP. Beyond that, however, we have no choice or even knowledge of which ISPs handle our email as it winds its way to the ultimate recipient.

It might be argued that we assume the risk of search as to the ISP with whom we contract for Internet access, but we do not assume the risk as to other ISPs who handle our email. Based on the Court's requirement of choice to trigger the assumption of risk doctrine, this argument fails. In 2010, 78% of Americans could choose between only one of two local ISPs, and 13% had only one option.[235] Even if someone has two (or more) options when it comes to ISPs, it is highly likely that both (or all) of these ISPs will have the same privacy policy that enables them to search email contents. There is no choice, and so no assumption of risk.

E. ISPs' Countervailing Interests

ISPs would likely not want to be limited in their actions by the Fourth Amendment or any other type of law. They would likely have at least four arguments against this. First, they consider themselves to be private actors, and so not subject to the Fourth Amendment. Second, they want and need to be free to manage their networks. Third, they provide Terms of Service agreements listing their privacy policies that potential customers can accept or reject. Finally, ISPs may claim that their interest in searching email contents is limited to uncovering criminal activity.

ISPs certainly can make a strong, almost dispositive, claim that they are private actors and so shouldn't be limited by the Fourth Amendment. This article suggests a way that they may be so limited and argues that resort to constitutional law isn't necessary, and may not be desirable. ISPs may be limited in their right to search users' email contents through statutory, constitutional, or subconstitutional law. Whichever mechanism is used, ISPs should be limited. ISPs provide to users the modern equivalent of the Postal Service, town square, marketplace of ideas, and shopping mall all rolled into one. If an individual's constitutional rights increase as a private space is increasingly used for public purposes,[236] then we ought at least to ask how and to what extent individuals' Fourth Amendment rights apply to online communication. A necessary aspect of this inquiry is how and to what extent ISPs might be limited in their ability to

---

[234] *Id.*
[235] Pegoraro, *supra* note 49.
[236] *Marsh*, 326 U.S. at 506.

perform certain searches and seizures.

ISPs would respond, of course, that they need to be free to manage their networks. The law has never been blind to the needs of parties whose actions are limited by the establishment of others' rights. The law's history is largely one of balancing interests and making rulings that respond to the legitimate interests of all. There is no reason to think that ISPs would be hindered in their ability to manage their networks if they are unable to search users' email contents.

Email contents are relatively small bodies of data, and to the Internet, they are indistinguishable from other data such as music files, movies, money transfers, and so forth. In order to manage their networks, ISPs need to know only how much data there is to be transferred, where it's coming from, where it's going, and whether any viruses, worms, bots, or other malware are contained in the data. Under my proposal, it would be entirely reasonable for ISPs to perform the necessary searches to find malware and to facilitate the transfer of data from one computer to another. If ISPs were to present evidence that they had to perform additional searches in order to secure their networks, the law could make space for these searches.

A more difficult issue is the ISPs' searches of email contents in order to inhibit spam or divert it to users' spam inboxes. This is a valuable service that ISPs perform and one that consumers welcome. Regulations designed to ensure users' privacy while continuing to address the problem of spam may be tricky, but are certainly possible. As Lawrence Lessig writes, "code is law,"[237] which means that we can structure the Internet largely how we want to achieve the ends we want.

There may be some undesirable knock-on effects of such regulation. One effect might be that we have to purchase virtual stamps for our emails. A cost of half a cent per email, for example, may not be so prohibitive to someone who sends ten or twenty emails per day. The same cost might be prohibitive to spammers, who send millions, if not billions of emails each day. One can imagine other forms of regulation. For example, the government might require all email-based solicitors to use emails ending in "@spam.net." ISPs would easily be able to filter out those emails and allow non-spam emails to be transmitted without having to search their contents. In the first example, the cost is directly borne by email senders; in the latter, it is borne indirectly by taxpayers, and results in cost spreading.

