INTERNET SURVEILLANCE LAW AFTER THE USA PATRIOT ACT: THE BIG BROTHER THAT ISN'T

Orin S. Kerr

97 NORTHWESTERN UNIVERSITY LAW REVIEW
(forthcoming 2003)

This paper can be downloaded without charge from the Social Science Research Network Electronic Paper Collection: http://ssrn.com/abstract_id=317501
INTERNET SURVEILLANCE LAW
AFTER THE USA PATRIOT ACT:
THE BIG BROTHER THAT ISN’T

Orin S. Kerr

97 NORTHWESTERN UNIVERSITY LAW REVIEW
(forthcoming 2003)

In this article, Professor Kerr argues that the common wisdom on the USA Patriot Act is wrong. Far from being a significant expansion of law enforcement powers online, the Patriot Act actually changed surveillance law in only minor ways and added several key privacy protections. By explaining the basic framework of surveillance law and applying it to the Patriot Act, Professor Kerr shows how the Patriot Act helped rationalize Internet surveillance law in ways that both law enforcement and civil libertarians should appreciate.

---

*A Associate Professor, George Washington University Law School. From October 1998 to July 2001, the author was a Trial Attorney at the Computer Crime and Intellectual Property Section of the United States Department of Justice. All of the views expressed in this article are solely the author’s, and do not reflect the positions of the Department of Justice. Thanks to Peter Swire, Steve Saltzburg, Peter Raven-Hansen, Cynthia Lee, Jon Molot, and Mark Eckenwiler for commenting on earlier drafts.

** The current version of this paper has been accepted for publication but has not yet been edited by the Northwestern University Law Review and remains a work-in-progress. Do not quote without permission. The author welcomes comments at okerr@main.nlc.gwu.edu.
INTRODUCTION

Following the terrorist attacks against New York and Washington on September 11, 2001, Congress rushed into action and quickly passed anti-terrorism legislation known as the USA Patriot Act. The Patriot Act has been widely understood as a "sweeping" anti-terrorism law that gave the government "vast powers" to conduct electronic surveillance over the Internet. The Act’s surveillance provisions proved so controversial that House Republicans refused to support the Act absent a sunset provision that will nullify several of its key provisions after four years, on December 31, 2005. To many legislators, the vast law enforcement authorities unleashed by the Patriot Act seemed too dangerous to extend indefinitely.

The Patriot Act triggered tremendous anxiety in part because few understood exactly what it did. At the time of its passage, even many key legislators seemed to have very little idea of the rules

---

1 Pub. L. 107-56, 115 Stat. 272, enacted October 26, 2001. The formal title is the "Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (USA Patriot Act) Act of 2001." Id. The awkward name of the USA Patriot Act derives from its legislative history: the Act combines elements of two anti-terrorism bills, the Senate’s USA Act, S. 1510, and the House of Representative’s Patriot Act, H.R. 2975. The Senate approved the Uniting and Strengthening America Act (or "USA" Act) by a vote of 96 to 1 on October 11th, 2001. The House approved the Provide Appropriate Tools Required to Intercept and Obstruct Terrorism Act (or "Patriot" Act), by a vote of 337 to 79 on October 12th, 2001. The final bill started with the basic framework of the Senate bill, and then added many of the components of the House bill, to create a compromise bill that combined both titles to create the USA Patriot bill. The USA Patriot bill was approved by the House on October 24th by a vote of 356 to 66, passed the Senate on October 25th a vote of 98 to1, and was signed by President Bush on October 26th. For simplicity’s sake, I will refer to the final enacted law as the USA Patriot Act, the Patriot Act, or simply the Act.


3 Id.

4 See Pub. L. 107-56, § 224 ("[T]his title and the amendments made by this title . . . shall cease to have effect on December 31, 2005.") This so-called sunset provision does not apply to all of the Patriot Act’s amendments involving electronic surveillance: it applies to about half of the provisions. See id. (explaining the sections to which the sunset provision does not apply).

governing electronic surveillance, both before the Patriot Act and following it.⁶ Did the Act go too far? How much privacy did Internet users have, and how much were they giving away? No one seemed to know, and because the legislation rushed through Congress with remarkable speed,⁷ little in the way of Committee reports or other legislative history existed to help explain it.⁸ Most commentators simply assumed the worst: they sensed that Internet users probably had very little privacy on-line before the Patriot Act, and that the Patriot Act bargained away whatever precious drops of privacy they had left.⁹

This article argues that the common wisdom on the Internet surveillance provisions of the USA Patriot Act is wrong. The Patriot Act did not expand law enforcement powers on-line dramatically, as its critics have alleged. The Patriot Act made mostly minor amendments to the electronic surveillance laws. Some of these changes expanded law enforcement powers, but some of them protected privacy and civil liberties. Ironically, several of the most controversial amendments may have actually increased privacy protections, rather than decreased them. While critics of the Patriot Act have rightly insisted that the government should have no more surveillance power than it needs, they have failed to see that the Patriot Act generally offers a balanced approach that in many ways protects civil liberties more than the laws it replaced. The Patriot Act is hardly perfect, but it is not the Big Brother law that many have feared.

In this article, I hope to explain how and why the popular understanding of the Patriot Act missed the mark. I will begin by explaining what Internet surveillance is and how it works, which creates

---

⁶ See Editorial, Stampeded in the House, WASH. POST., Oct. 16, 2001, at A22 (noting that when the House voted on H.R. 2975 on October 12, 2001, “all manner of members of both parties complained that they had no idea what they were voting on, were fearful that aspects of the . . . bill went too far – yet voted for it anyway”).
⁹ See notes 68 to 79, infra.
the framework for the decisions that Congress must make when deciding how to regulate it. I will then apply this framework to study three of the major criticisms of the Patriot Act. This approach unfortunately sacrifices breadth for depth, but it allows us to see how misconceptions about both the law and technology of the Internet led to significant misunderstandings about the effect of the USA Patriot Act.

The article proceeds in four sections. Section I explains the basic framework of network surveillance law that governs any communications network. It explains how we can classify the laws that govern the surveillance of communications networks such as the postal system, the telephone, and the Internet using a series of dichotomies. Once we have developed the framework, we can articulate the entire set of surveillance laws for each network and make comparisons across different technologies. This section also explains how Internet surveillance includes both e-mail and packet-level surveillance, and how laws that govern Internet surveillance must grapple with both levels of surveillance.

Section II considers the highly controversial pen register amendments to the Patriot Act. These amendments applied a privacy law originally designed for the telephone to the Internet. The amendments have been widely criticized on the ground that they granted the government sweeping powers to investigate crime in cyberspace. After explaining why Internet surveillance is primarily governed by statutory law, rather than the constitutional protections of the Fourth Amendment, Section II argues that the criticisms of the pen register amendments are unfounded. The pen register amendments reaffirmed existing practice, and on the whole probably increased privacy protections afforded to Internet communications, rather than decreased them.

Section III studies the Patriot Act’s impact on the FBI Internet surveillance tool popularly known as “Carnivore.” The Patriot Act has received broad criticism for expanding the use of Carnivore, which itself has been portrayed as a dangerous tool that enables the FBI to invade privacy online. The analysis explains how surveillance tools such as Carnivore work, and how Carnivore was itself designed to ensure compliance with court orders, not invade privacy in an effort to circumvent judicial review. It also explains how the Patriot Act
strengthens legal restrictions on the use of Carnivore.

Section IV addresses the new “computer trespasser” exception to the Wiretap Act. The trespasser exception has drawn criticism for weakening the Wiretap Act’s privacy protections in cyberspace. The analysis explains how the Wiretap Act applies to the Internet, and how the application of the law designed for the telephone to the Internet creates the need for a trespasser exception. The section also explains how the trespasser exception should help to protect privacy rather than threaten it by minimizing the scope of other exceptions to the Wiretap Act.

Finally, I must acknowledge that the contents of this article were shaped in part by my personal experience at the Department of Justice. For three years leading up to the summer of 2001, I was a lawyer in the Computer Crime and Intellectual Property Section of DOJ’s Criminal Division. My experience at DOJ included working with the Internet surveillance laws that existed before the Patriot Act. I also spent substantial time drafting and commenting on legislative proposals to amend those laws, including some that influenced portions of what later became the Patriot Act. I hope that my familiarity with these laws from my time in government will shed light that outshines the occasionally myopic effect of my personal experience.

I. A GENERAL FRAMEWORK OF NETWORK SURVEILLANCE LAW

Communications networks are a defining feature of modern life. Hundreds of millions of Americans use the postal system, the telephone network, and the Internet to communicate with each other. Although these technologies differ from each other in important ways, they share a common function: they are all global communications

---

10 The Computer Crime and Intellectual Property Section maintains a website at www.cybercrime.gov. (last visited March 2, 2002). The Section is often referred to by its acronym CCIPS, pronounced SEA-sips.


12 See CASTELLS, supra note 12, at 6-10.
networks that allow us to send, receive, and store information.

Unfortunately, communications networks also provide a stage for the commission of criminal activity.\textsuperscript{13} Networks can be used by criminals to contact co-conspirators, deliver threats, further frauds, or engage in countless other criminal activities.\textsuperscript{14} When communications networks are used to further crimes, the network itself can becomes a crime scene.\textsuperscript{15} Telephone records, stored e-mails, and undelivered packages may contain important clues for law enforcement. Much like a physical neighborhood, the networks themselves can become surveillance zones, complete with criminals seeking to evade detection and police trying to catch them.

The goal of this section is to offer a taxonomy of network surveillance law. I hope to articulate a basic framework for understanding the legal rules that apply to the surveillance of communications networks such as the Internet, the postal network, or the telephone network. The framework allows us to appreciate the relationship between the different types of surveillance that can occur in a network, as well as to compare how the rules differ across different networks. I hope to show that the basic contours of surveillance law for any communications network involves only a small number of questions, which correspond to the “what,” “who,” “when,” and “how” of collecting evidence from the network. What kind of information exists in

\begin{flushright}
\textsuperscript{15} See \textit{United States Department of Justice, Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations} at vii (2001) (hereinafter “CCIPS manual”) (available at www.cybercrime.gov/ searchmanual.wpd) (“The dramatic increase in computer-related crime requires prosecutors and law enforcement agents to understand how to obtain electronic evidence stored in computers.”)
the network? Who collects it, how, and under what circumstances?

I will illustrate these principles by focusing on three network technologies: the Internet, the telephone system, and the postal system. For each network, I will show that the same surveillance issues arise in relatively similar form for each network independently of the technology involved. Different technologies may merit different answers to these questions, of course, but the basic questions remain the same. The analysis starts with the “what,” moves next to the “who,” turns to the “when,” and then concludes with the “how.”

A. Envelope Information vs. Content Information (“What”)

The fundamental purpose of a communications network is to send and receive communications. As a result, every communications network features two types of information: the contents of communications, and the addressing and routing information that the networks use to deliver the contents of communications. We can call the former “content information,” and the latter “envelope information.”

The essential distinction between content and envelope information remains constant across very different technologies, from postal mail to e-mail. Let’s start with postal mail. The content information for postal mail is the letter itself, stored safely inside its envelope. The envelope information is the information derived from the outside of the envelope, including the “to” and “from” address, the stamp and postmark, and the size and weight of the envelope when sealed.

Similar distinctions can be made for telephone conversations. The content information for a telephone call is the actual conversation between participants that could be captured by an audio recording of the call. The envelope information includes the number the caller dialed, the originating number from which the caller dialed, the time of the call, and the number of the receiver.

17 See 39 C.F.R. § 233.3 (c)(1) (articulating an administrative procedure for obtaining a “mail cover”, which is defined as “the process by which a nonconsensual record is made of any data appearing on the outside cover of any sealed or unsealed class of mail matter, or by which a record is made of the contents of any unsealed class of mail matter as allowed by law.”).
18 See 18 U.S.C. § 2510(8) (defining the “contents” of a “wire communication” as “any information concerning the substance, purport, or meaning of that communication.”)
and its duration. This information cannot be found on a physical envelope, of course. However, it equates roughly with the information derived from the envelope of a letter. In both cases, the envelope information contains “to” and “from” addressing, data about the time the communication was sent, and some information about the communication’s size and/or length.¹⁹

We can translate these principles to the Internet quite readily in the case of e-mail. The content information for an e-mail is the message in the body of the e-mail itself, much like the conversation in the case of a phone call and the letter in the case of postal mail. The e-mail also carries addressing information in what is known as a “mail header.” Mail headers are essentially digital postmarks that accompany every e-mail and carry information about the delivery of the mail.²⁰ Many e-mail programs show users only some of this information by default, but can be configured to reveal the full mail header.²¹ A full mail header looks something like this:

```
Received: from SpoolDir by NLCMAIN (Mercury 1.48); 25 Oct 01 20:56:41 EST/EDT
Return-path: <eck@panix.com>
Received: from mail2.panix.com (166.84.0.213) by main.nlc.gwu.edu (Mercury 1.48) with ESMTP;
    25 Oct 01 20:56:40 EST/EDT
Received: from panix3.panix.com (panix3.panix.com [166.84.1.3])
    by mail2.panix.com (Postfix) with ESMTP id 272278F14
    for <okerr@main.nlc.gwu.edu>; Thu, 25 Oct 2001 20:56:01 -
0400 (EDT)
Received: (from eck@localhost)
    by panix3.panix.com (8.11.3nb1/8.8.8/PanixN1.0) id
f9Q0u1d15137
    for okerr@main.nlc.gwu.edu; Thu, 25 Oct 2001 20:56:01 -
0400 (EDT)
From: eck@panix.com
Message-Id: <200110260657.8050u1d15137@panix3.panix.com>
Subject:
```

¹⁹ This information is generally known as “pen register” and “trap and trace” information. See notes 99 to 104, infra.


²¹ See id.
This gobbledygook is a mail header that was generated from an e-mail sent to my George Washington University e-mail account on October 25, 2001 from the e-mail address “eck@panix.com.” Each of the lines in the mail header has specific meaning, and read together tells a story about the message, how it was processed, and how and when the network directed it from its origin to its destination. Notice that the mail header above does not contain a subject line: although subject lines appear in the mail header, they are generally recognized to be “contents.” Viewed as a whole, the e-mail header (minus the subject) line provides information about the e-mail that is roughly analogous to envelope information for a postal letter or telephone call.

So much for e-mail. There is much more to Internet surveillance than e-mail. In fact, only a small fraction of the Internet’s traffic involves human-to-human communications such as e-mail messages. Most Internet communications are communications between humans and computers, such as World-Wide-Web pages in transit, commands sent to remote servers, and file transfers. Many others are computer-to-computer communications, such as network administrative traffic designed to keep the Internet running smoothly. These communications can provide evidence of crime just as e-mail can. For example, the government may wish to monitor a computer hacker by watching and recording the commands he sends to the computers he has hacked. These commands do not involve e-mail, but instead consist of

---

22 For example, the e-mail was sent at 8:51 pm, and was received at 8:56 pm. For more on how to read e-mail headers, see, e.g., Reading E-Mail Headers, http://www.stopspam.org/email/headers/headers.html (last visited June 4, 2002).

23 See CCIPS Manual, supra note [], at 148.


25 See id. at 13.
commands sent directly to the victim computer. When we think about Internet surveillance, we need to think beyond e-mail surveillance to include the surveillance of human-to-computer and computer-to-computer communications.

To understand how the envelope/content distinction applies to human-to-computer and computer-to-computer communications, it helps to understand a few details about how the Internet works. The Internet is a “packet switched” network. This means that every communication sent over the Internet is broken down into individual packets – the cyber equivalent of letters between two computers, each containing about one page of information – and the packets are sent across the Internet to their destination. Computers communicate with each other by sending and receiving packets of information across the Internet.

Surveilling the Internet at the packet level provides a second way of conducting Internet surveillance that we can think of as distinct from e-mail surveillance. Like other forms of surveillance, packet surveillance divides into envelope information and content information. When a computer sends information across the Internet, it breaks the communication into packets and creates a “packet header” to direct the packet to its destination. The packet header contains addressing information, such as the “to” and “from” Internet addresses of the two computers (often referred to as the Internet Protocol addresses, or

---

26 See, e.g., United States v. Seidlitz, 589 F.2d 152, 154-55 (4th Cir. 1978) (explaining how a recording device can be used to monitor the commands entered by a computer hacker unauthorized to use a network).
27 See GRALLA, supra note [ ], at 13.
28 See id.
29 See id. at 14-15 (explaining the packet-based nature of Internet communications). Consider web surfing. When an Internet user types in a website address into a browser, the computer sends out packets to the remote computer that hosts the website. These packets contain requests for the remote computer to send back the contents of the website. See id. at 140-45 (explaining how web pages work). The remote computer then sends back several packets that together contain the contents of the web page, and the user’s computer reassembles them and presents him with the web page requested. Although it appears to the user as though he is “visiting” the website, the computers achieve this appearance through a complex exchange of packets across the Internet.
30 See GRALLA, supra note 26, at 34-38.
simply IP addresses\textsuperscript{31}, as well information about what kind of packet it is (part of a web page, part of a picture file, etc.).\textsuperscript{32} When the packet arrives at its destination, the receiving computer sheds the packet header and keeps the original message. At the packet level, this message is the content information in the packet, generally referred to as the packet’s “payload.”\textsuperscript{33} Some communications (such as web pages in transit) typically are “packetized” only once: the host computer creates the packets, and the destination computer sheds the packet headers and reassembles the original file when the packets arrive. Other communications can be packetized several times over in the course of delivery; for example, an e-mail may be broken down into packets and reassembled into the original e-mail a few times on its trip from sender to receiver.

While I don’t wish to lose technophobic readers, it helps to understand the basic relationship between e-mail surveillance and packet surveillance. E-mail surveillance is a subset of packet surveillance, in that while an e-mail travels across the Internet, both the envelope and content information of e-mails are transferred as payloads of individual packets. Obtaining content information at the packet level for a packet that happens to carry an e-mail message may yield either envelope information for the e-mail (the e-mail header), or content information (the e-mail itself), or both (in the case of a short e-mail that can fit the entire header and message on one packet). We can visualize this relationship with the following figure:

\begin{figure}
\centering
\includegraphics[width=\textwidth]{packet_vs_email_surveillance.png}
\caption{Packet vs. E-Mail Surveillance}
\end{figure}

\textsuperscript{31} See Brendan P. Kehoe, \textit{Zen and the Art of the Internet} 5 (4th Ed. 1996) (explaining IP addresses). IP addresses consist of a set of four numbers, each from 0 to 255, linked with a period. So, for example, an IP address might be 123.9.232.87. See id.

\textsuperscript{32} See Vincenzo Medillo, \textit{et al.}, \textit{A Guide to TCP/IP Networking}, available at http://www.ictp.trieste.it/~radionet/nuc1996/ref/tcpip/ (last visited February 23, 2002) (“IP’s job is simply to find a route for the datagram and get it to the other end. In order to allow routers or other intermediate systems to forward the datagram, it adds its own header. The main things in this header are the source and destination IP address, the protocol number, and another checksum.”)