ISPs might argue that their Terms of Service are available to potential customers and include privacy policies. If someone does not want to subject herself to such policies, she can sign up with another ISP. There are a few problems with this approach. Most people only have one or two ISPs from which to choose.[238] Most ISPs have relatively similar privacy policies. Finally, these policies are typically unclear as to the extent to which ISPs may perform searches of user communications. And so like the

[237] LAWRENCE LESSIG, CODE: VERSION 2.0 5-6 (20).
[238] Pegoraro, *supra* note 49.

Lochnerian baker,[239] potential ISP customers can choose among at most a handful of ISPs, probably all of whom have the same unclear but intrusive privacy policies. Some sort of protection for users' privacy is necessary.

Finally, and perhaps most compellingly, ISPs might argue that when they do perform searches of users' email contents, they do so only to detect illegal conduct, such as the possession and trade of child pornography. While this is a good goal, it misses the point of users' privacy interests. The Fourth Amendment and the law in general are not intended to protect criminals' privacy; they are intended to protect everyone's privacy. The fact that criminals sometimes get away with their crimes because of privacy laws is an unfortunate but necessary side effect of ensuring everyone's privacy.

ISPs do have the ability to detect the transmission over the Internet of images that are known to be child pornography. This detection would peer into the contents of an email and any attachment and see only the illegal image. For that reason this type of search would probably be considered either not a search for Fourth Amendment purposes, or a reasonable search. Either way, ISP searches specifically for child pornography would probably be approved of, even if ISPs are considered state actors.

The difficulty may come if and when ISPs begin to search email contents for evidence of other criminal conduct. They could, for example, perform searches for the term "violent jihad," "money laundering," or "put $500 on the Vikings to win." Searches for these terms are as likely to uncover innocent communications as they are to uncover illegal communications.

Although there's no evidence that ISPs are performing such searches, there is evidence that they're performing searches for marketing and customer service purposes. Users have an interest in ISPs not seeing their buying patterns, topics of conversation, and political opinions, no matter how innocent. Users also have an interest in ISPs not seeing their medical information, learning about their love life, and so forth. Finally, if ISPs uncover questionable terms like "violent jihad," email users who use this term innocently have an interest in not being investigated and wrongfully accused of a crime. The law should protect these interests.

F. A Middle Ground

Users and ISPs both have legitimate interests at stake. Plotting a middle ground that protects both is imminently possible. Even if ISPs are declared to be state actors for the purposes of searching users' email contents, ISPs could remain free to perform such searches in order to root out viruses, worms, bots, and so forth. Additionally, ISPs could apply packet sniffers to uncover known images of child pornography. As technology develops, ISPs' ability to perform surgical searches for malware and clearly illegal content is likely to increase. Any law that limits ISPs' right to search email contents need not limit ISPs' right to use such technology.

[239] Lochner v. New York, 198 U.S. 45 (1905).

This proposal also says nothing about any other type of search an ISP might perform. Chat rooms, instant messages, Facebook postings, and all other forms of online communication would be considered on their own ground. Although my proposal would guide these considerations, the middle ground principles and a totality of the circumstances approach would ensure that ISPs maintain their interests while users' privacy is also secured.

How might a court or legislature enact this middle ground into law?

VI. A MODEL APPROACH

If courts or legislatures are to find that ISPs are limited in their right to search email contents existing on their networks, the law will have to be carefully drafted. We don't want to saddle ISPs with too many restrictions; they, too, have liberty interests, and they deserve to run their networks as they see fit. However, we also want to make sure that the law is applied so as to protect individuals' reasonable expectations of privacy. Where ISPs engage in a public function and are entwined with state actors, they should be limited under the Fourth Amendment so that individual rights are protected. The following four-part model approach supports individual rights while maximizing ISPs' ability to control their networks.