\textsuperscript{33} See id.
This figure presents three Internet packets traveling in a row from right to left, carrying an e-mail as its payload. The first packet, Packet 1, starts with the packet header, and is then followed by a payload that consists of both a mail header and then the beginning of the contents of the e-mail. Packet 2 then starts with its own packet header, followed by a payload that consists of the next portion of the contents of the e-mail. Packet 3 comes last, and consists of a packet header and then the last portion of the e-mail. 34

At this point, we can summarize the envelope and content information for the four types of communications network surveillance with the following table:

<table>
<thead>
<tr>
<th>Surveillance Type</th>
<th>Envelope Information</th>
<th>Content Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Postal Mail</strong></td>
<td>1) To, from mailing address of a letter</td>
<td>The contents of the letter</td>
</tr>
<tr>
<td></td>
<td>2) Postmark, stamp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3) Color, size, weight of package</td>
<td></td>
</tr>
<tr>
<td><strong>Telephone</strong></td>
<td>1) To, from telephone numbers for a call</td>
<td>The contents of the telephone conversation</td>
</tr>
<tr>
<td></td>
<td>2) Time of call</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3) Length of call</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1) To, from e-mail</td>
<td></td>
</tr>
</tbody>
</table>

34 Notably, each packet includes its own number, so that the different packets can arrive at different times to their destination and computer at the destination will be able to reassemble them into the original communication. See Gralla, supra note [], at 13.
E-mail

<table>
<thead>
<tr>
<th>E-mail</th>
<th>Address for an e-mail</th>
<th>2) Mail header info (length of e-mail, digital postmarks) minus the subject line</th>
<th>The contents of the e-mail, including the subject line</th>
</tr>
</thead>
</table>

Internet Packets

<table>
<thead>
<tr>
<th>Internet Packets</th>
<th>1) To, from IP addresses</th>
<th>2) Remaining packet header information (length of packet, type of traffic)</th>
<th>Payload of the packet (the contents of any communication between two computers)</th>
</tr>
</thead>
</table>

Notably, all four categories mirror the distinction between envelope and content information. The envelope provides addressing information, and the content provides the actual communication that the network will deliver to its destination.

**B. Prospective vs. Retrospective Surveillance**

The next distinction to draw considers when the surveillance will occur. Is the surveillance designed to capture future communications that have not yet been sent over the network, or is it designed to look for stored records and past communications that may be retained in the network? I will call the former “prospective” surveillance, and the latter “retrospective” surveillance.

Wiretapping a telephone provides the classic example of prospective surveillance. When the FBI wiretaps a telephone line, it seeks to listen to the contents of future conversations. In the case of retrospective surveillance, in contrast, the government seeks to access stored records made from past communications. The use of O.J. Simpson’s telephone records in his murder trial furnishes a well-known example. The Los Angeles Police Department obtained Simpson’s phone records to show that Simpson had made several suspicious calls the night of his wife’s murder. This was an example of retrospective surveillance, and more specifically retrospective surveillance of envelope information: the police used the phone company’s stored business records relating to past communications to try to prove Simpson’s

---

36 See Michael Miller, Time of Phone Call a Key to O.J. Case, SAN FRANCISCO EXAMINER, at A1 (August 13, 1994).
guilt.37

The law often distinguishes between prospective and retrospective surveillance because they raise somewhat different privacy concerns. As Justice Douglas noted in his concurrence in Berger v. New York,38 prospective surveillance can at worst constitute “a dragnet, sweeping in all conversation within its scope.”39 The surveilling party taps into the network at a given place and picks up traffic passing through. The party cannot know in advance exactly what the traffic will be. Some of the traffic may be relevant, but usually most of the traffic will not be.40 Further, it can be technically difficult (if not impossible) to filter the communications down to the relevant evidence before the government observes it. Accordingly, prospective surveillance tends to raise difficult questions of how the communications should be filtered down to the evidence the government seeks.41 In contrast, the scope of retrospective surveillance is generally more limited. The primary difference is that in most cases a substantial portion of the evidence will no longer exist.42 because retrospective surveillance involves accessing records that has been retained in a network, the scope of surveillance ordinarily will be limited to whatever information or records may have been retained in the ordinary course of business.43 Some records may be kept, but others will not be.

A second difference between prospective and retrospective surveillance is that the process of storing records may itself help filter them. For example, e-mails arriving at an Internet service provider will ordinarily be screened and deposited by the ISP’s computer into

37 See id.
39 Id.
40 See Scott v. United States, 436 U.S. 128, 145 (1978) (Brennan, J., dissenting) (“Because it is difficult to know with any degree of certainty whether a given communication is subject to interception prior to its interception, there necessarily must be a margin of error permitted.”).
41 See Scott, 436 U.S. at 140-43 (discussing difficulties of filtering the fruits of a wiretap).
42 See CCIPS Manual, supra note 16, at 137 (“In general, no law regulates how long network service providers must retain account records in the United States. Some providers retain records for months others for hours, others not at all.”).
43 See id.
individual accounts. If law enforcement obtains an order compelling the ISP to divulge all stored e-mails in a particular e-mail account, the ISP will be able to find those e-mails without screening through unrelated files. Because of this, retrospective surveillance often presents less formidable filtering challenges than prospective surveillance. The difference is merely one of degree -- filtering through unrelated files for materials targeted by a court order is inevitable -- but the more limited scope of the evidence reduces the likelihood that retrospective surveillance will become the “dragnet” that Justice Douglas feared.

We can see these differences clearly in the case of Internet surveillance. Retrospective surveillance of a computer network generally means accessing stored files; an individual will log on to a computer and look through logs and/or files that the system may have retained in a particular folder or storage location. In contrast, prospective surveillance means either intercepting Internet packets as they cross the Internet, or else installing a monitoring device that collects the information immediately before it is packetized and sent across the Internet or else immediately after it arrives at its destination and is depacketized. The latter will tend to pick up more information than the

---

44 See id. at 82.
45 See, e.g., United State v. Lamb, 945 F. Supp. 441, 458-59 (search warrant ordering AOL to divulge “all stored files” in specific Internet accounts).
46 See Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) (“In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. Similar dangers, of course, are present in executing a warrant for the "seizure" of telephone conversations. In both kinds of searches, responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.”).
47 Notably, the technology of the Internet can blur the line between prospective and retrospective surveillance because communications in transit from their origin to their
C. Powers of the Government vs. Powers of the Provider ("Who")

Having explored the types of information that the government may wish to monitor on a communications network, we can now look to the different types of legal rules that may regulate the surveillance. Legal rules governing surveillance of communications networks generally divide into two types: rules concerning government surveillance of the network for law enforcement purposes, and rules governing network providers who may conduct surveillance on their own and wish to disclose the information to the government.49

Of these two types of rules, the latter is less understood, but no less important. In any communications network, each segment of the network will be administered by a service provider with responsibility for

---

48 See Gralla, supra note 26, at 15. This may depend on the particular circumstances, however. For example, a network may or may not have a “firewall” in place that records packet header information entering and/or exiting the network protected by the firewall. Absent a firewall, no record of these packets would ordinarily be kept.

49 Another possible category exists: rules concerning provider surveillance of the network at the request of (or pursuant to a court order obtained by) law enforcement. However, I will consider these rules as a subset of the rules concerning government surveillance of the network.
that portion of the network. A network can have a single provider: for example, the U.S. Postal Service enjoys a statutory monopoly over the United States postal mail system. Most networks are decentralized, however. The Internet provides a clear example of a highly decentralized network. No one “owns” the Internet as a whole. Instead, thousands of independent Internet service providers (known as ISPs) each administer small corners of the network.

Rules governing provider surveillance are quite important because providers often need to conduct surveillance of their corner of the network for a variety of business-related reasons. For example, the phone company may need to keep records of calls for long-distance billing (envelope surveillance), or may need to listen to calls on occasion to combat telephone fraud or check the quality of the line (content surveillance). Similarly, ISPs may need to maintain e-mail logs, or may need to intercept communications in transit to determine the source of a network problem or unauthorized intruder. Providers may discover evidence of a crime on their own and wish to report it to law enforcement. When we analyze rules that govern network surveillance, we need to examine both the rules that apply to law enforcement, and the laws that apply to the providers themselves.

1. Government Powers

There are several ways to categorize the rules that regulate government surveillance. Of these, two features tend to be the most important. The first considers the legal threshold that the government must satisfy before it can collect a particular type of information. The

---

50 See Castells, supra note 12.
52 See Gralla, supra note 26 (“How the Internet works”)
53 See, e.g., Smith v. Maryland, 442 U.S. 735, 742 (1979) (“In fact, pen registers and similar devices are routinely used by telephone companies for the purposes of checking billing operations, detecting fraud and preventing violations of law.”) (internal quotations omitted).
54 See, e.g., Bubis v. United States, 384 F.2d 643 (9th Cir. 1967)
55 See, e.g., Clifff Stoll, The Cuckoo’s Egg (1989) (recounting how a system administrator conducted electronic surveillance of his network to trace a computer hacker).
Internet Surveillance Law

second considers whether different rules govern depending on whether the government conducts the surveillance of the network itself, as opposed to when the government obtains an order requiring the provider to monitor on the government’s behalf.\(^{56}\)

\(\textit{a. Thresholds ("When")}\)

The first question is, for a given type of information to be acquired in a certain way, what threshold showing should the government be required to make before it can acquire the information? For example, should the FBI be allowed open postal mail without a court order, or must the FBI first obtain a search warrant? Can the local police require the phone company to provide a customer’s long-distance records without a court order, or is some court order required, and if so, what kind of order?

We can place the different threshold showings along a continuum, ranging from the lowest threshold to the highest. A continuum based on thresholds commonly found in current surveillance law might look something like this:

\[\textbf{Table 2: Legal Thresholds for Government Surveillance}\]

1) \textit{No legal process.} The government can acquire the information without process or order.

2) \textit{Subpoena.} The government must obtain a subpoena, such as a grand jury subpoena duces tecum\(^{57}\) or an administrative subpoena, before acquiring the information.\(^{58}\) The subpoena compels the provider to disclose the information to the government.

3) \textit{Relevance court order.} The government must obtain a court order before acquiring the information, but can obtain the order merely by certifying to the court that the information likely to be obtained is relevant to a law

\(^{56}\) Other questions include the role of judicial review in obtaining the order and later challenging it, as well as the remedy when the law has been violated. From a practical standpoint, these factors can be important determinants of how closely and consistently the laws are followed. For the sake of simplicity, however, I will skip these questions in the course of the analysis.

\(^{57}\) See, \textit{e.g.}, Fed. R. Crim. Pro. 6 (granting subpoena power to federal grand jury).

\(^{58}\) See, \textit{e.g.}, 5 U.S.C. App. (authorizing administrative subpoenas pursuant to § 6(a)(4) of the Inspector General Act).
enforcement investigation.\footnote{See, e.g., 18 U.S.C. § 3123 (describing process for obtaining a pen register or trap and trace order).}

4) \textit{Articulable facts court order.} The government must obtain a court order before acquiring the information, and to obtain the order must offer specific and articulable facts establishing reasonable grounds to believe the information to be obtained is both relevant and material to an ongoing criminal investigation.\footnote{See, e.g., 18 U.S.C. § 2703(d) (requiring government to obtain a court order before ordering an Internet surface provider to divulge records, and stating that the order must state "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.").}

5) \textit{Probable cause search warrant.} The government must obtain a search warrant before acquiring the information. The search warrant requires "probable cause," which in the criminal context means that the government must offer facts establishing a likelihood that a crime has occurred and that evidence of the crime exists in the location to be searched.\footnote{See Fed. R. Crim. Pro. 41 (authorizing the issuance of search warrants based on probable cause); 18 U.S.C. § 2703(a) (requiring a search warrant to compel an ISP to disclose the contents of certain types of stored communications held by the ISP).}

6) \textit{"Super" search warrant.} The government must obtain a special search warrant before acquiring the information that adds threshold requirements beyond those of ordinary search warrants (e.g., requiring the government to exhaust all other means of obtaining the information, requiring special authorization, etc.).\footnote{See 18 U.S.C. § 2516 (describing procedure for obtaining a Wiretap order).}

7) \textit{The government may not acquire the information under any legal process.} The law may forbid the government from acquiring the information regardless of the legal process.

Importantly, this list is not designed to be comprehensive. Instead, it reflects the continuum of court orders and legal processes that Congress currently uses to govern law enforcement surveillance of communications networks. For the most part, the greater the privacy interest at stake, the higher the threshold Congress uses. Exactly what thresholds apply is up to Congress when it enacts statutory privacy laws and the courts when they interpret the Fourth Amendment.
b. Direct vs. Indirect Surveillance ("How")

The second issue raised by government surveillance is the difference between what I will call “direct” and “indirect” government surveillance. Direct government surveillance rules authorize the government to conduct surveillance of the network on its own. In contrast, indirect government surveillance rules authorize the government to compel providers to conduct surveillance on the government’s behalf. The difference between direct and indirect surveillance lies in how court orders are implemented: does the government install its own monitoring device and tap into the network directly, for example, or does it serve the order on the provider and require the provider to conduct the monitoring and provide the results to law enforcement? The former is direct surveillance, the latter indirect surveillance.

The law may distinguish between direct and indirect surveillance because the two raise somewhat different privacy concerns. Indirect surveillance imposes a third party screen between the network and the government: the government sees only what the provider shows them. If the prospect of government overreaching concerns us more than that of provider overreaching, we may wish to impose more serious legal constraints on direct surveillance. At the same time, if there is reason to believe that a provider will be unwilling or unable to comply fully with a surveillance order, it may be preferable to allow the government to engage in direct surveillance. Each type of surveillance requires us to trust someone, and the difference is who we must trust: direct surveillance asks us to trust the government, and indirect surveillance asks us to trust the provider.

These competing concerns occupied central stage in the recent debate over Carnivore, the FBI’s tool for conducting direct surveillance of the Internet.63 Carnivore (later incarnations of which have been known as “DCS-1000”) is a “packet sniffer,” an Internet wiretap that

---

reads traffic while it is in transit in packet form.\textsuperscript{64} We will discuss Carnivore in depth in Section II, but for now it is important to note that the Carnivore debate relates in part on whether Internet surveillance should proceed by way of direct surveillance, as opposed to indirect surveillance. Should we trust providers use their own surveillance devices to effectuate court orders to conduct surveillance, or can we trust the FBI to conduct the surveillance with Carnivore? Who do we trust more: ISPs, or the FBI?

2. Provider Powers

We now turn to the second set of rules that govern surveillance of a network: rules that regulate providers, rather than the government. These rules govern when and how providers can collect information about the communications within their network, and also when they can disclose that information to law enforcement.

The rules regulating provider surveillance focus not on legal process, but rather on the factual circumstances in which the law prohibits provider surveillance and disclosure. Consider the following example. Imagine that a band of computer hackers breaks into a provider’s computer network, and that the hackers set up illegal servers from within the network to distribute counterfeit software to other hackers. The provider would likely notice the illegal entry when the unauthorized traffic slowed down the rest of the network. To locate the problem and block the unauthorized traffic, a network administrator would likely conduct various forms of surveillance. He might look through the network for the illegal server (conducting retrospective surveillance), set up a sniffer to watch the unauthorized traffic in an effort to trace it (prospective surveillance), and, if that is successful, may wish to disclose the records to the police to help them crack the case (disclosure). The rules governing the providers regulate the provider’s authority to conduct surveillance within its own network. What kind of surveillance should the provider be allowed to do, and in what circumstances, and when should the provider be permitted to disclose that information to law enforcement?

D. Constructing a Surveillance Matrix

\textsuperscript{64} See Section III, infra.
We can summarize the different categories using a fairly simple matrix. A blank matrix might look like this:

Table 3: Network Surveillance Matrix

<table>
<thead>
<tr>
<th>Type of Information</th>
<th>Conditions When Government Surveillance and Disclosure to Provider Allowed</th>
<th>Conditions When Government Surveillance Allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Envelope Information,</td>
<td>Direct:</td>
<td>Direct:</td>
</tr>
<tr>
<td>Prospective</td>
<td>Indirect:</td>
<td>Indirect:</td>
</tr>
<tr>
<td>Envelope Information,</td>
<td>Direct:</td>
<td>Direct:</td>
</tr>
<tr>
<td>Retrospective</td>
<td>Indirect:</td>
<td>Indirect:</td>
</tr>
<tr>
<td>Content Information,</td>
<td>Direct:</td>
<td>Direct:</td>
</tr>
<tr>
<td>Prospective</td>
<td>Indirect:</td>
<td>Indirect:</td>
</tr>
<tr>
<td>Content Information,</td>
<td>Direct:</td>
<td>Direct:</td>
</tr>
<tr>
<td>Retrospective</td>
<td>Indirect:</td>
<td>Indirect:</td>
</tr>
</tbody>
</table>

When we ask what rules should govern the surveillance of a particular matrix, we can now be specific and focus in the corresponding to the proper row and column of the matrix. The next section of the paper uses the insights developed above to consider the impact of the USA Patriot Act on Internet surveillance.

II. THE PATRIOT ACT AND APPLYING THE PEN REGISTER STATUTE TO THE INTERNET

The passage of the USA Patriot Act on October 26, 2001, has been widely portrayed as a dark moment for the civil liberties of Internet users. The ACLU declared that the Act gave law enforcement “extraordinary new powers.” Another civil liberties group, the Electronic Frontier Foundation, announced that “the civil liberties of ordinary Americans have taken a tremendous blow with this law.”

---

66 www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html (last visited March 2, 2002).
website of the Electronic Privacy Information Center featured a drawing of a tombstone that stated “The Fourth Amendment: 1789-2001.”\(^{67}\) Major media outlets agreed. *The New York Times* viewed the Act as an overreaction to September 11\(^{th}\), and concluded that the law gave the government unjustified “broad new powers.”\(^ {68}\) *The Washington Post* also opposed the Act: its editorial board described the Patriot Act as “panicky legislation” that “reduce[d] the healthy oversight of the courts.”\(^ {69}\) The unanimous verdict was that the Patriot Act created a sweeping and probably unjustifiable expansion of law enforcement authority in cyberspace.\(^ {70}\)

Is this verdict justified? To answer this, we first need to recognize that the Patriot Act is not a single coherent law. The Act collected hundreds of minor amendments to federal law, grouped into ten subparts or “Titles,” on topics ranging from immigration to money laundering.\(^ {71}\) With many of these amendments, the devil is in the details: especially in the electronic surveillance context, the complex relationship among sections of statutory text means that the changes often defy easy soundbites. Further, the language that passed on October 26\(^{th}\) differed in significant ways from the language the Justice Department first proposed just a few days after September 11\(^{th}\). The Congressional negotiations that ensured the quick passage of the Patriot Act led to many compromises, and even considerable victories for the Act’s opponents. Altogether, these features make broad characterizations of the Patriot Act difficult to maintain.