A. Part One

> *Senders of email retain the privacy protections in email contents that are associated with Fourth Amendment protections of letters sent through the post. This means that senders lose their privacy expectations in the emails once the emails reach the recipients. In other words, the recipients may disclose the email contents to whomever they choose. Senders do, however, retain their privacy expectation in those emails that exist on an ISP's network, as against searches by ISPs. They retain these privacy expectations when the email is travelling on an ISP's network from the sender's computer to the recipient's computer. They also retain these privacy expectations in emails that remain on the ISP's network after the email has arrived at the recipient's computer. In the latter case, recipients may access and disclose the email contents, but ISPs may not do either. This expectation of privacy exists throughout time. Part One of this holding is subject to the qualification in Part Two.*

This proposed rule first equates emails with letters sent through the post. That means that email contents "are as fully guarded from examination and inspection, except as to their outward form . . . as if they were retained by the parties forwarding them in their own domiciles."[240] Just as emails are treated as letters, ISPs are treated as the Postal Service; ISPs are responsible for upholding the same privacy protections of their

[240] *Ex parte Jackson*, 96 U.S. at 733; United States v. Barry, 853 F.2d 1479, 1486 (8th Cir. 1988).

customers that the Post Office upholds under the Fourth Amendment of people who send letters through its service. This protection does not, of course, extend to "searches" or disclosures by the intended recipient of the email (or letter).[241]

Just as letter senders retain an expectation of privacy as the letters they send are being managed by the Postal Service, email senders retain an identical expectation as their emails are being routed from their computer to the recipient's computer. Unlike letters, however, emails can remain on ISPs networks long after a recipient has received the email. Web based and IMAP email programs entail this; governmental requests to disclose[242] or preserve data[243] might result in this; and data may simply persist on servers around the world for a period of time after the transmission is complete.[244] For this reason, when it comes to possible searches of email content by ISPs, an email sender's expectation of privacy doesn't dissipate throughout time.

Part One of this holding is qualified by the limitation in Part Two.

B. Part Two

> *ISPs* may *conduct limited searches of the contents of emails that exist on their networks in order to ensure the functioning of their network and in the normal course of business. The traditional rules that regulate and limit administrative searches apply to such limited searches performed by ISPs.*

ISPs such as AOL in *United States v. Richardson* have an interest in making sure their networks function well. They should be able to do everything they can to ensure this. They should, for example, be able to perform in-depth searches of data in order to find viruses, worms, bots,[245] and other programs that could harm the network or their customers' computers.

To satisfy the law, these searches must satisfy the constitutional rulings regarding administrative searches. This means that ISPs may perform searches for such threats based upon "a general administrative plan . . . derived from neutral sources."[246] ISPs

---

[241] *Barry*, 853 F.2d at 1486.

[242] *Transparency Report: Governmental Requests*, GOOGLE.COM, http://www.google.com/transparencyreport/governmentrequests/ (last visited Dec. 12, 2010).

[243] *Gonzales wants Internet companies to preserve data*, BUCKS COUNTY COURIER TIMES, Sept. 19, 2006, at A3, at 2006 WLNR 16394508; *DoJ Asks Internet Providers to Save User Data*, WASHINGTON INTERNET DAILY, June 2, 2006, at 2006 WLNR 10299708.

[244] CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 21:2, WIRETAP § 21:2 (2010) ("Even when delivery [of an email] is immediate, intermediate computers often retain backup copies, which they delete later.").

[245] Brief for the United States at 8, United States v. Richardson, No. 09-4072 (4th Cir. Oct. 15, 2009).

[246] Marshall v. Barlow's, Inc., 436 U.S. 307, 321 (1978).

"may not use an administrative inspection scheme to search for criminal violations."[247]

An ISP may perform searches designed and able to detect *only* clearly illegal data that is exceptionally harmful on its network. Usually, this will mean searches performed by programs like IDFP that detect only known images of child pornography. ISPs have an interest in expelling such images and their trade on ISPs' networks. Given ISPs' interest in doing so, society's interest in eliminating this trade, and the absence of any legitimate countervailing interests, such searches would likely satisfy the Fourth Amendment and could easily be approved of in any legislation or development of tort law.

C. Part Three

> *If, during the course of these limited searches, ISPs incidentally find evidence of criminality, they are not required to ignore it, and may disclose it to law enforcement authorities. It will be the burden of the prosecuting governmental agency to prove by a preponderance of the evidence that the ISP's search was performed in accord with the traditional rules of administrative searches, noted above. If the government cannot prove this, evidence derived from the ISP's search and any resulting searches are subject to the exclusionary rule.*

As with administrative searches performed by actual governmental agencies, any contraband that ISPs happen to find during a validly conducted administrative search may be disclosed to law enforcement and is not subject to the exclusionary rule.[248] This offshoot of the plain view doctrine furthers the truth-finding function of criminal procedure, and, because there would be no misconduct by ISPs or law enforcement, does not have any deterrence value. This means that the disclosure law at issue in *U.S. v. Richardson* would remain legal.

When misconduct is alleged and exclusion is the issue, courts have generally required that the prosecution carry the burden of proving by a preponderance of the evidence that exclusion is *not* warranted.[249] This makes sense: if the prosecution wants to introduce evidence, it should bear the burden of justifying its admission. It should not, however, have to satisfy the stringent beyond a reasonable doubt standard reserved for elements of a crime. Neither should it succeed in admitting the evidence based on an

[247] New York v. Burger, 482 U.S. 691, 724 (1987).

[248] Illinois v. Krull, 480 U.S. 340 (1987).

[249] Colorado v. Connelly, 479 U.S. 157, 168 (1986) (regarding the suppression of a statement made allegedly in violation of Miranda); Nix v. Williams, 467 U.S. 431, 438 (1984) ("After the defendant has shown unlawful conduct on the part of the police, the State has the burden to show by a preponderance of the evidence that (1) the police did not act in bad faith for the purpose of hastening discovery of the evidence in question, and (2) that the evidence in question would have been discovered by lawful means."); Lego v. Twomey, 404 U.S. 477, 486-87 (1972) (regarding the admissibility of a confession).

unconvincing, less-than-preponderance showing. Apart from such a showing, the preponderance standard is the most prosecution- and ISP-friendly standard there is. If there is no evidence that administrative search regimes result in governmental abuses, as the Supreme Court has stated,[250] ISPs would be especially unlikely to misuse such regimes. Because the likelihood of abuse of administrative searches is low, and the sanction of the exclusionary rule is extreme,[251] the burden to admit the evidence in question should favor the prosecution as much as is reasonable.

D. Part Four

We do not here express the right that employers may have to monitor the email use of their employees on company networks.

The issue of searches of employee emails on employers' networks is a discrete one, and has been treated separately from searches by commercial ISPs.[252] The interests for employers vis-à-vis their networks are different than the interests for commercial ISPs. For example, employers may be liable for emails sent from one employee to another that constitute sexual harassment.[253] Employers should therefore be able to protect themselves by monitoring contents of emails that exist on their networks. Furthermore, there is no overbearing privacy interest to counteract the employer's interest: courts often find that employees have less (but not wholly nonexistent) privacy rights in their workplace.[254] The assumption of risk doctrine may, therefore, be more applicable in the workplace. The doctrine may also be applicable because employees have a genuine choice: they can send private emails via their employer's network, or they can wait until they get home to send their emails via the commercial ISPs with whom they have contracted.[255] These emails will not get routed through their employer.

---

[250] *Krull*, 480 U.S. at 351.

[251] *Id.*

[252] Karyn F. Horner, *Guard Publishing Co.: Work E-Mail and the Battle Over Where Employers Can Draw the Line on Employees' E-Mail Use*, 29 BERKELEY J. EMP. & LAB. L. 487 (2008); Christine Neylon O'Brien, *Employees on Guard: Employer Policies Restrict NLRA-Protected Concerted Activities on Email*, 88 OR. L. REV. 195 (2009); Eric P. Robinson, *Update on Employer E-Mail Monitoring: The Ninth Circuit Joins the Mainstream*, 18 LAB. LAW. 355 (2003).

[253] Burkhart v. Am. Railcar Indus., Inc., 603 F.3d 472 (8th Cir. 2010).