When we focus on the Internet surveillance provisions that passed into law, however, it becomes clear that the popular

\(^{67}\) See www.epic.org (visited November 12, 2001).


\(^{70}\) As a student author recently concluded: “Although it is unlikely that the USA PATRIOT Act’s far-reaching extensions of surveillance law would have enabled the government to prevent the tragedy we witnessed on September 11\(^{th}\), 2001, it is patently apparent how we will all pay the price of a false sense of security at the cost of cherished freedoms.” Sharon H. Rackow, Comment, *How The USA PATRIOT Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of “Intelligence” Investigations*, 150 U. Pa. L. Rev. 1651, 1696 (2002).

\(^{71}\) See Pub. L. 107-56. The Act consists of ten subparts, Titles I through Title X. Only one of these subparts, Title II, directly relates to Internet surveillance laws.
understanding of the Patriot Act is substantially wrong. The Patriot Act did not tilt the balance between Internet privacy and security strongly in favor of security. Most of the Patriot Act’s key changes reflected reasonable compromises that updated antiquated laws. Some of these changes advanced law enforcement interests, but others advanced privacy interests, and several did both at the same time. The media portrayal of the Patriot Act as “extraordinary” and “panicky legislation” turns out to have little in common with the law Congress actually enacted.

The remainder of this article explores how the common understanding of the Patriot Act missed the mark by focusing on three particularly controversial aspects of the Patriot Act. Admittedly, this approach sacrifices breadth for depth. It means that the article ignores dozens of Patriot Act amendments that are equally deserving of careful study. However, the approach also lets us examine a few specific controversies with care, and to use them as examples that generally apply to the Patriot Act as a whole.

For example, the Patriot Act made many minor changes to the rules governing retrospective surveillance, which affected the privacy protections governing both voicemails and Internet records. These changes appear in the newly revamped 18 U.S.C. § 2703. However, the three examples I study in this article all involve prospective surveillance. The limited scope of my approach also means that I focus on fairly specific changes to the surveillance laws, while ignoring others that may be related. For example, the pen register amendments clarified that the laws applied the Internet (which I discuss in this Section) and also allowed the government to obtain nationwide orders (which I do not discuss).

Of course, some provisions of the Patriot Act may prove to have serious negative consequences for privacy and civil liberties. The Patriot Act’s amendments relating to the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq., are particularly notable in this regard, as is the broader restructuring of the relationship between law enforcement and the intelligence community in surveillance investigations.

At the same time, several of the most controversial provisions in the Patriot Act were controversial primarily because they were misrepresented in the press. The attention paid to “roving wiretaps” provides a good example. Congress first enacted a law allowing the government to obtain roving wiretaps in criminal cases in 1986, and the debate over their use goes back to that period. See, e.g., Clifford S. Fishman, Interception of Communications in Exigent Circumstances: The Fourth Amendment, Federal Legislation, and the United States Department of Justice, 22 Ga. L. Rev. 1 (1987). These laws were challenged and upheld by the courts. See, e.g., United States v. Petti, 973 F.2d 1441, 1444 (9th Cir. 1992) (Browning, J.). Section 206 of the Patriot Act expanded this authority to FISA cases, so that it could be used in terrorism investigations, in addition to criminal investigations. The press and commentators often ignored this preexisting authority,
In particular, this section of the article will explore one of the most controversial provisions of the Patriot Act: the amendments making the “pen register” law applicable to the Internet. The pen register law has governed prospective envelope surveillance of the telephone since it was enacted in 1986, and the Patriot Act made clear that this law also applies to the Internet. The press uniformly presented this change as a significant expansion of law enforcement authority. The Washington Post stated that this change “makes it easier for the government to engage in wiretapping by, in effect, lowering the standard of judicial review.” The New York Times described this change as a grant of “broad authority to inspect logs of Internet use and the address fields of e-mail messages.” Both the political left and the political right agreed that this was a significant and potentially dangerous change. On the left, The New Republic thundered that this change gave the government “essentially unlimited authority to install recording devices” to monitor the Internet. On the right, a group of lawyers affiliated with the Federalist Society approved of the Patriot Act as a whole, but singled out the pen register amendments as the only really troubling change to the electronic surveillance laws.

however, and instead discussed the Patriot Act as if it were the first law to introduce roving wiretaps. See, e.g., Editorial, Constitutional Concerns, Daily Oklahoman, Sept. 29, 2001, at 6A; Erwin Chemerinsky, Giving Up Our Rights for Little Gain, L.A. Times, Sept. 27, 2001, at B17. As a result, to a large extent the public debate over the roving wiretap provisions of the Patriot Act concerned whether the events of September 11th justified a law that Congress had already enacted fifteen years earlier. Of course, the fact that Congress enacted a law in 1986 does not in itself justify its existence today, but it does seem relevant to whether the amendment broke new ground.

The pen register law is codified at 18 U.S.C. §§ 3121-27.

The pen registers laws were passed as part of the Electronic Communications Privacy Act, Pub. L. 99-508. (passed October 21, 1986).

See, e.g., Declan McCullagh, USA Act Stampedes Through, Wired News, Ocl. 25, 2001 available at www.wired.com/news/conflict/0,2100,47858,00.html (“The U.S. Senate is set to end a month-long debate over balancing freedom and security on Thursday by granting police more surveillance power and sharply curtailing Americans' privacy.”) (last visited March 9, 2002).

See Editorial, supra note 6.


See Federalist Society for Law and Public Policy Studies, White Paper on Anti-Terrorism Legislation: Surveillance & Wiretap Laws, Developing Necessary and
This section will explain why this criticism of the Patriot Act is unfounded. The pen register amendments to the Patriot Act do not signal an unwarranted expansion of law enforcement authority. To the contrary: the changes merely reaffirm existing law that aligns Internet surveillance law with postal and telephone surveillance. More importantly, the changes on the whole probably add to the privacy of Internet communications, rather than take from it. Ironically, the pen register amendments that have been portrayed as unwarranted expansions of law enforcement authority are neither unwarranted, nor even expansions of authority. This does not mean that Congress could not increase the privacy protections of the pen register law in the future; it could, and I think it probably should. However, the Patriot Act is not the source of the problem, but rather the first step toward a better solution.

To understand how the press and civil liberties groups misjudged the Patriot Act’s pen register amendments, we need first to step back and understand why statutory protections matter in this area, as well as how the law treats the prospective surveillance of envelope information in other contexts, such as the postal network and the telephone. We can then look at how the law applied to Internet envelope surveillance before the Patriot Act, and compare that to the law after the Patriot Act.

A. Internet Privacy is Statutory Privacy

When most of us think about surveillance and privacy law, we naturally think about the Fourth Amendment and the “reasonable expectation of privacy” test. In the case of Internet privacy law, however, the real action tends to be in the legislature, not the courts. The explanation for this lies in the narrow way that the Courts have interpreted the reasonable expectation of privacy test in communications networks. While many questions remain, the existing cases appear to have left Congress with a relatively free hand to create the set of rules it thinks best. To a surprising extent, Internet privacy is statutory

---

Constitutional Tools for Law Enforcement (authored by Tom Gede, Montgomery Kosma, and Arun Chandra) at 21-22 (calling the pen register amendments “the single most difficult issues presented by the new law”), available at http://www.fed-soc.org/Publications/Terrorism/Anti-TerrorismLegislation.pdf (last visited March 2, 2002)

privacy.\textsuperscript{82}

The cases most responsible for the fairly narrow Fourth Amendment protections in communications networks hold that an individual has no reasonable expectation of privacy in information revealed to third parties.\textsuperscript{83} If I tell you a secret, the government cannot violate my reasonable expectation of privacy by persuading you to disclose my secret to the police.\textsuperscript{84} While such as expectation of privacy might seem reasonable in a practical sense – a reasonable person might expect you not to disclose the secret – it is not “reasonable” in a constitutional sense.\textsuperscript{85}

This principle carries tremendous significance when we consider how the Fourth Amendment applies to communications networks. First, it means that envelope information ordinarily does not receive constitutional protection. After all, envelope information is simply the to/from information offered to the network provider to help the provider deliver the contents. It is necessarily disclosed to the provider. In the case of a telephone call, a caller necessarily discloses the phone number

\textsuperscript{82} Of course, this statement is based on current law. The Courts may start finding constitutional protections in Internet communications that may be difficult to see based on existing precedents. \textit{Cf.} Kyllo v. United States, 533 U.S. 27, 34 (2001) (suggesting that as technology advances, the courts should interpret the Fourth Amendment to “assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.”).


\textsuperscript{84} \textit{See Hoffa}, 385 U.S. at 302 (holding that Jimmy Hoffa’s Fourth Amendment rights were not violated when his friend to which he disclosed secrets became a government informant).

\textsuperscript{85} As the Supreme Court stated in \textit{Miller}:

the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, \textit{even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.}

he is dialing to the phone company when he communicates it to the phone company so the company can complete the call; this eliminates Fourth Amendment protection in the numbers dialed. 86 Similarly, in the case of postal mail, the courts have held that postal mail customers have no reasonable expectation of privacy in the outside of their envelopes and packages because it can be (and even must be) seen by Postal Service employees in the course of delivery. 87 As a result, the government can examine the outside of an envelope and copy the envelope information without a court order or a search warrant. 88 The courts have applied the same rationale to the Internet, holding that an Internet user cannot enjoy a reasonable expectation of privacy in non-content information sent to an ISP because the user has disclosed the information to the ISP. 89

The disclosure principle also has important implications for Fourth Amendment protections in the case of content information. Here, we have to be quite careful: the courts have struggled to apply the Fourth Amendment to contents sent over communications networks. The law is quite murky and may change. In general, however, the courts have held that a user does have a reasonable expectation of privacy in content information that is sealed away from the network provider, but does not retain such protection in information disclosed or openly visible to the provider. In the postal context, for example, a person normally enjoys Fourth Amendment in the contents of their sealed letters, 90 but

87 See United States v. Huie, 593 F.2d 14, 15 (5th Cir. 1979) (“There is no reasonable expectation of privacy in information placed on the exterior of mailed items and open to view and specifically intended to be viewed by others.”).
90 See Ex Parte Jackson, 96 U.S. (6 Otto) 727, 733 (1877)(concluding that the Fourth Amendment protects sealed postal letters); United States v. Phillips, 478 F.2d 743 (5th Cir. 1973) (“[T]he privacy of a sealed item bearing the proper amount of postage for a first class item is protected from warrantless opening, not because it is given the appellation ‘first class’ but because the Constitution commands that result.”).
not in their unsealed postcards or opened packages. In the context of the telephone network, a caller normally enjoys Fourth Amendment protection in the contents of their calls, but not when they are using cordless phones that operate via radio waves disclosed to the public. The courts have not yet reached how this rationale applies to Internet communications. However, because the contents of Internet communications are mixed together with envelope information and disclosed to the ISP, it is at least possible that courts will find that Internet users cannot have a reasonable expectation of privacy in Internet content information, much like postcards or cordless phone calls.

Under these precedents, Internet surveillance law has become predominantly statutory law. The rules that actually govern electronic

---

91 See United States v. Jacobsen, 466 U.S. 109, 119 (1984) (Respondents could have no privacy interest in the contents of the package, since it remained unsealed . . . .”); United States v. Vasquez, 858 F.2d 1387, 1391 (9th Cir. 1988) (concluding that because envelope was found unsealed, police officer’s search of its contents did not violate the defendant’s Fourth Amendment rights). Remarkably, no cases exist directly dealing with Fourth Amendment protections in postcards. However, there are many cases dealing with Fourth Amendment rights in unsealed packages and information on the exterior of packages and envelopes, all of which hold that a person has no Fourth Amendment protection in such information.


93 See, e.g., Tyler v. Berodt, 877 F.2d 705, 707 (8th Cir. 1989); McKamey v. Roach, 55 F.3d 1236, 1239-40 (6th Cir. 1995); United States v. McNulty, 47 F.3d 100, 104-106 (4th Cir. 1995); United States v. Smith, 978 F.2d 171, 177-81 (5th Cir. 1992). Of course, Congress can protect such calls when the Fourth Amendment does not. In the case of cordless telephone calls, Congress added statutory protection against their interception in 1994. See McKamey, 55 F.3d at 1238 n.1.

94 The Eighth Circuit may reach the issue in United States v. Bach, Cr. 02-1238, an appeal from the District of Minnesota that is currently pending. See also United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996) (concluding that an AOL user does retain a reasonable expectation of privacy in unopened e-mails stored with AOL).

95 Of course, this case law has not stopped most commentators on Internet surveillance law from making the case for strong privacy protections in constitutional terms. The most common approach is to recite a brief history of Fourth Amendment law ending in 1967 with Katz v. United States, 389 U.S. 347 (1967), and then to announce that Katz guarantees strong privacy protections in new technologies. See, e.g., Rackow, supra note 91, at 1656 (following this path and concluding that “[p]rivacy as protected by the Fourth Amendment denotes a right to be free from unwanted governmental surveillance.”). This approach surely reflects honorable aspirations, but it strangely ignores the fact that in the 35 years since Katz, the courts have mostly rejected such an expansive view of its
surveillance tend to be statutory rules, inspired by constitutional values but not necessarily governed by constitutional commands.\textsuperscript{96} These statutory laws govern network surveillance even when the Constitution does not: for example, Congress made it a crime to wiretap telephone lines in 1934,\textsuperscript{97} although wiretapping did not violate the Fourth Amendment at that time.\textsuperscript{98} Further, Congress has revisited the surveillance statutes every few years for the last few decades to take into account advancing technology and changing social norms. The two most important dates are 1968 and 1986: In 1968, Congress created the modern Wiretap Act that regulates prospective content surveillance of telephone lines today,\textsuperscript{99} and in 1986, Congress expanded that law to the Internet and added regulations of retrospective surveillance as well when it enacted the Electronic Communications Privacy Act.\textsuperscript{100}

B. \textit{Prospective Envelope Surveillance of the Postal Network and the Telephone}

Although Congress has enacted statutory privacy protections that govern network surveillance, Congress historically has shown little interest in protecting mere envelope information. While prospective content information has been regulated very strictly – with a warrant holding. \footnote{In fact, the courts have often deferred to Congress’s judgment when confronted with a Fourth Amendment challenge to electronic surveillance. \textit{See}, \textit{e.g.}, \textit{McNulty}, 47 F.3d at 104 (rejecting a claim of constitutional protection in calls to a cordless phone user, in part on the ground that holding to the contrary would force the court “to rule the statutory exceptions of Title III unconstitutional,” an “untoward result” given the “heavy presumption of constitutionality that attaches to the carefully considered decisions of a coequal and representative branch of our Government.”) (internal quotations and brackets omitted). \textit{See also}, \textit{Adams v. City of Battle Creek}, 250 F.3d 980, 986 (6th Cir. 2001) (“The Electronic Communications Privacy Act is part of detailed legislative scheme under Title III of the Omnibus Crime and Control Act of 1986. The legislation seeks to balance privacy rights and law enforcement needs, keeping in mind the protections of the Fourth Amendment against unreasonable search and seizure. Congress made the Act the primary vehicle by which to address violations of privacy interests in the communication field.”).}

\textsuperscript{97} \textit{See} 47 U.S.C. § 605 (1934); \textit{Nardone v. United States}, 302 U.S. 379, 384 (1937).

\textsuperscript{98} \textit{See \textit{Nardone}}, 302 U.S. at 384 (citing \textit{Olmstead v. United States}, 277 U.S. 438 (1928)).


\textsuperscript{100} \textit{See Pub. L.}, 99-508 (1986), Title I.
requirement in the case of the postal system, and a super-warrant requirement for telephones and the Internet – mere envelope information has received very different treatment. Envelope information has traditionally received little if any protection in communications networks such as the postal system and the telephone.

In the postal case, no statutory protection exists; surveillance of envelope information is governed solely by a postal regulation enacted in 1975. The regulation prohibits envelope surveillance of postal mail unless it is conducted pursuant to a request to initiate a “mail cover.” The regulation defines a mail cover as a “nonconsensual record . . . of any data appearing on the outside cover of any sealed or unsealed class of mail.” A mail cover can be instituted whenever a law enforcement agent files a written request with the Postal Inspector that “specifies . . . reasonable grounds to demonstrate that the mail cover is necessary to . . . obtain information regarding the commission or attempted commission of a crime.” When that request is received, the postal inspectors will initiate the mail cover and conduct envelope surveillance for 30 days. As a matter of privacy law, the mail cover regulation offers only meager privacy protection. No court order is required, and no judge need ever learn of the surveillance. If agents violate the statute,

---

101 See Ex Parte Jackson, 96 U.S. (6 Otto) 727, 733 (1877). Of course, this limitation is constitutional, not statutory. Congress has protected the content of sealed letters and packages sent through the mail through a criminal prohibition. See 18 U.S.C. § 1703 (“Whoever, being a Postal Service officer or employee, unlawfully . . . opens any letter . . . shall be fined under this title or imprisoned not more than five years, or both.”).

102 See 18 U.S.C. § 2518 (discussing the requirements that the government must meet to obtain a Wiretap Order).


104 39 C.F.R. § 233.3(b).

105 See id. at § 233.3(c)(1) (defining the phrase “mail cover.”) The reference to “contents” of “unsealed” matter presumably refers to postcards. This includes “the name of the addressee, the postmark, the name and address of the sender (if it appears), and the class of mail” Huie, 593 F.2d at 15, but may simply consist of a photograph of the exterior of the envelope. See 39 C.F.R. § 233.3(c)(2) (defining a “record” as “a transcription, photograph, photocopy or any other facsimile of the image of the outside cover, envelope, wrapper, or contents of any class of mail.”).

106 See id. at § 233.3(e)(2)(iii). The mail cover can be authorized on other grounds, see id., but these are the most common ones.

107 See id. at § 233.3(g)(5).
there is no remedy—criminal, civil, or suppression.  

The law offers somewhat higher protection for prospective envelope surveillance of the telephone network. For historical reasons, this law is known as the pen register law: it carries the name because in the 1960s the phone company could create a record of numbers dialed from a telephone by installing a device known as a pen register. The pen register law was first enacted in 1986, and creates a statutory criminal prohibition on the prospective surveillance of envelope information for the telephone network, subject to a few exceptions.

The pen register law allows the government to obtain a court order authorizing the collection of envelope information for renewable periods of 60 days. Although the application must be made by an attorney and approved by a federal judge, the threshold for obtaining the order is low: the attorney must only certify to the Court that “the information likely to be obtained . . . is relevant to an ongoing criminal investigation.” Violations of the pen register statute do not result in

---

108 See United States v. Hinton, 222 F.3d 664, 674 (9th Cir. 2000) (“Although it is undisputed that the officers did not follow the proper procedures for obtaining a mail cover, suppression is not the appropriate remedy . . . .”)

109 A pen register was described by one early court as follows:

The pen register is a mechanical device attached on occasion to a given telephone line, usually at central telephone offices. A pulsation of the dial on a line to which the pen register is attached records on a paper tape dashes equal to the number dialed. The paper tape then becomes a permanent and complete record of outgoing calls as well as the numbers called on the particular line. Immediately after the number is dialed and before the line called has had an opportunity to answer (actually the pen register has no way of determining or recording whether or not the calls are answered) the pen register mechanically and automatically is disconnected. There is neither recording nor monitoring of the conversation.

110 See Pub. L. 99-508, Title III, § 301(a).


113 18 U.S.C. § 3123(a). See also United States Telecom Ass’n v. FCC, 227 F.3d 450, 455 (D.C. Cir. 2000) (“Rather than the strict probable cause showing necessary for wiretaps, pen register orders require only certification from a law enforcement officer
suppression of the evidence; instead, the remedy is a criminal prosecution,\textsuperscript{114} and in the case of a lawyer, possible ethical charges.\textsuperscript{115}

C. Prospective Envelope Surveillance of the Internet: The Uncertain Privacy Protections before the USA Patriot Act

So much for the telephone and postal networks. How about the Internet? More specifically, in the period leading up to the Patriot Act, what privacy laws regulated the prospective surveillance of envelope information in the case of e-mail surveillance and packet surveillance?

The answer is surprisingly unclear. The only law that could conceivably have applied was the pen register statute, but it provided an odd mix of telephone-specific language and more general text. The statute divided the category of envelope information into two subcategories: the “to” addressing information, which historically would be obtained by installing a pen register, and the “from” addressing information, which historically would be obtained by running a “trap and trace.”\textsuperscript{116} Rather than refer to the information to be gathered, the

\[
\text{that } \text{"the information likely to be obtained is relevant to an ongoing criminal investigation."} \\
\text{So long as the application contains these elements, the court will authorize the installation of the pen/trap device. The court will not conduct an \text{"independent judicial inquiry into the veracity of the attested facts."} \text{In re Application of the United States, 846 F. Supp. 1555, 1558-59 (M.D. Fla. 1994). See also United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) (\text{"The judicial role in approving use of trap} \\
\text{\text{and trace devices is ministerial in nature."}).}}
\]

\text{\textsuperscript{114} As one court has explained:}

\[
\text{[t]he salient purpose of requiring the application to the court for an order} \\
\text{is to affix personal responsibility for the veracity of the application (i.e.,} \\
\text{to ensure that the attesting United States Attorney is readily identifiable} \\
\text{and legally qualified) and to confirm that the United States Attorney has} \\
\text{sworn that the required investigation is in progress. . . . As a form of} \\
\text{deterrence and as a guarantee of compliance, the statute provides . . . for a} \\
\text{term of imprisonment and a fine as punishment for a violation [of the} \\
\text{statute].}}
\]

\text{\textit{In re Application of the United States, 846 F. Supp. at 1559.}}

\text{\textsuperscript{115} A knowingly false certification would constitute not only a violation of} \\
\text{the statute, but also a materially false statement to the court in the course of an attorney’s} \\
\text{official duties.}

\text{\textsuperscript{116} \text{"Trap and trace" information is so called because collecting the information} \\
\text{originally required the telephone company to trace the phone line using a tool known as a}
structure of the pen register law prohibited the installation or use of a pen
register or trap and trace device without a court order.

Before the Patriot Act, however, the definitions of the terms
“pen register” and “trap and trace device” did not make clear whether
they applied only to the telephone, or whether they could also apply to
the Internet. The definition of “trap and trace device” was quite broad:
it referred to “a device which captures the incoming electronic or other
impulses which identify the originating number of an instrument or device
from which a wire or electronic communication was transmitted.” 117
Given that most Internet communications are “electronic
communication[s],” 118 this definition appeared to apply to the Internet as
well as to the phone system. In contrast, the definition of “pen register”
appeared strikingly telephone-specific: the law defined a pen register as
“a device which records or decodes electronic or other impulses which
identify the numbers dialed or otherwise transmitted on the telephone to
which such device is attached.” 119

“terminating trap.” In re Application of the United States for an Order Authorizing the
Installation of A Pen Register or Touch-Tone Decoder and A Terminating Trap, 610 F.2d
1148, 1151 (3d. Cir. 1979).


118 See CCIPS Manual, supra note 16, at 106 (“[A]lmost all Internet
communications (including e-mail) qualify as electronic communications.”). The phrase
“electronic communication” means

any transfer of signs, signals, writing, images, sounds, data, or
intelligence of any nature transmitted in whole or in part by a wire,
radio, electromagnetic, photoelectronic or photooptical system that
affects interstate or foreign commerce, but does not include--

(A) any wire or oral communication;

(B) any communication made through a tone-only paging
device;

(C) any communication from a tracking device (as defined in
section 3117 of this title); or

(D) electronic funds transfer information stored by a financial
institution in a communications system used for the electronic storage
and transfer of funds;


Peter P. Swire, Administration Wiretap Proposal Hits the Right Issues But Goes Too Far,
Brooking Institution Analysis Paper #3, October 3, 2001 (available at
So did the pen register laws apply to the Internet? The Justice Department’s view was that they did, and that the pen register laws regulated both Internet e-mail and packet-level envelope surveillance just as they did telephone envelope surveillance. In fact, Justice Department practice had embraced the pen register statute for several years as the means of conducting Internet envelope surveillance. Federal judges had at least implicitly agreed: judges had signed pen register orders authorizing Internet e-mail and packet surveillance hundreds if not thousands of times in the years leading up to the Patriot Act. While some magistrate judges had asked prosecutors whether the statute applied to the Internet, the judges always satisfied themselves that it did and signed the order. One magistrate judge in Los Angeles had also written an unpublished order agreeing that the statute applied to the Internet: “[a]lthough apparently not contemplated by the drafters of the original statute,” Judge James McMahon wrote, “the use of a pen register order in the present situation is compatible with the terms of the statute. The text remained uncertain, but as a matter of law enforcement practice, it was generally understood that the pen register

http://www.brook.edu/dybdocroot/views/articles/fellows/2001_swire.htm) (“ECPA has not aged gracefully. Much of its language reflects the telephone technology of the 1980s rather than the Internet realities of today.”)

120 See CCIPS Manual, supra note 16, at 102. As the DOJ described in their January 2001 Manual, “The Pen/Trap statute permits law enforcement to obtain the addressing information of Internet communications much as it would addressing information for traditional phone calls. . . . The Pen/Trap statute [also] permits law enforcement to obtain the addressing information of Internet e-mails (minus the subject line, which can contain contents, cf. Brown, 50 F.3d at 292) using a court order, just like it permits law enforcement to obtain addressing information for phone calls and individual Internet “packets” using a court order.” Id.

121 See Carl S. Kaplan, Concern Over Proposed Changes in Internet Surveillance, N.Y. TIMES, September 21, 2001, at E1 (quoting Marc Zwillinger, former Trial Attorney of the Computer Crime and Intellectual Property Section of DOJ, that during his time at the Justice Department, he used the pen register statute to obtain envelope information “hundreds of times”).

122 When I was at the Justice Department, I would occasionally hear of magistrate judges raising such questions with Assistant U.S. Attorneys who applied for pen register orders to conduct Internet surveillance.

laws applied to the Internet.\textsuperscript{124}

Notably, the government’s conclusion that the pen register statute applied to the Internet created a double-edged sword. Without the pen register statute, the government could conduct envelope surveillance without a court order: the government – or anybody else – could wiretap the Internet and collect any non-content information it wished without restriction.\textsuperscript{125} Applying the pen register laws to the Internet denied the government the power to conduct envelope surveillance without a court order, limiting government power, and blocked private entities from conducting prospective envelope surveillance, protecting privacy. At the same time, applying the pen register statute to the Internet benefited law enforcement by giving the government a relatively easy way of obtaining orders compelling ISPs to conduct prospective envelope surveillance on the government’s behalf. Absent that authority, the government would need to either install monitoring devices itself, rely on the voluntary cooperation of ISPs, or try to use other laws requiring a higher factual showing than the pen register laws to obtain court orders compelling ISPs to conduct envelope surveillance.\textsuperscript{126}

Despite the fact that federal judges appeared willing to agree with DOJ’s conclusion that the pen register applied to the Internet before the Patriot Act, two events helped precipitate the Patriot Act’s pen register amendments. First, on July 17, 2000, President Clinton’s Chief of Staff John Podesta announced the Clinton Administration’s support for amendments to the pen register statute making clear that the statute applied to the Internet.\textsuperscript{127} Podesta, who earlier had worked on

\textsuperscript{124} See CCIPS Manual, supra note 16, at 102.

\textsuperscript{125} So long as the device did not pick up any “content,” 18 U.S.C. § 2510(8), it did not violate the Wiretap Act.

\textsuperscript{126} See United States v. New York Telephone, 434 U.S. 159 (1977) (holding that in the absence of an explicit law, the government can obtain a search warrant to order the installation of a pen register). A plausible claim could be made that the government could have also used the retrospective authority of 18 U.S.C. § 2703 in combination with the All Writs Act, 28 U.S.C. § 1651, in order to obtain a court order to perform such surveillance with a specific and articulable facts threshold rather than probable cause otherwise required by the New York Telephone case.

\textsuperscript{127} See John Schwartz, U.S. Hopes to Extend Online Wiretapping, WASH. POST at E1 (July 18, 2000). The amendment was only one of several relating to Internet surveillance that the Clinton administration endorsed at that time. See id.
electronic surveillance issues as a staffer to Senator Leahy, argued that it was “time to update and harmonize our existing laws to give all forms of technology the same legislative protections as our telephone conversations.”

Although the Clinton Administration’s proposal did not go far in Congress, it set a precedent for clarifying the scope of the pen register laws.

The second event that helped precipitate the pen register amendments in the Patriot Act was much less public than Podesta’s announcement. On November 17, 2000, Magistrate Judge Patricia Trumbull of the Northern District of California in San Jose denied a government request for an Internet pen register order, and rendered an unpublished written decision holding that the pen register laws did not apply to the Internet. Judge Trumbull reasoned that the language of the pen register statute was sufficiently telephone-specific that it could not be read to apply to the Internet. In particular, she noted that the pen register statute required the court to specify in its order “the number and, if known, the physical location of the telephone line to which the . . . device is to be attached.” Because Internet pen register orders did not specify a telephone line, Judge Trumbull reasoned that “the proposed technology does not fall within the scope of the statute.”

Judge Trumbull’s decision added special urgency to the call for a legislative clarification of the scope of the pen register statute. On one hand, the decision was an unpublished and unpublicized order by a sole Magistrate Judge, in conflict with general practice and the prior written

---

128 Remarks by White House Chief of Staff John Podesta on Electronic Privacy, available at 2000 WL 21168908 (transcript by U.S. Newswire). The Clinton Administration proposals were the product of a 15-agency White House working group chaired by Peter Swire, the Clinton Administration’s Privacy “czar.” See Swire, supra note [].

129 The Administration’s proposal was introduced as S. 3083. Some of its pro-privacy measures appeared in a strongly pro-privacy House bill that passed the House Judiciary committee as H.R. 5018. See Swire, supra note [].

130 See In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register, Trap and Trace Device, or Other Device on an E-Mail Account, Cr-00-6091 (N.D. Cal., November 17, 2000) (Trumbull, M.J.) (unpublished) (on file with author).

131 See id. at 4.

132 See id. (quoting 18 U.S.C. § 3123(b)(1)(C)).

133 See id. at 5 (citing In the Matter of the Application of the United States, 885 F. Supp. 1976, 2000 (C.D. Cal. 1995)).
opinion of another Magistrate Judge in the same circuit. On the other hand, Judge Trumbull was the only Magistrate Judge in San Jose, California. Note the location: the San Jose division of the Northern District of California covers Silicon Valley, and includes the home of such powerhouse Internet service providers as Yahoo! and Hotmail. Even if Judge Trumbull’s decision could be appealed and overturned, the slow pace of litigation meant that it would be many months if not several years before the government could use the statute to authorize envelope surveillance at some of the country’s most popular Internet service providers. Within DOJ, a sense emerged that the best approach was to keep quiet about Judge Trumbull’s decision, which it did: DOJ has never shared Judge Trumbull’s unpublished decision with the public. Instead, DOJ remained committed to pursuing a legislative fix when an opportunity arose that would establish clearly that the pen register laws applied to the Internet.

D. The Patriot Act and the Expansion of the Pen Register Laws

In the wake of the terrorists attacks on New York and Washington on September 11, 2001, pressure built on the Bush Administration to propose anti-terrorism legislation. Just days after the attacks, Attorney General John Ashcroft contacted various divisions within DOJ seeking recommendations for legislative changes that could help fight the war on terrorism. One area that surfaced as a promising arena was Internet surveillance law. DOJ had been clamoring for

---


135 The Justice Department has maintained its silence about Judge Trumbull’s decision to this day. In one recent document, DOJ announced that “[a]lthough numerous courts across the country have applied the pen/trap statue to communications on computer networks, no federal district or appellate court has explicitly ruled on its propriety.” Computer Crime and Intellectual Property Section, Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, available at http://www.cybercrime.gov/PatriotAct.htm. (last visited March 1, 2002). Not the Clintonian phrasing here: because neither of the Magistrate Judge orders were appealed to a District Court Judge or the Ninth Circuit, the statement may be technically true. However, it is certainly misleading. Further, to the extent that a Magistrate Judge decision is generally considered a ruling by a district court, rather than by a separate “Magistrate’s Court”, cf. United States v. Raddatz, 447 U.S. 667 (1980), the statement may be simply false.

changes to the antiquated surveillance laws for years, and the September 11th attacks provided an obvious opportunity. Notably, the link between the surveillance laws and terrorism was not direct: the September 11th attacks did not directly implicate the Internet. However, terrorists groups such as Al-Qaeda were known to favor the latest Internet technologies to communicate with each other, which meant that updating the Internet surveillance laws could assist law enforcement in terrorism-related cases. In any event, the obviously antiquated surveillance laws provided one of the few areas in which new laws were both clearly needed and could conceivably help the Justice Department fight terrorism.

Fortunately for Ashcroft, DOJ had already prepared a comprehensive proposal for updating the Internet surveillance laws. For several years, teams of lawyers within the Justice Department and elsewhere in the executive branch had worked on legislative proposals to update the electronic surveillance laws. Many bills had been introduced in Congress, including ones that previously had Clinton Administration support. By the time September 11th arrived, amendments that had been proposed and debated within the Justice Department for several years were already drafted. In the wake of September 11th, these proposals provided an obvious starting point for amendments to the electronic surveillance laws. Eight days after September 11th, the proposals formed the basis for the electronic surveillance portions of the Justice Department’s proposed Anti-

137 See, e.g., Kevin Maney, Osama’s Messages Could be Hiding in Plain Sight, USA TODAY, December 19, 2001, at B6 (noting Al Qaeda’s use of advanced technologies such as encrypted Internet communications and steganography).

138 For example, within the Computer Crime and Intellectual Property Section of DOJ’s Criminal Division, an informal “High Tech Crime Bill” working group within the Section that tasked itself with writing proposed legislative amendments to the Internet surveillance laws. I was one of the attorneys who participated in the Working Group.

139 See Schwartz, supra note [], at E1.

140 For example, the High Tech Crime Bill working group had spent two years studying, writing, and debating the need for dozens of changes to the surveillance laws. The group had drafted proposed legislative text for the changes, and had also written explanations of the sections that could form the basis for a future House or Senate Committee report on the amendments if the amendments ever became law. The written explanations later emerged as a “Field Guide” to the Patriot Act. It is available at the CCIPS website at http://www.cybercrime.gov/PatriotAct.htm. (last visited March 1, 2002).
Terrorism bill. The DOJ bill in turn provided the basis for the USA Patriot Act passed on October 26.

In light of the Clinton Administration’s failed efforts and Judge Trumbull’s order, amending the pen register statute so that it clearly applied to the Internet provided one obvious priority. The Justice Department’s proposal aimed to do this in a minimalist way. Rather than rewrite the entire statute, DOJ proposed to amend the definition of “pen register and “trap and trace device” to make clear that it applied broadly to network envelope information, encompassing both telephones and the Internet. The DOJ proposed to describe envelope information as “dialing, routing, addressing, or signaling information,”141 and to amend the definitions of pen register and trap and trace device to incorporate this broader definition.142

Congress essentially adopted DOJ’s approach in the Patriot Act, with the slight modification that the phrase “dialing, routing, addressing, or signaling information,” was supplemented with a clarification that “such information shall not include the contents of any communication.”143 This clarification to DOJ’s proposal was added at Senator Leahy’s recommendation to ensure that the expanded pen register amendment did not trump the Wiretap Act.144 The clarification

142 Id.
143 See 18 U.S.C. § 3127 (3), (4). Notably, the minimalist approach of the USA Patriot Act retains the pen register statute’s awkward structure. The statute does not directly prohibit prospective envelope surveillance without a court order. Instead, the statute achieves the same goal in a roundabout way: it prohibits the use or installation of a pen register or trap and trac device without a court order, and then defines a pen register and trap and trace device as a “device or process” that conducts prospective envelope surveillance.

The Administration and the Department of Justice flatly rejected my suggestion that these terms [“dialing, routing, addressing, and signaling”] be defined to respond to concerns that the new terms might encompass matter considered content, which may be captured only upon a showing of probable cause, not the mere relevancy of the
was arguably redundant -- the Wiretap Act already regulated the acquisition of content information separately,\textsuperscript{145} and presumably would have trumped any reading of the new pen register statute that could otherwise include contents\textsuperscript{146} -- but nonetheless reinforced that the pen register laws applied to envelope information but not content information.

E. Why Criticisms of the Pen Register Amendments Are Misplaced

As we saw earlier, the Patriot Act’s modification of the pen register statute to include all “dialing, routing, addressing, or signaling information” proved to be one of the most controversial provisions in the Act. The change was interpreted as a sweeping expansion of law enforcement authority that had not been justified by the Justice Department. Now that we have seen the context of the Patriot Act’s amendment of the pen register laws, can see why these criticisms are surprisingly weak.

First, the criticisms ignore the fact that the pen register statute is primarily a privacy law: it protects envelope information, making it a federal crime to collect envelope information without a court order.\textsuperscript{147} If the pen register statute did not apply to the Internet, then e-mail and packet envelope surveillance would be totally unregulated by federal privacy law. Surely no privacy advocate would have wanted this. In

\textsuperscript{145}Contents “includes any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8).

\textsuperscript{146}18 U.S.C. § 2511 prohibits the interception of “contents,” and does not provide an exception when the contents are intercepted by a pen register or trap and trace device. See 18 U.S.C. § 2511. As a result, a pen register or trap and trace device that collects contents must comply with the Wiretap Act. Cf. Brown v. Waddell, 50 F.3d 285, 294 n.11 (4th Cir. 1995) (noting that whether an electronic device “has the capability to receive by that means coded substantive messages--whether or not it happens to do so during a particular period of interception . . . --is what makes the interception subject to the authorization requirements” of the Wiretap Act.).