[254] O'Connor v. Ortega, 480 U.S. 709, 717 (1987) ("The operational realities of the workplace, however, may make *some* employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."); I.N.S. v. Delgado, 466 U.S. 210, 224 (1984) ("[T]he employees' expectation of privacy in the plant setting here, like that in an automobile, certainly is far less than the traditional expectation of privacy in one's residence.").

[255] This approach to workplace emails isn't, of course, without controversy. Even at work, employees retain some privacy rights. In an era in which email is a primary medium of communication, an employee may have a need to communicate via email that cannot wait until

Although Parts One through Three of this holding may eventually be applied to employers, it is not certain that they will or should. This issue, therefore, should be left open for further analysis.

VII. CONCLUSION

The subject of this article concerns a very small part of a larger paradigm shift that criminal procedure and privacy law are currently undergoing. That shift is characterized by relatively fundamental and quickly evolving social realities brought about, in part, by the development of computers and cyberspace and the concomitant interconnectedness of the world. This shift challenges the law to keep pace.[256]

Prior to the 1980s, criminal procedure law was characterized by adherence to well-established common law principles, the law's ability to keep pace with technological developments,[257] predictable borders (geographic, communicative, and personal),[258] and the limited criminalization of conduct.[259] Currently, the rapid development and

---

she gets home. She may have to send or receive information about a sick relative, for example, or communicate with her child's school. Although this article is limited to non-work related emails, there certainly may be a zone of privacy for such work emails.

[256] *See* Amy E. Wells, *Criminal Procedure: The Fourth Amendment Collides With the Problem of Child Pornography and the Internet*, 53 OKLA. L. REV. 99, 99 (2000) ("For modern individuals, cyberspace is the 'new frontier.' Increasingly, it has become the realm in which business is conducted, friendships are cultivated, and information is exchanged. Unlike all other uncharted territories, however, cyberspace has no physical geography; no territorial boundaries exist. Largely for this reason, traditional legal doctrines appear ill equipped to deal with contemporary problems that originate in cyberspace. In all likelihood, the immensity and rapid growth of cyberspace has already outstripped the ability of the law to keep pace.").

[257] To illustrate this, consider that before the 1930s, the number of Supreme Court cases per decade using the terms "technology" or "communications" were always below forty. This number gradually increased, and hit a plateau in the 1980s, with over 500 cases that decade. The plateau has remained stable since then. Consider further the numbers associated with all federal courts: through the 1950s, these courts issued under 100 opinions each decade using the terms "technology" or "communications." This number increased to 1,247 in the 1990s, and then nearly tripled in the new century, with 3,606 cases between 2000 and the September 2010.

[258] A map of worldwide telegraph cables in 1901 shows that international communications remained focused on the east coast of the United States and the United Kingdom. In other words, they consisted of linear and limited structures centered on traditional nodes of power. *File: 1901 Eastern Telegraph Cables.png*, WIKIMEDIA COMMONS, http://commons.wikimedia.org/wiki/File:1901_Eastern_Telegraph_cables.png (last visited Dec. 15, 2010). Although the Internet backbone reflects this linear shape, the reality of its communicative nature is illustrated as an intricate web of communicative lines, with millions of nodes able to connect directly with millions of others. *History of the Internet*, UNC.EDU, http://www.unc.edu/~unclng/Internet_History.htm (last visited Dec. 15, 2010); *File: Internet Map 1024.jpg*, WIKIPEDIA, http://en.wikipedia.org/wiki/File:Internet_map_1024.jpg (last visited Dec. 15, 2010).

[259] After 1980, the number of federal criminal statutes exploded. John S. Baker, Jr., *Measuring the Explosive Growth of Federal Crime Legislation*, FEDERALIST SOC'Y FOR LAW & PUB. POL'Y 3 (2004),

redevelopment of technologies that fundamentally alter people's relations with others, with themselves, and their worlds are changing our notions of privacy, especially when it comes to communications.