\textsuperscript{147}See 18 U.S.C. 3121(d) (“Whoever knowingly violates [the prohibition against installing a pen register or trap and trace device ] shall be fined under this title or imprisoned not more than one year, or both.”)
such a world, the government would be allowed to conduct envelope surveillance of the entire country’s e-mails and Internet communications without a court order, or without even any prior authorization within the Executive Branch. Even more broadly, any private party would be allowed to do the same.

The Patriot Act’s pen register amendments helped avert this situation: the amendments require a court order where before it may not have been necessary. From a civil libertarian standpoint, the problem with the Patriot Act was not that it went too far: the problem was that it didn’t go far enough in protecting the privacy of envelope information. Making it a crime to conduct envelope surveillance on the Internet without a court order was a step in the right direction, but from a civil libertarian viewpoint should have been matched with a higher threshold to obtain the court order that was required. From a policy standpoint, I support such a change; I believe that a higher “specific and articulable facts” threshold would not add substantial burden for law enforcement, and at least on paper it would add privacy protection. However, the fact that this section of the Patriot Act could have offered stronger protection shouldn’t obscure the fact that as a whole the amendment helped add privacy protections, not reduce them.

The second reason that the criticisms missed the mark was that they failed to recognize that the changes codified a decade’s worth of preexisting practice that had matched Internet privacy protections to telephone privacy protections. The Justice Department had been obtaining court orders to conduct envelope surveillance for years, and the new text explicitly recognized and approved the practice. The

---

148 The ACLU has made this argument. See Calvin Galvin, Rights And Wrongs; Why New Law-Enforcement Powers Worry Civil Libertarians, SEATTLE TIMES, December 6, 2001, at A3.


150 I add the caveat “on paper” because in my government experience I never knew or even heard of any law enforcement agent or lawyer obtaining a pen register order when the agent did not also have specific and articulable facts, which would satisfy the higher threshold. My experience is narrow, but it suggests that the practical burden of obtaining the order combined with the certification to a federal judge and potential for criminal liability effectively regulates government officers and deters them from obtaining pen register orders in bad faith. On the other hand, there may be rogue officers out there, if not now then in the future, and a higher threshold could potentially provide an extra barrier to abuse.
legislative change did not expand any authority: at most, the change merely overruled Magistrate Judge Trumbull’s unpublished order.\textsuperscript{151} Although styled a “change” in the law by its critics, the pen register amendments merely reaffirmed the status quo. In itself this provides no reason to celebrate the amendments, of course: it’s possible that the status quo was inadequate. However, the fact that the change reaffirmed longstanding practice would seem to undercut claims that the change dramatically expanded law enforcement powers.

Further, applying the pen register laws to the Internet matched the regulation of the Internet to the regulation of the telephone network, and exceeded the protection that the law provides to similar surveillance of the postal network. After the Patriot Act, envelope surveillance of the telephone and the Internet requires a pen register order, whereas envelope surveillance of postal mail still requires no court order whatsoever.\textsuperscript{152} Although we may believe that the standards for Internet envelope surveillance should be more strict than their analogues in the telephone context\textsuperscript{153} – a question I consider shortly – at the very least the Patriot Act imposes same standard for analogous information in the case of the telephone, and more privacy protection for analogous information in the case of the postal network.

Finally, criticisms of the pen register amendments failed to note that the negotiations over the various bills that led to Patriot Act actually resulted in added privacy protections to the pen register statute that prohibit the disclosure of information obtained through envelope surveillance.\textsuperscript{154} Prior to the Patriot Act, government officials were free

\textsuperscript{151} See In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register, Trap and Trace Device, or Other Device on an E-Mail Account, Cr-00-6091 (N.D. Cal., November 17, 2000) (Trumbull, M.J.) (unpublished) (on file with author).

\textsuperscript{152} Note that despite the public perceptions that we have no privacy our use of new technologies, in fact there is a general trend in privacy law that the more advanced the technology, the more privacy protection the law extends.

\textsuperscript{153} See notes 137 to 154, infra.

\textsuperscript{154} See 18 U.S.C. 2707(g) (2001) (”Any willful disclosure of a 'record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the
to publish or leak information obtained by use of a pen register or trap and trace device.\textsuperscript{155} During the Congressional negotiations, pro-privacy legislators managed to insert language that limits the disclosure of information obtained through prospective envelope surveillance of Internet and telephone communications to disclosures made “in the proper performance of the official functions of the officer or governmental entity making the disclosure.”\textsuperscript{156} Any other disclosure is prohibited.\textsuperscript{157} Although the exact contours of this prohibition remain unclear, the new provision bolsters the privacy protections that the pen register statutes offer to envelope information.

\textbf{F. Does the Internet Deserve Higher Standards? The Weak Case for Internet Particularity}

So the Patriot Act applies the standard for the telephone network to the Internet. But so what? According to the Patriot Act’s critics, Internet envelope surveillance invades far more serious privacy interests than telephone envelope surveillance.\textsuperscript{158} Critics reason that e-mail accounts reveal more private information about their users than telephone accounts, and that Internet envelope surveillance encompasses private activities such as websurfing that deserves higher privacy protection than a mere pen register order.\textsuperscript{159} As a result, they claim, the low threshold for obtaining a telephone pen register order is too low, and should be replaced by a higher threshold such as “specific and

\begin{flushleft}
\textsuperscript{155} In contrast, evidence obtained pursuant to a Title III order cannot be disclosed except in limited situations, see 18 U.S.C. § 2517, and federal law places strict limits on information obtained pursuant to a grand jury subpoena, see Fed. R. Crim. Pro. 6(e).
\end{flushleft}

\begin{flushleft}
\textsuperscript{156} See 18 U.S.C. 2707(g).
\end{flushleft}

\begin{flushleft}
\textsuperscript{157} See id.
\end{flushleft}

\begin{flushleft}
\textsuperscript{158} See, e.g., ACLU Says Congress Should Treat Administration Proposal Carefully; Says Many Provisions Go Far Beyond Anti-Terrorism Needs, available at http://www.aclu.org/news/2001/n092001e.html (last visited January 22, 2002) (“The Administration’s bill would extend this low threshold of proof to Internet communications that are far more revealing than numbers dialed on a phone.”)
\end{flushleft}

\begin{flushleft}
\textsuperscript{159} See Kaplan, \textit{supra} note 108 (quoting Professor Dan Solove for the view that evidence of websurfing is “much more telling about an individual” than the numbers they dialed from a telephone).
\end{flushleft}
I think these criticisms are also misplaced. While I think the standards for both the telephone and the Internet should probably be raised, the argument for raising the Internet standards while maintaining the current standards for the telephone turns out to be surprisingly weak.

Let’s start with the argument that prospective envelope surveillance of an Internet account provides more private information than the same surveillance of a telephone accounts. In most cases, I think this will not be the case: Internet envelope surveillance will usually provide roughly equally sensitive information than postal and telephone envelope surveillance will, and in some key ways, it will provide much less sensitive information.

Consider the envelope information for a telephone call. In particular, imagine that the police are investigating Bugsy and Mugsy, two alleged mobsters. The police have placed a pen register Bugsy’s telephone, and it reveals that at 3:10 pm the telephone located at Bugsy’s home at 123 Main Street was used to place a 12 minute call to Mugsy’s home at 62 Pine Street. This will be very important information for the police. Although the police cannot be sure that the call was placed by Bugsy or received by Mugsy, they do know that there was someone present at Bugsy’s place at 123 Main Street between 3:10 pm and 3:22 pm, and that there was also someone at 62 Pine Street at those times as well. The twelve minute call suggests that the two participants to the phone knew each other, or at least had something substantial to discuss. The pen register yields fairly private information: activity from within the suspects’ homes that tells the police where they were, at what time, and how long they spoke.

If we replace the call with an e-mail, however, the police would tend to know comparatively less, and the invasion of privacy would be less severe. Imagine that a pen register is placed on Bugsy’s e-mail account, bugsy@criminal.com, and that it records the fact that an e-mail was sent at 3:10 pm to the account mugsy@gangster.com. Again, the police cannot be sure that the communication was sent by Bugsy or received by Mugsy: in the case of e-mail as with the telephone, the fact that an account was used does not necessarily mean that any particular

\[160\] See note [], supra.
person used it. More importantly, however, the police will know very little about the whereabouts of Bugsy and Mugsy. They will know that someone (probably Bugsy) sent an e-mail at 3:10 pm to Mugsy’s account. However, they will not know where Bugsy is located at that time, whether Mugsy ever received the e-mail, or where Mugsy is located. And of course this assumes that Mugsy and Bugsy each have known e-mail accounts in the first place, which is generally not true: there is no centralized “e-mail book” that matches the phone book, making it harder for the police to associate suspects with particular addresses. In sum, if the police are trying to find Bugsy and Mugsy, or are trying to pin down and identify their whereabouts and conduct at particular times, the telephone envelope surveillance will tend to yield more private and useful information than e-mail envelope information.

Further, comparing e-mail surveillance to telephone surveillance itself stacks the deck slightly in favor of finding greater privacy interests in the case of Internet surveillance than phone surveillance. The reason is that many pen register orders are executed on packet headers, not e-mail headers. You will recall from Section I that e-mail surveillance has far greater privacy interests at stake than mere packet-level surveillance of the Internet. When the government obtains a pen register order to collect packet headers, the information it yields involves a much lesser privacy interest than in the case of either e-mail or telephone surveillance.

Similar weaknesses counter the criticism that the Patriot Act improperly allows the government to collect Internet search terms and

---

161 See CCIPS Manual, supra note 16, at 90-91 (noting that the fact that an account or address was used does not establish conclusively the identity or location of a particular person who used it.)

162 Further, this hypothetical assumes that Mugsy uses an e-mail address with a username “Mugsy,” and Bugsy has a username “Bugsy.” Criminals who are seeking to evade the detection of the police are not so stupid. Mugsy and Bugsy will be much more likely to have less illuminating usernames such as “Cathy27,” “akjs3242K,” or “62Power.” Further, they will likely register their e-mail accounts using fake names and stolen credit card numbers so the accounts cannot be easily identified with them. Of course, in the telephone context criminals will also take similar measures by using stolen “cloned” cellular phones.

163 For example, the IP header will reveal only that at a particular time, a packet of information such as part of a web page or an e-mail was sent from one computer to another computer. Who was responsible for sending the packet, or where that person might be, or who was the intended recipient, will remain entirely unknown.
lists of websites visited with a mere pen register order.\textsuperscript{164} The difficulty is that whether current law actually allows this turns out to be far from clear, and turns out to have nothing to do with the Patriot Act.

We should begin by recognizing that whether the pen register laws allow the government to collect websurfing data beyond packet headers is largely an academic question. As far as I know, the government has never tried to obtain a pen register order to monitor websurfing in this way.\textsuperscript{165} Because the government has never sought such an order, no court has ever considered whether in fact it would be allowed.\textsuperscript{166} As a matter of legal doctrine, the question is whether the government could monitor websurfing conduct such as search terms entered into search engines and URLs visited without collecting the “contents”\textsuperscript{167} of communications, which would presumably bring websurfing-related information into the default pen register category of “dialing, routing, addressing, or signaling information.”\textsuperscript{168} The government can get a pen register order quite easily, but needs a Title III super warrant to obtain “contents.” The key question is, is such websurfing information “contents”? If so, the government must obtain a super warrant to monitor websurfing in this way.\textsuperscript{169}

\begin{flushleft}
\textsuperscript{164} See, e.g., Kaplan, supra note 108; Jane Black, Uncle Sam Needs Watching, Too, BUSINESS WEEK ONLINE, available at http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011129_3806.htm (last visited January 25, 2002) (“The Patriot Act also expands the “pen register” statute to include e-mail and Internet surfing.”).
\textsuperscript{165} In an informal survey of experienced federal prosecutors, I was unable to find any who had had heard of such an application. Prospective surveillance of websurfing turns out to be of fairly limited help to a criminal investigation. At the same time, such surveillance is possible: for example, the FBI’s DCS-1000 surveillance tool has a setting that allows the tool to collect websurfing information.
\textsuperscript{166} Unless the government seeks a court order, no case and controversy exists and no court has the opportunity to resolve the question.
\textsuperscript{167} 18 U.S.C. § 2510(8) (“‘contents’, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.”)
\textsuperscript{168} 18 U.S.C. § 3127. This raises an interesting question not clearly answered by the Patriot Act. Is all non-content information “dialing, routing, addressing, and signaling” information, so that all prospective information triggers either the Pen Register statute and/or Title III? Or is there a third category outside of “contents” and “dialing, routing, addressing, and signaling” information?
\textsuperscript{169} See Brown v. Waddell, 50 F.3d 285, 294 n.11 (4th Cir. 1995). One subtlety to this question is that we must go beyond the abstract question of whether the pen register allows the government to monitor websurfing to the more specific question of
The conceptual difficulty is that the legal categories of “contents” and “addressing information” are straightforward in the case of human-to-human communications, but quite murky when we consider human-to-computer communications. In the case of human-to-human communications, the “contents” are any message or communication that the human sender intends to communicate to the human recipient. This covers the subject line and the body of e-mails, as well as the substance of the call in a telephone call. In these cases, the “contents” are the messages that the sender wants to send to the recipient.

How does this apply when the message is destined for a computer instead of a person? This is a profoundly important question, but not one that Congress or the courts have fully answered. When an Internet user surfs the web, he sends commands to his computer directing it to send commands to the host computer, asking it the host to send back packets of data that will be assembled by his computer into a web page. We can look at the user’s command in two ways: either the command is the “content” of the communication between the user and his computer, or it is merely “addressing information” that the user has entered into his computer to tell the computer where it should go and what it should do, much like the pen register information in Smith v. Maryland.

The same problem arises in a slightly different context when we

---

170 See id. Notably, the definition of “wire communication” that Congress enacted in the original 1968 Act explicitly requires that the communication contain “the human voice.” See 18 U.S.C. § 2510(18).


172 See Gralla, supra note 26, at 139-40.

173 This is a difficulty latent in Smith v. Maryland that has not yet fully been appreciated. In Smith, the Court analogized dialing a phone number to contacting an operator and asking the operator to connect the call. See Smith, 442 U.S. at 744-45. Because disclosing the number to an operator would eliminate the speaker’s reasonable expectation of privacy in the information, so did disclosing the information to the phone company’s computer. See id. So far, so good. The difficulty is that if a speaker calls the operator and places that request, then that request constitutes the contents of the communication between the speaker and the operator. The contents of the conversation between the speaker and the operator becomes the addressing information for the ensuing conversation between the speaker and the person he wishes to call. As a result, it is difficult in the abstract to say whether that initial communication should be considered addressing information or contents.
ask what legal order is required to monitor a computer hacker’s commands sent to a remote server. We can ask: are these commands “contents” of the communications between the hacker and the computer, “addressing” information telling the computer what to do, or something else? No court has yet considered such questions squarely,\textsuperscript{174} which means that the legal distinction between “contents” and “addressing information” remains murky for human-to-computer communications.

For our purposes, the key point is that these ambiguities predate the Patriot Act. The essential question asks how the Wiretap Act’s definition of “contents” applies to human-to-computer and computer-to-computer communications.\textsuperscript{175} This definition has remained unchanged since 1986, before the World Wide Web was even invented,\textsuperscript{176} and was not changed in any way by the Patriot Act.\textsuperscript{177} As a result, the Patriot

\textsuperscript{174} See United States Telecom Ass’n v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000) (noting that “[n]o court has yet considered” whether digital signals entered by a user to a computer over a telephone line are contents, and stating that “it may be that a Title III warrant is required . . . .”) The D.C. Circuit did suggest that human-to-computer communications can in fact be “contents” according to Title III, at least in the context of the telephone network. In discussing whether the government can intercept dialed digits entered after a call has been completed (known as “post-cut-through dialed digits”), the court offered the following analysis:

Post-cut-through dialed digits can also represent call content. For example, subjects calling automated banking services enter account numbers. When calling voicemail systems, they enter passwords. When calling pagers, they dial digits that convey actual messages. And when calling pharmacies to renew prescriptions, they enter prescription numbers.\textsuperscript{Id. at 462.}

\textsuperscript{175} See 18 U.S.C. § 2510(8).

\textsuperscript{176} See DAVE RAGGET, ET. AL., RAGGET ON HTML 4 at 18 (1997) (crediting the invention of the Web to Tim Berners-Lee in 1989).

\textsuperscript{177} In its original form in 1968, Congress defined contents by stating that it “includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8) (1968). At the time Congress noted that “[t]he definition thus include(s) all aspects of the communication itself. No aspect, including the identity of the parties, the substance of the communication between them, or the fact of the communication itself, is excluded. The privacy of the communication to be protected is intended to be comprehensive.” S.Rep.No.1097, supra, at 91; U.S. Code Cong. & Admin. News, p. 2179.

In 1986, however, Congress enacted the pen register statute and amended the definition of “contents” to exclude the identity of the parties to such communication. See S. Rep. 99-541 reprinted at 1986 U.S.C.C.A.N. 3555, 3567. According to the Senate
Act could not have changed whether the government needs a Wiretap Order to monitor websurfing. Perhaps it does, perhaps it does not. However, the Patriot Act did not change the answer. We can criticize the Patriot Act for failing to clarify how the law treats surveillance of websurfing activities, of course. The statutory text leaves many questions open, leaving the Justice Department, commentators, and the courts with relatively little guidance.\textsuperscript{178} More broadly, Congress has not yet made a careful determination of how the electronic surveillance statutes (and especially the Wiretap Act) apply to human-to-computer communications, and the Patriot Act was a missed opportunity.\textsuperscript{179} This is a valid criticism, but seems far from the charges levied by the Patriot Act’s critics. Perhaps the problem with the Patriot Act is not that it changed too much, but that it answered too little.

\textsuperscript{178} In a press release issued on October 11, 2001, Senator Leahy blamed the Bush Administration and the Justice Department for refusing to define the terms “dialing, routing, addressing, and signaling” information. According to Leahy, “[t]he Administration and the Department of Justice flatly rejected my suggestion that these terms be defined,” with the unfortunate result that Congress was “leaving the courts with little or no guidance of what is covered by “addressing” or “rout[ing],”” \textit{Statement of Senator Patrick Leahy on The Uniting and Strengthening of America Act (“USA ACT”), October 11, 2001}, available at http://leahy.senate.gov/press/200110/101101a.html.

\textsuperscript{179} Notably, several members of the House and Senate and their staff were quite aware of the ambiguities over the scope of the new pen register laws, and in particular how they applied to websurfing. For example, the House Report on H. 2975 contain a statement that post-Patriot Act pen register orders could not be obtained “to collect information other than ‘dialing, routing, addressing, and signaling’ information, such as the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article.” \textit{See H.R. Rep. No. 107-236 (2001), at [].} The proper weight to be afforded to this statement is unclear. The phrase “dialing, routing, addressing, and signaling” information derived from the original DOJ proposal and was shared by both the House and Senate versions of the bill. Because the House proved more resistant to the DOJ’s proposal than the Senate, this statement may reflect an effort by the authors of the House Report to “spin” later judicial interpretations of DOJ’s language. \textit{Cf. ANTONIN SCALIA, A MATTER OF INTERPRETATION} 34 (1997) (noting that Committee Reports are often written with the “primary purpose” of affecting later judicial constructions of the statutory text). Further, the critical question is less the scope of “dialing, routing, addressing, and signaling” information than the meaning of “contents,” which the Patriot Act did not change.
III. THE PATRIOT ACT AND THE FBI’S “CARNIVORE” SURVEILLANCE TOOL

A second major criticism levied at the Patriot Act is that it explicitly sanctioned and even encouraged the use of Carnivore, the FBI’s controversial Internet surveillance tool.\textsuperscript{180} Although the Patriot Act does not explicitly mention Carnivore, the press frequently reported that the Patriot Act provided for its expanded use.\textsuperscript{181} According to The New York Times, the use of Carnivore was in fact “at the heart of the debate” over the Patriot Act.\textsuperscript{182} This was troubling, the Times reported, because Carnivore acts as a powerful tool that poses significant dangers to civil liberties: it “give[s] government more power than ever before to encroach on the privacy of citizens.”\textsuperscript{183} “When Carnivore sits down to eat, it tastes everything.”\textsuperscript{184} By expanding the use of Carnivore, the Patriot Act created a significant danger to civil liberties.

In this section, I will argue that this criticism of the Patriot Act is exactly backwards. The only provisions of the Patriot Act that directly address Carnivore are pro-privacy provisions that actually restrict the use of Carnivore. Further, Carnivore itself stands out from other similar

\textsuperscript{180} See, e.g., Guernsey, supra note 77 (stating that an earlier bill “implies the wider use of Carnivore”); John Schwartz, Privacy Debate Focuses on F.B.I. Use of an Internet Wiretap, N.Y. TIMES, Oct. 13, 2001, at A14; Stephanie Olson, Patriot Act Draws Privacy Concerns, C.NET NEWS, available at news.com.com/2100-1023-275026.html (October 26, 2001) (“Part of the new legislation includes the expansion of Internet eavesdropping technology once known as Carnivore.”); Michael Connor, Brave New Web, Boston Phoenix, March 11, 2002 available at www.bostonphoenix.com/boston/news_features/ other_stories/documents/02105031.htm (“Another controversial provision of the USA PATRIOT Act allows increased use of Carnivore, a wire-tapping program for the Internet.”); Anne Kandra, The New Anti-Terrorism Law Steps Up Electronic Surveillance of the Internet, PC WORLD, January 2002 (“The new law opens the door for increased use of Carnivore”); Sonia Arrison, New Anti-Terrorism Law Goes Too Far, SAN DIEGO UNION TRIBUNE, Oct. 31, 2001, (“The law also expands Internet surveillance by making Carnivore, the controversial e-mail wiretapping system official even though there is a real danger that it over-collects information.”).

\textsuperscript{181} See id.

\textsuperscript{182} Schwartz, supra note 155, at A14.

\textsuperscript{183} Id.

\textsuperscript{184} Id.
tools that ISPs use every day only in the sense that it was specifically designed to protect privacy and preserve government accountability more than other tools. Oddly enough, the public debate over Carnivore has the issue backwards. While the press has pounced on Carnivore as Public Enemy #1, in truth the tool is designed to implement a pro-privacy technology that both law enforcement and civil libertarians should appreciate.

This section begins by explaining how prospective Internet surveillance works, and how the FBI’s Carnivore tool was designed to be a privacy-protecting means of conducting it. The analysis argues that Carnivore is an perplexing target for criticism by the civil liberties community. The section then turns to the impact of the USA Patriot Act on the use of Carnivore, and shows how the Patriot Act actually adds restrictions to the use of Carnivore, rather than takes them away.

A. Understanding the Technology of Prospective Internet Surveillance: Packet Sniffers

As explained in Section I of this article, the Internet is a packet-switched network. All Internet communications are broken down into discrete packets and sent over the network, and are then reassembled into the original communications when they reach their final destination.185 As a result, a great deal of prospective Internet surveillance is packet surveillance.186 To conduct prospective surveillance, a tool must “tap” a particular line of Internet traffic at a particular physical location to look for the communication sought. Tapping the line allows that person to view the packet traffic flowing through that particular point in the network. Any device or software programmed to do this is on the Internet is generally known as a “packet sniffer,”187 for the way that it “sniffs” Internet packets flowing through the particular point in the network.

One implication of this technology is that Internet packet surveillance must always involve examining all of the packet traffic

---

185 See GRALLA, supra note 26, at 13.
186 The remainder is non-packet surveillance that occurs immediately before the information has been packetized, or else immediately after it has been arrived and depacketized.
streaming by a particular point on the network. The tool must look at all of the traffic passing through the particular point in the network to see if it is the communication sought, much like a police officer walking through a public place looking for a known criminal suspect must look at every person just to see whether they are in fact the suspect.  

For example, if the FBI obtains a court order allowing it to collect envelope information at the packet level (such as IP headers for traffic originating from a specific IP address), it must scan all of the traffic flowing over the network to locate, isolate, and collect the IP headers.

While this may sound like a gross invasion of privacy, it is less so in practice than in theory. While the Internet uses packets to send and receive information, the packets are really just digital ones and zeroes that computers use to communicate with each other. The ones and zeroes can be reassembled into text to be read by a human, but computers do not need to do this and generally will not. This means that a computer surveillance tool programmed to look for all e-mails to the Internet account “bob@aol.com” does not actually look for the text “bob@aol.com.” To simplify a bit, the tool instead starts off by looking for e-mails, and when it finds an e-mail scans the right place in the e-mail for the digital equivalent of “bob@aol.com,” which is 

\[
0110001001101111011000010010000001100111011011101101110110011101100110110 111101101101.
\]

If this exact sequence of ones and zeros appears in the packet, the tool will know that an e-mail has arrived from bob@aol.com. This is not quite as invasive as it sounds, because computers operate by executing instructions composed of binary digits of “zeros” and “ones.”

---

188 See Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) (“In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. Similar dangers, of course, are present in executing a warrant for the "seizure" of telephone conversations. In both kinds of searches, responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.”)


190 E-mails are identifiable because a section of the packet header contains an identifying number that lets the server know that the packet should be sent to the mail server. To be technical, e-mails are carried on port 25, which means that the sniffer can just look for communications sent to port 25. See [[ ]].

191 I am using the standard ASCII format. ASCII is short for “American
the right place, the surveillance tool ‘knows’ that it has found an e-mail to bob@aol.com and will copy and record the entire block of ones and zeros that represent the e-mail so that someone can later come back, convert the ones and zeros into text, and read the e-mail. The billions of ones and zeros that do not relate to e-mails to the exact sequence of 0s and 1s that represent the target account will pass through the device and be forgotten. 192 The tool cannot think, cannot snoop around, and cannot understand what passes before it: it can only look for the exact sequence of ones and zeros it has been programmed to identify.

These technical details have profound implications for how Internet surveillance can best respect privacy interests. Most remarkably, the Internet reverses the normal associations we have about the relationship between technology and privacy. In the physical world, advanced technology provides a powerful way to invade privacy. 193 A single police officer can search a single room on a house, but cannot search an entire neighborhood, or a large city. To search an entire city, advanced technology would be required. At an intuitive level, we understand that a bigger and more invasive search requires a more powerful tool. 194

In the case of Internet surveillance, in contrast, the default is the most invasive search possible, and we need advanced technology to minimize the invasion of privacy. For example, a system administrator (or a 12-year old computer hacker) can monitor every single iota of information flowing through a particular point in a network by writing a simple program. The program simply instructs the computer to record all of the traffic flowing through that computer: it creates a packet sniffer and sets it to sniff all of the traffic. The system administrator (or hacker)

---

192 Once data is pushed out of the random access memory, it cannot be recovered. See Sherry Kinkoph, et. al., Computers: A Visual Encyclopedia 286-87 (1994)

193 See Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) (“Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.”)

194 Upon hearing that the government has spent substantial resources to develop a new surveillance tool, most people are likely to assume that the FBI was working on a tool to invade privacy, not to protect it.
can later convert the recorded digits into text and look through the entire world of traffic that flowed over the network. The real technological challenge is devising a tool that acts as an effective filter: the tool should isolate and record only the exact packets that a court order allows, rather than collect everything and require subsequent review by a human being. In contrast to the physical world, total surveillance of traffic through a point on the Internet is easy: narrow and limited surveillance requires advanced filtering.

B. The FBI and the Introduction of “Carnivore”

In the mid-to-late 1990s, the FBI recognized these difficulties and began designing surveillance tools that could filter and analyze Internet communications effectively. The core difficulty was that the private sector had not yet developed such a tool because the market had not demanded it: system administrators regularly used a host of available packet analyzer programs, but given the fairly broad provider rights to intercept communications inside their network, none incorporated the privacy protections that the FBI desired. In particular, commercially available programs generally did not allow the user to run a very narrow search that a court order might require, and none included auditing features that would be useful in court if a defendant challenged the fruits of surveillance.

We can see these deficiencies in the most popular off-the-shelf packet analyzer program for system administrators, a product known as “EtherPeek” that sells for about $1,000. The versions of EtherPeek

---

195 See Donald M. Kerr, Carnivore Diagnostic Tool, Testimony Before the Senate Judiciary Committee (September 6, 2000) available at http://www.fbi.gov/congress/congress00/kerr090600.htm (“Carnivore -- far better than any commercially-available sniffer -- is configurable so as to filter with precision certain electronic computer traffic (i.e., the binary computer code, the fast-flowing streams of 0's and 1's) . . . . to our knowledge, there are few, if any, electronic surveillance tools that perform like Carnivore, in terms of its being able to be tailored to comply with different court orders, owing to its ability to filter with precision computer code traffic.”)


197 EtherPeek is Wildpackets, Inc. software program. See http://www.wildpackets.com/products/etherpeek. According to Wildpackets’ promotional material, EtherPeek “is an award-winning Ethernet network traffic and protocol analyzer designed to make the complex tasks of troubleshooting and debugging mixed-platform, multi-protocol networks easy.” Id. See also James Sanders, Sniff Out
available in the late 1990s did not allow system administrators to limit searches by ordering the sniffer to exclude results that contained specific key words.\textsuperscript{198} The tool could search for e-mails to bob@aol.com, for example, but could not filter out e-mails to bob@aol.com that also included the word “personal.” Instead, the tool required the collection of \textit{all} e-mails to bob@aol.com, even if personal e-mails were beyond the scope of a court order. While this extra invasion of privacy might not matter to a business, to a law enforcement agent it raises the prospect that the tool might illegally collect information beyond the scope of a court order. To ensure that the FBI would have a tool that complied exactly with the terms of a court order, the FBI decided it needed to develop its own surveillance tools tailored specifically to the limits of the surveillance laws.\textsuperscript{199}

The FBI was relatively slow in developing such a tool because law enforcement agencies like the FBI rarely use its own surveillance tools when implementing court orders. In the overwhelming majority of the cases, the FBI simply hands the court order to the Internet service provider, which implements the order itself using its own tools.\textsuperscript{200} Although the ISP’s surveillance tools might collect more information than they should have, the ISP can manually filter the results down to just the information named in the court order before handing over the data to the FBI.\textsuperscript{201}

From a law enforcement perspective, this scheme of indirect surveillance is vastly preferable to direct surveillance, although it cannot be an exclusive arrangement. The advantage of indirect surveillance is primarily economic: it costs less and requires fewer technical resources to have ISPs implement court orders for the government rather than

\textit{Trouble, PC Magazine}, May 22, 2001 (offering a product review of EtherPeek).
\textsuperscript{199} \textit{See Kevin DiGregory, Concerning The “Carnivore” Controversy: Electronic Surveillance And Privacy In The Digital Age,} Testimony Before the Senate Judiciary Committee (September 6, 2000) available at http://www.cybercrime.gov/kvd_0906b.htm (last visited November 21, 2001).
\textsuperscript{200} \textit{See id.}
have the government conduct the surveillance itself. At times, however, ISPs lack the expertise or the willingness to implement court orders on law enforcement’s behalf. Trust of the ISP is also an issue. Indirect surveillance requires the government to trust that the ISP is implementing the court order effectively and turning over all of the evidence obtained to government investigators. While this may be true with regards to major ISPs like AOL and Earthlink, smaller ISPs may be uninterested in helping the Feds, may have other more pressing problems, or may even be in cahoots with the criminal suspects. This means that the government cannot rely exclusively on indirect surveillance to implement its court orders. If all else fails, it must have a surveillance tool that allows it to implement court orders directly.

The FBI dubbed the fruit of its efforts “Carnivore.” Ironically, the menacing name was originally intended to reflect how privacy protecting the tool was designed to be. The first–generation tool the FBI developed before Carnivore employed a fairly primitive filter that at times could collect more information than a court order allowed. As a

202 Although no official figures are available on this point, common sense suggests that an ISP that is familiar with its network and already has a sysadmin employed to oversee it can more easily and cheaply implement a court order to conduct surveillance of its network than the FBI. For the FBI to implement the order, it must learn about the network from the ISP, and send technical specialists out to the site in order to implement the surveillance tool.

203 I worked or consulted on several investigations as a lawyer in which agents feared that the provider at issue was either sympathetic to or co-conspirators with the suspects under investigation. This is a particular problem with small “mom and pop” ISPs that may serve a specialty audience.

204 In a sense, this capability is the Internet equivalent of what the telephone system guarantees by way of the Communications Assistance to Law Enforcement Act of 1994 (“CALEA”). See 47 U.S.C. §§ 1001 et seq.


206 See John Schwartz, Tapping Into Gray Areas, New Internet Surveillance Technology Raises As Many Questions As It Answers, HOUSTON CHRON., February 16, 2001, at 1 (noting that Carnivore “was derived from an earlier system, called Omnivore, that captured most of the Internet traffic coursing through a network. ‘As the tool developed and became more discerning’ - able to get at the meat of an investigation – ‘it was named Carnivore,’ an official said.”). See also IIT Research Institute, Independent Technical Review of the Carnivore System, Final Report at 4-2 (December 8, 2000) (hereinafter IITRI Final Report), available at http://www.epic.org/privacy/
result, it could collect snippets of other communications beyond the scope of the court order.\textsuperscript{207} This tool “ate” more than it was supposed to, and so the FBI dubbed it “Omnivore.”\textsuperscript{208} In contrast to Omnivore, the second-generation tool had an advanced filter that could precisely locate and record the exact information sought. The FBI called the second-generation tool “Carnivore,” the device \textit{only} devoured the “meat” that the tool was programmed to record.\textsuperscript{209}

Carnivore – and its progeny, such as the third-generation tool given the more innocuous label “DCS-1000”\textsuperscript{210} – was therefore designed by the FBI as a tool that could ensure compliance with court orders while minimizing the invasion of privacy. In fact, the tool’s user interface was designed with the law specifically in mind: the Carnivore software (which runs on a home PC or a laptop\textsuperscript{211}) prompts the user to enter in the exact type of traffic that the court order specifies: pen/trap vs. full content, e-mail envelope vs. packet envelope, etc.\textsuperscript{212} The program then executes the court order as instructed. Assuming the tool performs as it is designed to perform (which is always a question with any surveillance tool\textsuperscript{213}), it should be the most privacy-protecting Internet surveillance tool created. In fact, Carnivore is essentially just an everyday Internet tool with a few extra features designed to ensure compliance with court orders: as Peter Swire has pointed out, it could accurately be called the “Internet court order compliance tool.”\textsuperscript{214}

Unfortunately, both commentators and the press have portrayed Carnivore as a frightening and mysterious beast that invades privacy

carnivore/carniv_final.pdf (noting that Carnivore does not over-collect, in contrast to generically available sniffer software).

\textsuperscript{207} See IITRI Final report, supra note [], at 4-2.

\textsuperscript{208} See id.

\textsuperscript{209} See John Schwartz, \textit{Tapping Into Gray Areas, New Internet Surveillance Technology Raises As Many Questions As It Answers}, \textit{Houston Chron.}, February 16, 2001, at 1 (noting that Carnivore “was derived from an earlier system, called Omnivore, that captured most of the Internet traffic coursing through a network. ‘As the tool developed and became more discerning’ - able to get at the meat of an investigation – ‘it was named Carnivore,’ an official said.”).

\textsuperscript{210} See McCarthy, supra note 64, at 828 n.5.

\textsuperscript{211} See IITRI Final Report, supra note [], at 5

\textsuperscript{212} See id. at Ch.4.

\textsuperscript{213} See infra notes 191 to 195 and associated text.

willy-nilly.\textsuperscript{215} The menacing name itself probably accounts for much of this criticism, and a misunderstanding of how the Internet inverts the traditional relationship between privacy and technology accounts for much of the rest.\textsuperscript{216} The fact that tool is installed at the ISP in the form of a sealed black box hasn’t helped the FBI, either.\textsuperscript{217} While Carnivore’s critics have seen this as proof of the tool’s dangers,\textsuperscript{218} instead it reflects privacy and legal constraints. Installing the tool at the ISP minimizes the amount Internet traffic that needs to be scanned,\textsuperscript{219} minimizing the invasion of privacy, and sealing the computer so the ISP cannot interfere with it preserves the chain of custody for evidentiary purposes.\textsuperscript{220}

\footnotesize
\begin{itemize}
  \item \textsuperscript{215} See, e.g., Schwartz, supra note 155, at A14 (“When Carnivore sits down to eat, it tastes everything”). An amusing example of this hysteria can be found at the Internet website www.stopcarnivore.org (last visited January 10, 2002).
  \item \textsuperscript{216} That is, the public naturally assumes that if the FBI has invested in a program to develop an Internet surveillance tool, it must be to designed a tool that has new powers to invade privacy, not new powers to protect privacy.
  \item \textsuperscript{217} Press Release, ACLU, \textit{In Unique Tactic, ACLU Seeks FBI Computer Code On “Carnivore” and Other Cybersnoop Programs} (July 14, 2000) (hereinafter Press Release, Unique Tactic), available at http://www.aclu.org/news/2000/n071400a.html. The ACLU jumped on this with the following response: ’’‘Right now, the FBI is running this software out of a black box,’ said Barry Steinhardt, Associate Director of the ACLU . . . ‘The FBI is saying, ‘trust us, we’re not violating anybody’s privacy.’ With all due respect, we’d like to determine that for ourselves.’’” \textit{Id}.
  \item \textsuperscript{218} See \textit{id}.
  \item \textsuperscript{219} This is true for any kind of prospective Internet surveillance. Because tapping the line requires scanning the traffic passing through the line to identify the particular items sought in the court order, the best way to minimize the invasion of privacy is to install the tap where the amount of traffic unrelated to the court order is at an absolute minimum. When monitoring an Internet account, this will generally mean the ISP that hosts the account. Installing the monitoring device elsewhere would increase the amount of unrelated traffic scanned.
  \item \textsuperscript{220} Imagine that you are a prosecutor attempting to persuade a jury that records collected by a packet sniffer installed by the FBI link the defendant to a crime. If the employees of the ISP had access to the sniffer, your job could become quite difficult. Any good defense attorney will try to raise reasonable doubt based on the untrustworthiness of records that were created by the FBI’s sniffer but open to falsification by anyone present at the ISP. If employees could access the sniffer, they could modify the sniffer, reconfigure the settings, falsify data, and tamper with the evidence.. \textit{Cf.} United States v. Whitaker, 127 F.3d 595, 602 &7th Cir. 1997) (noting that defense attorney’s argument that computer records were unreliable because “with a few keystrokes” they could be modified or deleted was a question for the jury). In contrast, if the device is sealed and cannot be accessed by the ISP, this minimizes one source of possible tampering.
\end{itemize}
C. The Effect of the USA Patriot Act on Carnivore

Let’s now return to the criticism that the USA Patriot Act encourages the use of Carnivore. As the analysis above indicates, this seems an odd point to criticize: Carnivore is generally more privacy-enhancing than other less sophisticated packet sniffers in everyday use at ISPs. But even on its face, the criticism rings hollow.