There are, for example, countless ways to communicate with others: email, instant messaging, forum posting, text messaging, Twitter, Facebook postings, Facebook messages, blogs, Skype, and on and on. Many of these forms of communication are new relative to the age of the Internet. How people interact with them and how they impact people are still open questions.[260]

Along with these new forms of communication come new legal challenges to communication in cyberspace. The Obama administration has asked ISPs to modify their networks to facilitate the placement of e-wiretaps. This would include enabling the government to successfully wiretap even encrypted emails.[261] Countries such as the United Arab Emirates,[262] Saudi Arabia,[263] and India[264] have threatened to monitor, censor, or cut off BlackBerry communications. New technologies like GPS[265] and OnStar[266] provide an unprecedented opportunity for law enforcement to watch people in novel ways. It is not clear that courts or legislatures are capable of addressing these many new issues. The danger is that their inability or unwillingness to do so will leave a trail of criminal defendants and others in their wake who receive something less than justice.

In this new digital era, there are five imperatives. First, we must understand the challenges, limits, and opportunities for law inherent in new and emerging technologies. Second, we must continue to address the applicability of traditional legal rules to novel technological developments. Third, we must adopt flexible rules that can address constantly evolving technology but that don't hinder the development of settled rules

---

http://fedsoc.server326.com/Publications/practicegroupnewsletters/criminallaw/crimreportfinal.pdf. Similarly, prison populations have skyrocketed since 1980. *Prison Population Counts*, BUREAU OF JUSTICE STATISTICS, http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=131 (last visited Dec. 15, 2010); *The Punishing Decade: Prison and Jail Estimates at the Millenium*, JUSTICE POLICY INSTITUTE, May 2000, http://www.justicepolicy.org/images/upload/00-05_REP_PunishingDecade_AC.pdf (last visited Dec. 15, 2010).

[260] Until recently, research into online speech has been relatively sparse. *See* PATRICIA WALLACE, THE PSYCHOLOGY OF THE INTERNET 2 (1999).

[261] Charlie Savage, *U.S. is Working to Ease Wiretaps on the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1.

[262] Barry Meier & Robert F. Worth, *Emirates to Cut Data Services of BlackBerry*, N.Y. TIMES, Aug. 2, 2010, at A1.

[263] Kevin J. O'Brien, *Saudis Relent a Bit on Shutting Down BlackBerry*, N.Y. TIMES, Aug. 11, 2010, at B2.

[264] Vikas Bajaj, *India Warns That It Will Block BlackBerry Traffic That It Can't Monitor*, N.Y. TIMES, Aug. 13, 2010, at B3.

[265] There is a circuit split regarding whether a government agent attaching a GPS device to a car violates the car operator's Fourth Amendment rights. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) (yes); United States v. Smith, 387 F.App'x 918 (11th Cir. 2010) (no).

[266] John Schwartz, *This Car Can Talk. What It Says May Cause Concern*, N.Y. TIMES, Dec. 29, 2003, at C1.

when technological innovations slow. Fourth, we must take control of redrawing electronic borders to maximize the free trade of ideas and an open cyberspace. We must regulate cyberspace to ensure both a free market and individual liberties. Fifth, we must be prepared to make precedent-settling rulings where the technology and its use are clear and stable.

Enter the question of ISPs' ability and right to search the contents of people's emails that exist on the ISPs' networks. This is an issue ready to be settled. Email has remained a stable technology for years, if not decades. It is no longer emerging. Rather, its nature as a technology and communicative medium has remained the same for a long time. It is a locus of a lot of private, legal communication. The law regarding it therefore can be settled and deserves to be settled. By doing so, we can maximize individual privacy interests, but we can also begin to map out exceptions to that interest that will allow ISPs to manage their networks and law enforcement to be more effective. For example, we might conclude that using sniffer programs to detect *only* known images of child pornography is not a prohibited search. Currently, that question is an open one.

We need to begin to make some precedent-setting rulings regarding communication in the digital age. Because it is stable and well known, email is a very uncontroversial place to start. Whether we choose to use statutory, constitutional, or subconstitutional law to ensure email users' privacy, we ought to act. The circumstances allow it, and our privacy interest demands it.