The view that the Patriot Act furthers the use of Carnivore is based largely on a faulty logical premise. The premise is that because Carnivore provides a means of conducting Internet surveillance, a law that appears to further the government’s ability to conduct the use of Internet surveillance must also further the use of Carnivore. The problem is that Carnivore is merely one particular tool among many that could be used to conduct electronic surveillance, and there is no reason to think that the Patriot Act encourages the use of Carnivore as compared to any other tool (in fact, as we shall see shortly the opposite is true).

As a result, saying that the Patriot Act encourages the use of Carnivore is something like saying that a new highway bill furthers the use of Volvos. Yes, some cars on the road are Volvos. Yes, a new law that helps the highway system may eventually encourage more driving, some of which presumably will be done at the wheel of Volvos. But the connection between the highway bill and a particular of car is a tenuous one: there are hundreds of different cars that can be driven, and there is no reason to think that a highway bill would encourage the use of Volvos more than any other car. Tying the Patriot Act to the increased use of Carnivore rests on similarly weak logic.

In part, the problem is that the Carnivore debate has been focused on the wrong question. The critical question is not what particular tool is used to conduct surveillance, but instead what the law authorizes the government to do, and whether the government stays within the scope of that authority. Again, a comparison to an automobile proves helpful. It is crime to drive a car at 100 miles per hour, or to

---

221 See www.toyota.com (last visited January 19, 2002).
drive a car while drunk, 223 or to possess a stolen car. 224 However, whether the car happens to be a Ford or a Chevrolet is entirely irrelevant. What matters is not the model of the car, but what the driver does with the car, and whether that is legal or illegal.

Viewed in this light, the Carnivore debate seems a red herring. Whether the government uses Carnivore or some other tool to conduct prospective surveillance, the legal questions remain the same. Unless an exception to the statute applies, the government must obtain a pen register order to obtain “dialing, routing, addressing, and signaling information,” and must obtain a Wiretap Order to obtain “contents.” This was true before the Patriot Act (although the first part was uncertain), and it is true after the Patriot Act. If the government does not obtain the right court orders, it violates the statute regardless of whether it has used Carnivore or Fluffy Bunny. 225

D. The Patriot Act and New Rules for Direct vs. Indirect Surveillance of Packet Switched Networks

Notably, the Patriot Act does include one amendment that is Carnivore-specific. However, this amendment is actually a pro-privacy law, designed to monitor Carnivore by imposing a reporting requirement on direct prospective surveillance of the Internet by law enforcement. 226 The reporting requirement has been codified at 18 U.S.C. § 3123(a)(3), and states:

(A) Where the law enforcement agency implementing an ex parte order under [the Pen Register Statute] seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify—

(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain

223 See, e.g., Va. Code Ann. § 18.2-266 (“It shall be unlawful for any person to drive or operate any motor vehicle . . . while such person is under the influence of alcohol.”).


225 Currently, there is no Internet surveillance tool called Fluffy Bunny. However, the FBI may want to try using the name.

information from the network;
(ii) the date and time the device was installed, the date and
time the device was uninstalled, and the date, time, and
duration of each time the device is accessed to obtain
information;
(iii) the configuration of the device at the time of its
installation and any subsequent modification thereof;  and
(iv) any information which has been collected by the
device.

To the extent that the pen register or trap and trace device can
be set automatically to record this information electronically,
the record shall be maintained electronically throughout the
installation and use of such device.
(B) The record maintained under subparagraph (A) shall be
provided ex parte and under seal to the court which entered the
ex parte order authorizing the installation and use of the device
within 30 days after termination of the order (including any
extensions thereof).227

Although this statutory text does not mention Carnivore or
DCS-1000 by name, it was clearly designed to regulate it: the primary
law enforcement tool for conduct direct prospective surveillance is
Carnivore and the third-generation DCS-1000, and the “packet-
switched data network” is of course a network connected to the
Internet. This text requires the government to follow a strict reporting
regime whenever it conducts direct (as opposed to indirect) prospective
envelope surveillance of the Internet and installs its own device at an
Internet service provider that provides service to the public.229

The section was added to the Patriot Act at the insistence of House Majority
Leader Dick Armey in an effort to increase the judicial review of the use
of Carnivore as a way of implementing pen register orders.230

The Patriot Act’s new provision regulating direct surveillance
more heavily than indirect surveillance reflects a significant shift from the
traditional approach found in United States surveillance and search and

228 See id.
229 The requirement that the service be available “to the public” is explained in
230 See Editorial, Proceed With Caution, DENVER POST, October 26, 2001 at Page
B6 (“There are some safeguards, such as . . . a requirement, added at the last minute by
House Majority Leader Dick Armey, R-Texas, that a judge monitor the FBI’s use of the
controversial Carnivore e-mail surveillance system.”).
seizure law. Federal privacy laws have traditionally preferred that law enforcement implement court orders itself, and have signaled significant skepticism at the prospect of allowing private parties to implement court orders on the government’s behalf.\textsuperscript{231} For most of the last century, having the police implement their own court orders with their own tools has been the norm, and allowing the private provider to do so has been the exception.

For example, federal law governing the execution of search warrants in actually \textit{prohibits} having private parties execute search warrants on behalf of law enforcement.\textsuperscript{232} Similarly, when the Wiretap Act first allowed the FBI to conduct prospective surveillance of the telephone network in 1968, it effectively required the FBI to conduct direct surveillance. While the telephone company could volunteer to help the government, providers could not be compelled to execute the court order on the government’s behalf.\textsuperscript{233} Congress later amended the statute in 1970 to allow the courts to compel providers to help the government, but offered the government the choice: it could either implement the order itself, or it could order the provider to implement the order on its own and to send the results to law enforcement.\textsuperscript{234} This is the standard that Congress has consistently enacted in surveillance laws since 1970: Congress has offered law enforcement the choice of how it wants to implement surveillance orders, without placing a thumb on the scale in favor either direct or indirect surveillance.\textsuperscript{235}

The reporting requirement for Carnivore added by the Patriot

\textsuperscript{231} \textit{See infra} notes 202 to 207 and associated text.

\textsuperscript{232} \textit{See} 18 U.S.C. § 3105 (“A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution.”)

\textsuperscript{233} \textit{See} In re Application of the United States, 427 F.2d 639, 644(9th Cir. 1970) (“If the Government must have the right to compel regulated communications carriers or others to provide such assistance, it should address its plea to Congress.”).

\textsuperscript{234} \textit{See} 18 U.S.C. § 2518(4) (“An order authorizing the interception . . . shall, upon the request of the applicant, direct that a provider of wire or electronic communication service . . . shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception. . . .”) (emphasis added).

\textsuperscript{235} Notably, however, the postal service regulation governing mail covers is an indirect regulation: it allows the Postal Service to implement a mail cover, but no others. \textit{See} 39 C.F.R. § 233.3. Of course, this is easier to do in the case of the postal mail given that the government Postal Service enjoys a monopoly over postal mail.
Act appears to be the first statutory privacy law to regulate direct surveillance more heavily than indirect surveillance. The irony is clear. Not only is Carnivore probably more privacy-enhancing than other surveillance tools, but the Patriot Act actually introduced measures to monitor and restrict its use.\textsuperscript{236}

III. THE COMPUTER TRESPASSER EXCEPTION TO THE WIRETAP ACT

A third major criticism of the USA Patriot Act has centered around a new exception to the Wiretap Act, the computer trespasser exception.\textsuperscript{237} The computer trespasser exception concerns prospective content surveillance: it allows law enforcement to intercept the contents of Internet communications sent by a “computer trespasser” without a warrant from the computer of a consenting victim of the trespasser.\textsuperscript{238}

The computer trespasser exception proved so controversial that Congress enacted it only pursuant to the sunset provision: the exception will cease to exist on December 31, 2005, unless Congress chooses to reauthorize it.\textsuperscript{239} According to its critics, the sunset was necessary because the computer trespasser exception poses significant dangers to privacy. In particular, the broad language of the exception would allow the government to monitor all of an Internet user’s communications whenever the user violated minor rules like their ISP’s terms of

\textsuperscript{236} An even greater irony is that technological advances in commercial packet sniffers may have significantly decreased the need for the FBI’s own surveillance tool. In the last two years, for example, new versions of the commercial EtherPeek software have been introduced that significantly enhanced the tool’s filtering capability. \textit{See WildPackets Releases EtherPeek™ v4.2: New Version of Industry’s Leading Packet Analyzer Provides Multiple Filtering and Decoding Upgrades} (August 2, 2001), available at http://www.wildpackets.com/corporate/news/01-08-02 (noting the introduction of advanced filtering capabilities in Version 4.2 of EtherPeek, including “’Accept Matching’ and ‘Reject Matching’ Filter Modes.”). If EtherPeek allows system administrators to implement surveillance orders quickly and effectively, Carnivore and its progeny will be needed less and less often.

\textsuperscript{237} See, e.g., Rosen, \textit{supra} note 78, at A14; ACLU Press Release, \textit{supra} note 92.

\textsuperscript{238} \textit{See} 18 U.S.C. § 2511(2)(i) (added October 26, 2001).

\textsuperscript{239} \textit{See} Pub. L. 107-56, § 224 (“[T]his title and the amendments made by this title . . . shall cease to have effect on December 31, 2005.”)
In this section, I will explain why the computer trespasser exception is an important and appropriate addition to the Wiretap Act that should make sense to law enforcement and civil libertarians alike. In the interests of full disclosure, I should make clear that I am not a neutral player in this debate: I first proposed adding a computer trespasser exception to the Wiretap Act to several colleagues at the Justice Department in the summer of 1999, and pushed it within DOJ until I left in the summer of 2001. Although success has a thousand fathers, my understanding is that my efforts helped persuade other DOJ officials to support a computer trespasser exception, and that such an exception eventually became a part of the package that DOJ picked up as its Anti-Terrorism proposal. The DOJ proposal then led in modified form to the Patriot Act.

This section begins by showing how the structure of the Wiretap Act reflects its origins as a means of protecting telephone privacy, and how applying the same legal framework to the Internet triggers the need for a computer trespasser exception. It then explains how the computer trespasser exception fills this need, and carves out a middle course that will preserve privacy protections and more closely translate Fourth Amendment protections to the Internet. I argue that the computer trespasser better matches the Wiretap Act’s protections to the Fourth Amendment, and in the long run should increase the privacy protection of the Wiretap Act by imposing implicit limits on the scope of other exceptions to the Wiretap Act. At the same time, critics of the trespasser exception are right to note that the current language needs slight redrafting to clarify its scope and purpose.

A. The Structure of the Wiretap Act and the Assumptions of the Telephone System

To understand why the Wiretap Act needs a computer trespasser exception, we must begin by seeing how the Wiretap Act applies to the communications network for which it was designed, the telephone network. As enacted in 1968, the Wiretap Act imposes a strikingly broad privacy regime that protected essentially all telephone

---

240 See Rosen, supra note 78, at A14 (quoting Alan Davidson).
communications within the United States. The Act presumes that all telephone communications would occur between two human “parties” to the call, and prohibits both the government and private parties from breaking into the communication with a surveillance tool to tap the “contents” of the communication without a special court order. We can represent this prohibited act of surveillance with the following figure:

![Diagram of surveillance](image)

This scheme is easy to understand in the case of a telephone call: imagine A and B conversing on a dedicated line, and a surveillance device being used to tap the line and intercept their conversation. The Wiretap Act makes it a crime for anyone to use a device to tap the line between A and B without a “super warrant” court order, subject to a few exceptions.

Although the Wiretap Act has many exceptions, only two are particularly important. The first is the consent exception. The exception allows any “party to the communication” to consent to surveillance. In the case of the telephone call between A and B, the parties to the communication prove easy to identify: they are A and B. This exception allows participants to telephone calls to record the calls, or to consent to having someone else do so. So long as one of the participants to the call consents to the monitoring, the surveillance does not violate the Wiretap Act. The courts have construed consent fairly broadly in this context: for example, notice that monitoring will occur can

---

243 18 U.S.C. § 2510(8)
244 18 U.S.C. § 2518.
245 18 U.S.C. § 2511(1)
247 Id.
248 See United States v. Davis, 1 F.3d 1014, 1015 (10th Cir. 1993).
249 18 U.S.C. § 2511(2)(c)-(d). If the party is not acting under color of law, he must not have the purpose to commit “any criminal or tortious act.” § 2511(2)(d).
generate consent. If a person uses the telephone after receiving notice that they will be monitored, the theory goes, they have given "implied consent" to monitoring. However, if the telephone user has not either expressly consented or received notice of the monitoring, consent will not be "cavalierly implied."

The second important exception allows providers to intercept communications through their network when it is a "necessary incident. . . to the protection of the rights or property of the provider of that service." In the parlance of Section I of this article, this is a provider power, not a government power, and is often known as the provider exception. In the telephone context, the provider exception permits the phone company to wiretap phones when it necessary to combat unauthorized use of the phone network. The exception arose out of a series of "blue box" cases in the 1960s, in which individuals used illegal blue box devices that allowed them to trick the telephone system into letting them make unlimited long-distance calls for free. Importantly, however, the courts have stressed that this is a narrow exception: it only allows the phone company to conduct limited surveillance for business-related reasons, and does not allow them to monitor even unauthorized use to help law enforcement.

The structure of the Wiretap Act allows it to produce counterintuitive results. Many lawyers and citizens assume that wiretapping powers track ownership in the network: if a company owns the network and provides the phones, we assume, it must have intrinsic

---

250 See United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987). Implied consent exists when circumstances indicate that a party to a communication was "in fact aware" of monitoring, and nevertheless proceeded to use the monitored system. United States v. Workman, 80 F.3d 688, 693 (2d Cir. 1996) See also Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990) ("[I]mplied consent is consent in fact which is inferred from surrounding circumstances indicating that the party knowingly agreed to the surveillance.") (internal quotations omitted). Proof of notice to the party generally supports the conclusion that the party knew of the monitoring. See Workman, 80 F.3d. at 693.

251 See Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998).


255 See, e.g., United States v. Auler, 539 F.2d 642, 646 (7th Cir. 1976).

256 See, e.g., Bubis v. United States, 384 F.2d 643, 648 (9th Cir. 1967).

257 See id.

authority to monitor the network.\textsuperscript{259} Not so. In fact, ownership of the network bestows no special monitoring privileges under the Wiretap Act;\textsuperscript{260} nor does unauthorized use trigger any traditional exception.\textsuperscript{261} Under the Wiretap Act, an employee has successfully sued her employer for listening to the employee’s personal calls at work on the employer’s phone during work hours.\textsuperscript{262} More remarkably, a kidnapper once successfully sued the police for wiretapping his illegal cloned cellular phone calls in the course of locating the kidnapper and freeing his victim.\textsuperscript{263} Because the monitoring in these two cases fell outside of the Act’s exceptions, the monitoring violated the Wiretap Act.

\textbf{B. Applying the Wiretap Act to the Internet: How do the Exceptions Apply, and Who is a Party to the Communication?}

So much for the telephone. How about the Internet? In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA").\textsuperscript{264} ECPA created the basic statutory framework for Internet surveillance that exists today. Among the important changes brought about by ECPA was that the law applied the privacy protections of the telephone Wiretap Act to computer networks. The 1986 Act added

\begin{itemize}
  \item[\textsuperscript{259}] The New York Times has often repeated this as fact. See, e.g., Carl S. Kaplan, \textit{Big Brother as a Workplace Robot}, N.Y. TIMES, July 24, 1997.
  \item[\textsuperscript{260}] A possible exception is the so-called “extension telephone” exception. See 18 U.S.C. § 2510(5)(a). This exception makes clear that when a phone company furnishes an employer with an extension telephone for a legitimate work-related purpose, the employer’s monitoring of employees using the extension phone for legitimate work-related purposes does not violate Title III. See Briggs v. American Air Filter Co., 630 F.2d 414, 418 (5th Cir. 1980) (reviewing legislative history of Title III); Watkins v. L.M. Berry & Co., 704 F.2d 577, 582 (11th Cir. 1983) (applying exception to permit monitoring of sales representatives); James v. Newspaper Agency Corp. 591 F.2d 579, 581 (10th Cir. 1979) (applying exception to permit monitoring of newspaper employees’ conversations with customers).
  \item[\textsuperscript{261}] Or at least it did not until the computer trespasser exception.
  \item[\textsuperscript{262}] Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992) (holding employer liable for listening in on employee’s phone calls at work, on the ground that employer merely told employee that employer “might” listen in on employee’s calls, which was insufficient to generate consent.)
  \item[\textsuperscript{263}] McClelland v. McGrath, 31 F. Supp. 616 (N.D. Ill. 1998) (denying officers’ motion for summary judgment on the ground that the officers had encouraged the cellular service provider to engage in the monitoring, and therefore that it fell outside the provider exception.).
  \item[\textsuperscript{264}] Pub. L. 99-508. (passed October 21, 1986).
\end{itemize}
“electronic communications” to the telephone “wire communications” that the Wiretap Act protected, bringing the entire Internet within the broad protection of the wiretap laws.

Adding Internet e-mail to the category of communications protected by the Wiretap Act made obvious sense. However, it also created a series of difficult analytical problems that its drafters apparently failed to foresee. The difficulty begins with the fact that there is a great deal to the Internet beyond e-mail, as we saw in Section I. Internet communications can consist of e-mails, but they can also be web pages in transit, computer commands send to remote servers, music or pornography files, network traffic, and other communications.\textsuperscript{265} The Internet does not just provide a means of letting people connect with other people: it also creates a communications network that supports a range of hardware and software that together foster a virtual world of cyberspace.\textsuperscript{266}

The Internet’s multifunctionality creates a series of puzzling problems when we try to apply the Wiretap Act to it. We confronted one of those problems in Section II: what are “contents” of a communication in the case of a human-to-computer communication such as a computer command to retrieve a web page?\textsuperscript{267} This problem is matched with an even more puzzling question that helps explains the need for the computer trespasser exception. The problem is this: How does the consent exception apply to the Internet? More specifically, who is a “party to the communication” who can consent to monitoring in the case of a human-to-computer or computer-to-computer communication? The scope of privacy protection that the Wiretap Act provides hinges on the answer to this question.

We can see the question’s critical importance by considering a hypothetical law enforcement investigation into computer hacking, drawn from several cases that I worked on at the Justice Department. Imagine that a computer hacker in New York logs on to the Internet using a modem that connects him to his ISP in New Jersey. The hacker plans to attack sensitive Defense Department computers in California, but to

\textsuperscript{265} See Gralla, supra note 26.
\textsuperscript{266} See generally Lawrence Lessig, Code and Other Laws of Cyberspace (1999)
\textsuperscript{267} See supra notes 142 to 154 and associated text.
avoid detection he decides to first route his communications through a few victim computers along the way.\textsuperscript{268} This can effectively disguise his location because computers only know the immediate source from which a communication was sent: if a user routes a command from A to B to C, the computer at C will only know that the command came from B, and will not know that the command actually originated from A.

Let’s imagine that from his ISP in New Jersey, our hacker hacks into a computer at a small company in Nebraska, and from that site in Nebraska he hacks into another computer belonging to a high school in Arizona. Finally, from the computer in Arizona he launches a computer attack against Defense Department computers in California that contain potentially sensitive information relating to national security. Defense Department criminal investigators then begin an investigation into the attacks.

We can appreciate the importance of identifying who is a party to the communication by imagining how the investigation will likely proceed. From the perspective of the victims at the Defense Department, they will only know that they are under attack from a computer at a high school in Arizona\textsuperscript{269} Agents will call up the school and let them know that either a student at the school is attacking them, or that they have a hacker inside their network. The agents would prefer that the high school will want to monitor the hacker and either identify him (if he is local), or tell the agents the next hop in the chain that can lead back to the hacker (if he is not). It’s possible that the high school will prove eager and capable of helping the law enforcement agents, and will monitor the hacker itself and disclose to the agents that the next link back in the chain was the company in Nebraska. However, watching the attack occur is itself an interception of electronic communications under the Wiretap Act, and must be justified by an exception to the Act. If the school volunteers this information, the provider exception would clearly allow the school to conduct the monitoring and disclose it to the

\textsuperscript{268} This is a common tactic among hackers. See CCIPS Manual, \textit{supra} note 16, at 160 (“When a hacker launches an attack against a computer network, . . . he may route the attack through a handful of compromised computer systems before directing the attack at a final victim.”)

\textsuperscript{269} This is true because they can only read the packets that are directed to them, and those packets will only have the IP addresses of the computers that are the next hop back in the chain.
agents.\textsuperscript{270} The agents can then turn to the company in Nebraska and repeat the process, hoping it leads them to the ISP in New Jersey, which can identify the hacker as its customer.

However, the legal ground shifts considerably if the school is willing to let the agents monitor its network, but lacks the expertise or resources to conduct the monitoring itself. The provider exception does not itself allow law enforcement to step in and conduct monitoring on a provider's behalf, even with the provider’s consent.\textsuperscript{271} As a result, whether the police can conduct the monitoring with the school’s consent depends on whether the school is a “party” to the hacker’s communication. This in turn depends upon how we model the hacker’s conduct. If we say that the hacker sent a communication to the school with instructions for the school’s computer to launch attacks against the California victims, then we can say that the school itself is a party to the communication and can consent to the government’s monitoring. On the other hand, if we say that the hacker himself sent the communication to the California victim but merely routed the communication through the school, then the school is not a party and cannot consent.\textsuperscript{272}

\textsuperscript{270} 18 U.S.C. § 2511(2)(a)(i).


\textsuperscript{272} One way for law enforcement to get around this problem is to have the ISP install a “banner,” which is a notice that tells users that their use may be monitored. If a user sees the banner but proceeds to use the network, then cases indicate that he has “consented” to monitoring and therefore subsequent monitoring will not violate Title III. \textit{See} United States v. Amen, 831 F.2d 373, 379 (2d Cir. 1987). There are two difficulties with this approach. First, it is disturbing from a privacy standpoint: it requires all users who see the banner to relinquish their rights against monitoring solely to allow law enforcement to monitor unauthorized hackers. It may be possible to banner the network narrowly, but when it is not the use of a banner requires a broad waiver of privacy protection from entirely innocent network users. Second, if the hacker comes up with a clever way to enter the network that allows him to bypass the banner, the cases suggest that the government still cannot monitor the hacker unless it shows “convincingly” that the hacker actually knew of the monitoring. \textit{See} United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995) (“The surrounding circumstances must convincingly show that the party knew about and consented to the interception in spite of the lack of formal notice or deficient formal notice.”). This is extremely difficult to do in the electronic context. The result is an unsatisfying (if not downright silly) cat-and-mouse game between the hackers and law enforcement, in which the cops try to place the banners in front of the hackers to try to establish their consent, and the hackers try to evade them. When I was at the Justice Department, this cat-and-mouse game was a routine feature of computer intrusion
What complicates this picture is that labeling the school a party to the communication may sound logical here – after all, the school is a victim of crime – but ultimately would eviscerate the privacy protections that the Wiretap Act offers. Internet communications almost never travel directly from their point of origin to their destination: most travel from hop to hop as they traverse the network.\textsuperscript{273} If each hop is a party to the communication, then any provider can monitor any communication within its network, or can consent to monitoring by others.

Take the case of e-mail. If a friend sends me an e-mail from his account at eck@panix.com to my law school account at okerr@main.nlc.gwu.edu, he is actually sending the message to his ISP, panix.com, with instructions to send it to the George Washington University server, main.nlc.gwu.edu, with instructions for the GW server to send the message into the “okerr” account.\textsuperscript{274} If every hop is a party to communications it handles, that means that both panix and GW are parties to the e-mail between my friend and I, and that both can consent to law enforcement monitoring of every e-mail sent to or from their networks. This would be quite remarkable. It would mean that AOL would be able to watch all of the e-mails sent or received by its users because AOL was itself a “party” to those e-mails. In fact, the owner of every computer would have a right to consent to total surveillance of any communication directed to it.

When taken from the telephone context and applied to the Internet, the consent exception creates an unstable fulcrum upon which to rest Internet surveillance practice. The consent exception can either apply very broadly or very narrowly, and both extremes produce disturbing results. Under a broad reading of the consent exception, the Wiretap Act’s privacy protections are eviscerated; under a narrow reading, the protections are so broad that they do not even allow investigators to watch criminal attacks occur. While the Wiretap Act makes perfect sense as applied to the telephone network, translating its protections to the Internet results in either too little privacy, or too much.

\textit{C. The Computer Trespass Exception: An Attempted Middle}
Ground

The idea of a computer trespasser exception to the Wiretap Act first surfaced within the Justice Department in the summer of 1999. The goal was to fashion a new exception to the Wiretap Act that could take the pressure off the consent exception and more closely and accurately match the Wiretap Act to the Fourth Amendment.

To some extent, the push for a new exception reflected the adage that “necessity is the mother of invention.”275 Within the Justice Department, there was a strong institutional preference for cautious approaches to applying the Wiretap Act to the Internet. If one reading of the Wiretap Act allowed surveillance but another reading forbade it, DOJ would generally adopt the more cautious approach and refuse to sanction the surveillance. Under these restrictions, most of the government’s investigations into computer hacking proved unsuccessful: the government normally could not monitor the hacker’s communications, which made it difficult to identify the hacker or understand the scope of the hacker’s activity. Even though hacking victims were often willing to consent to law enforcement surveillance of the hacker within their network, the law was understood to forbid such a move.276 In most cases, the hacker’s trail went cold and the case remained unsolved.

The purpose of the computer trespasser exception was to carve out a narrow exception which would allow monitoring of hacker communications in some instances without disrupting an otherwise narrow reading of the consent exception. The proposed exception acted as a cross between the existing provider exception and consent exception: it would allow the government to intercept the communications of computer hackers who did not have authorization to use the network when the owner of the network consented to the surveillance in their network. Conceptually, this aligned the Wiretap Act more closely to the Fourth Amendment. If we understand a hacker’s communications as the virtual equivalent of a burglar inside the victimized network,277 then a hacker has no reasonable expectation of privacy in

---

275 GEORGE FARQUHAR, THE TWINS, Act i. (1672).
his attack and the Fourth Amendment would not afford him any privacy rights against monitoring.\textsuperscript{278} From the perspective of a victim’s rights, this also matched victim’s options on-line and off: just like a victim of a burglary in his home can consent to monitoring of a burglar there, a victim of hacking should be able to consent to monitoring of a hacker within its network.\textsuperscript{279}

The proposed computer trespass exception went through various drafts from the summer of 1999 until the fall of 2001, when it was introduced as part of the Justice Department’s proposed Anti-Terrorism Act. The language went through various changes during the legislative process until it emerged in its final form. In its final form, the exception states:

\begin{quote}
It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—
(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser’s communications on the protected computer;
(II) the person acting under color of law is lawfully engaged in an investigation;
(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser’s communications will be relevant to the investigation; and
(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.\textsuperscript{280}
\end{quote}

\textsuperscript{278} See Kerr, \textit{supra} note 243, at 1298.

\textsuperscript{279} This rationale matches the one offered by the Justice Department in the “field guide” it released to the public to help explain the Patriot Act. Prior law, the field guide noted, arguably prevented law enforcement from assisting victims to take the natural and reasonable steps in their own defense that would be entirely legal in the physical world. In the physical world, burglary victims may invite the police into their homes to help them catch burglars in the act of committing their crimes. The wiretap statute should not block investigators from responding to similar requests in the computer context simply because the means of committing the burglary happen to fall within the definition of a “wire or electronic communication” according to the wiretap statute.

The law also defines “computer trespasser” as follows:

"computer trespasser”—

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.\(^{281}\)

This approach largely captures the essence of the original proposed computer trespasser exception. It allows the government to intercept the communications of a “computer trespasser” with the consent of the owner or operator of the trespasser’s victim. In particular, the language of the exception clearly contemplates a situation like the one in my earlier hypothetical, in which government agents investigating a hacking incident need a victim’s consent to trace the communication the next hop back in the chain. In these circumstances, “person[s] acting under color of law”\(^{282}\) will be “lawfully engaged in an investigation,”\(^{283}\) will then approach the owner/operator of the system to have them “authorize the interception,”\(^{284}\) and will then intercept the communications of computer trespasser that they have “reasonable grounds to believe”\(^{285}\) will let them trace back and/or identify the hacker.

Unfortunately, the current text of the exception contains a few textual quirks that Congress will likely have to revisit and revise. For example, one condition of the exception states that it applies only when “such interception does not acquire communications other than those transmitted to or from the computer trespasser.”\(^{286}\) This can be read in two ways. Is “such interception” the interception of the precise communications that the government seeks to justify using the trespasser exception, or act of interception more broadly? Under the latter


\(^{282}\) § 2511(2)(i)

\(^{283}\) § 2511(2)(i)(II)

\(^{284}\) § 2511(2)(i)(I)

\(^{285}\) § 2511(2)(i)(III)

reading, the exception permits the government to rely on the exception only when all of the communications that the government intercepts relate to the computer trespasser. If the monitoring picks up any communications unrelated to the hacking, then the government cannot rely on the exception. Under the former reading, the condition merely clarifies that the exception can only justify the interception of a trespasser’s communication, and that other the interception of other communications must still be justified using other exceptions to the Wiretap Act, such as consent.

The DOJ field guide indicates that it is this latter interpretation that was intended, and this is the far more sensible rule. However, the text of the exception seems to point the other way: the exception only extends to the interception of “communications of a computer trespasser,” which presumably means communications “transmitted to or from the computer trespasser.” Under the former reading, the extra language of 18 U.S.C. § 2511(2)(i)(IV) appears entirely redundant.

A similar problem afflicts the definition of “computer trespasser” found in 18 U.S.C. § 2510(21). This provision defines a computer trespasser as one “who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer.” The phrasing here is quite strange. The term “reasonable expectation of privacy” is of course a constitutional standard from Fourth Amendment law. Whether a user who accesses a computer without authorization has any Fourth Amendment protections in communications to, through, or from the victim computer is a question for the courts, not Congress.

287 The Field guide explains that this language ensures that the exception “would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer.” (emphasis added). See Field Guide, supra note [].

288 My understanding is that DOJ intended the computer trespasser exception to work in conjunction with a banner that would generate a user’s consent. See note [], supra. All legitimate users would have seen the banner, justifying any inadvertent interception of their communications under the consent exception. The computer trespasser exception could then justify the interception of the communications belonging hackers who managed to enter through a backdoor and did not see the banner.


Further, the current language appears to make most of this definition a nullity: defining a computer trespasser as one “who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer” is no different from defining a computer trespasser as one “who accesses a protected computer without authorization.” The added Congressional articulation of how it thinks the courts should apply the Fourth Amendment has no place in the statute. The better approach would have been for the statute to define a computer trespasser and one who accesses a computer without authorization and has no reasonable expectation of privacy, which would leave the constitutional question for the courts where it belongs.291

D. The Benefits of the Computer Trespasser Exception

Despite these shortcomings, both law enforcement and civil libertarians should recognize the substantial benefits to having a computer trespasser exception to the Wiretap Act. From a law enforcement perspective, the exception guarantees that the Wiretap Act will not unnecessarily impede computer hacking investigations by giving hackers privacy rights in their attacks. This effect isn’t surprising: the DOJ pushed the exception, so we might expect it to serve DOJ’s interests.

What is surprising is that the exception should appeal at least in part to civil libertarians. The reason is subtle but important: the computer trespasser exception implicitly signals that courts should adopt a narrow view of the all-important consent exception. The trespasser exception only makes sense if mere pass-through computers are not parties to communications that can consent to monitoring; otherwise, the exception would merely cover ground already covered by the consent exception. The existence of the trespasser exception sends a strong signal to the courts: to give effect to the trespasser exception, courts will

291 This is the approach that Congress took when defining “oral communications,” the interception of which is protected by Title III to prevent eavesdropping and bugging. The definition states: “‘oral communication’ means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication.” 18 U.S.C. § 2510(2).
be forced to construe the consent exception narrowly.  

So while civil libertarians have criticized the trespasser exception for expanding the scope of wiretapping in open ended ways, they have missed the fact that the exception may have actually narrowed the scope of wiretapping. Before the Patriot Act, it was unclear whether a pass-through intermediary computer could consent to monitoring, but at least two courts of appeal had suggested that they might. By adopting the Justice Department’s proposal on the trespasser exception, Congress in effect adopted the DOJ’s cautious assumptions about how the Wiretap Act applied to the Internet. Rejecting the broad reading of the consent exception will reign in an exception that threatened to radically minimize the protections of the Wiretap Act. No matter how broadly the trespasser exception may be viewed, it cannot be as broad as the consent exception might have otherwise been.

Finally, the trespasser exception more closely aligns the Wiretap Act with the Fourth Amendment upon which it is based. In the

---

292 See Kungys v. United States, 485 U.S. 759, 778 (1988) (noting “the cardinal rule of statutory interpretation that no provision [of a statute] should be construed to be entirely redundant.”). An interesting question will arise if Congress decides not to renew the trespasser exception after it sunsets in 2005. Should that be seen as reinstating the broader

293 As Peter Swire has remarked, the trespasser exception “is a significant change to current law, because it creates conditions under which law enforcement officials can station themselves in communications companies to watch phone calls, e-mail, and web surfing as it occurs. Some non-government experts are beginning to point out how open-ended the computer trespasser exception may turn out to be in practice.” Swire, supra note[]. However, if is true with regards to the trespasser exception, it is much more true in the case of the consent exception, which the trespasser exception implicitly narrows.

294 See United States v. Seidlitz, 589 F.2d 152, 158 (4th Cir.1978) (concluding in dicta that a company that leased and maintained a compromised computer system was “for all intents and purposes a party to the communications” when company employees intercepted intrusions into the system from an unauthorized user using a supervisor’s hijacked account); United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993) (stating as an alternate holding that the consent exception of § 2511(2)(d) authorizes monitoring of computer system misuse because the owner of the computer system is a party to the communication).

295 Beyond the question of consent, the trespasser exception may also implicitly point to a broad reading of “contents.” If a hacker’s commands and traffic are not “contents” under the Wiretap Act, then the government does not need the trespasser exception to surveil those commands and traffic; the surveillance would not implicate the Wiretap Act at all.

296 See United States v. Torres, 751 F.2d 875, 884 (7th Cir. 1985).
physical world, the Fourth Amendment “reasonable expectation of privacy” test protects those who are legitimately on the premises, but not trespassers. The trespasser exception does the same for the Wiretap Act. Such an exception was not needed in the telephone era, when all communications were person-to-person communications that seemed intrinsically private. The Internet has introduced something new: human-to-computer and computer-to-computer communications that may or may not deserve privacy, depending on the circumstances. The new network now encompasses the full diversity of life in cyberspace, creating a new need for the Wiretap Act to make the same nuanced distinction between authorized and unauthorized communications made by the Fourth Amendment in the physical world.

**CONCLUSION**

The rapid pace of technological change will likely keep the Internet surveillance laws a work in progress for a long time to come. The sunset of many of the Patriot Act’s provisions on December 31, 2005, will prove only one of many opportunities to revisit and revise these laws in the future. Open questions remain, and Congress will have to keep a watchful eye on law enforcement practice and technology to maintain the crucial balance between privacy and security.

The surprise of the USA Patriot Act is that despite the remarkable circumstances of its passage, the Act updates the surveillance laws without dramatically altering the balance, as its critics feared. Some of the Patriot Act’s Internet surveillance previsions helped law enforcement, and others furthered privacy; many did both at the same time. But more than anything else, the Patriot Act started the process of answering how the surveillance statutes apply (and should apply) to the modern Internet. Before the Patriot Act, Congress had not made a comprehensive effort to consider how privacy laws applied to the latest technologies since 1986. The 1986 Act proved remarkably forward-thinking. However, by 2001 the technology had far outpaced

---

298 See Kerr, supra note [], at 1299.
299 See id. at 1298-1300.
The Patriot Act does not and should not represent the final word on electronic surveillance law. When we bypass the soundbites, however, and focus on the details of the legislation, the Act that has been portrayed as the road to Big Brother does not seem to take us there.