6 Va. J.L. & Tech. 4 (2001), *at* http://www.vjolt.net
1522-1687 / 2001 Virginia Journal of Law and Technology Association

VIRGINIA JOURNAL *of* LAW *and* TECHNOLOGY

UNIVERSITY OF VIRGINIA	SPRING 2001	6 VA. J.L. & TECH. 4

Issues Raised by the Application of the Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks

Paul Taylor[1]

I. Introduction
II. The Pen Register Statutes
  A. Current Federal Law Enforcement Interpretations of Its Authority Under the Pen Register Statutes
  B. Substantive Differences Between Telephone Numbers and E-Mail Addresses
III. The FBI's "Carnivore" Program: Problems Posed by Applying New Technologies to Technology-Specific Statutes Such as the Pen Register Statutes
  A. Substantive Differences Between Information Revealed by "Digits Dialed" Over "Circuit-Switched" Telephone Networks and Information Revealed by Addressing Information on "Packet-Switched" Internet Networks
  B. Issues Raised Under the Communications Assistance to Law Enforcement Act
    1. The Court of Appeals for the District of Columbia's Decision in United States Telecom Association v. Federal Communications Commission
    2. The Federal Communications Commission's Implementation of the Communications Assistance to Law Enforcement Act as Applied to "Packet-Switched" Networks
IV. Conclusion

I. Introduction

1. Seventy years ago, Justice Brandeis, in his dissenting opinion in *Olmstead v. United States*[2] predicted that ongoing technological developments would someday enable law enforcement to search people or their property without physical trespass. He also cautioned that courts should be alert to these changes in technology in determining the contours of privacy rights.[3] Today, advances in telecommunications technology have dramatically changed people's lives. Internet technology has increased in popularity and will significantly change the way people handle their affairs and consequently the government's handling of personal communications.[4] However, many statutes protecting privacy were written in an age when the telephone was the dominant means of long-distance communication. These statutes do not cover communications through increasingly popular modern means, such as electronic mail and other forms of electronic communication, leaving them vulnerable to violations of privacy and consequently tending to deter their use. Several such statutes are those governing the use of so-called "pen register" and "trap and trace" devices.[5]

II. The Pen Register Statutes

2. The statutes governing the use of pen register and trap and trace devices ("the Pen Register Statutes"), enacted when the telephone was the predominant mode of distance communication, currently allow the government to obtain, with a so-called "pen register," the "electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line" and, with a so-called "trap and trace device," the "electronic or other impulses which identify the originating number" of the device from which a wire or electronic communication was transmitted.[6] The government can obtain this information if a government attorney has simply "certified" to the court "that the information likely to be obtained by such installation and use [of the pen register or trap and trace device] is relevant to an ongoing criminal investigation."[7] Upon such "certification" by a government official, the court "shall" issue the order.[8] Thus, a court's approval of a government request to install and use a pen register or trap and trace device is a purely ministerial act.[9]

A. Current Federal Law Enforcement Interpretations of Its Authority Under the Pen Register Statutes

3. It may come as a surprise to many citizens that the government has such ready access to the telephone numbers one dials and those identifying incoming calls. However, authority under the Pen Register Statutes is also currently used by the government to obtain e-mail addresses sent and received. Officials from the Justice Department and the Federal Bureau of Investigation have testified before the House Judiciary Committee, Constitution Subcommittee, that the Pen Register Statutes grant the government the authority to capture e-mail addresses as well as telephone numbers.[10] Thus, if one person is under investigation, and that person sends an e-mail to a second person, law enforcement is likely to put a "cover" on all of the e-mail addresses going in and out of the second person's computer, even if such person is not involved in criminal activity, as the second person's communications would be "relevant" to the investigation insofar as law enforcement would like to know whether the second person is corresponding with other persons under investigation.

B. Substantive Differences Between Telephone Numbers and E-Mail Addresses

4. When the Supreme Court held that the retrieval of telephone numbers pursuant to a pen register request was not an "interception" of content – and that such numbers could therefore be obtained with the minimal showing of evidence required by the Pen Register Statutes – it made clear that "[p]en registers do not 'intercept' because they do not acquire the 'contents' of communications ... They disclose only the telephone numbers that have been dialed a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, *their identities*, nor whether the call was even completed is disclosed by pen registers."[11] Because an e-mail address, unlike a phone number, may contain not only letters but also a person's name, such as "john.smith@home.com," and other descriptive elements that could be considered "content," such as "wild-and-crazyjohn.smith@home.com," e-mail addresses may not only be outside the clear terms of the Pen Register Statutes, but the low standard under which the government may be authorized to access information under the Pen Register Statutes may be too low to constitutionally authorize its access to e-mail addresses.

5. Further, the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations ("Guidelines"), as in effect today and last revised by Attorney General Thornburgh in March, 1989, apply to the Federal Bureau of Investigation. The Guidelines make clear that "[a] general crimes investigation may be initiated by the FBI" only when "facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed."[12] This standard of "reasonable indicia" is higher than the current requirement of "relevance" to "an ongoing investigation" under the Pen Register Statutes.[13] The Guidelines also make clear that certain types of investigative techniques "shall not" be used prior to initiating an investigation, including "mail covers" and "[n]onconsensual electronic surveillance."[14] If an e-mail address is the conceptual equivalent of a mailing address on an envelope delivered through the federal postal service, which are the subject of "mail covers," a higher standard than that currently used by the government to obtain e-mail addresses under the Pen Register Statutes would seem appropriate.[15]

6. Courts have also held that the use of passwords to access e-mail accounts, which include access to e-mail addresses from which messages were sent to or received from, indicates users have an objective expectation of privacy in the communications transmitted between such accounts.[16] Courts have similarly held that users of pager devices have an objective expectation of privacy in the lists of incoming telephone numbers stored in the pager's memory.[17] The American Bar Association has also stated lawyers transmitting information related to their representation of clients have a reasonable expectation of privacy in such communications because "[t]he denial of external access ordinarily is ensured by the use of password-protected mailboxes or encryption."[18]

C. The FBI's "Carnivore" Program: Problems Posed by Applying New Technologies to Technology-Specific Statutes Such as the Pen Register Statutes

7. In recent years, with the growth of the Internet, the Federal Bureau of Investigation ("FBI") has encountered an increasing number of criminal investigations, including those involving terrorist threats, in which criminal subjects have used the Internet to communicate with each other or their victims. Because many Internet service providers ("ISP's") lack the ability to discriminate between communications in order to isolate the specific types of information that may be authorized to be gathered under a court order, the FBI has designed and developed a program called "Carnivore" which provides the FBI with a capability that is said to allow the interception and collection of communications that are the subject of lawful orders while avoiding those communications not authorized under such orders.[19]

8. The program is reported to be named Carnivore because it rapidly finds the "meat" in vast amounts of data. It was developed at FBI computer labs in Quantico, Virginia, and has been reported to have been used in fewer than 25 investigations over the past 18 months.[20] However, Marcus Thomas, chief of the FBI's cyber−technology section at Quantico, has indicated that the FBI has already has seen "growth in the rate of requests" for use of the Carnivore program.[21] The new program operates on commonly available personal computers and takes advantage of the "packet"-based nature of Internet communications in which computers on the Internet break up e−mail messages, World Wide Web site traffic, and other information into pieces and route the packets across the global network, where they are reassembled at the other end. FBI programmers are reported to have devised a "packet sniffer" system that can analyze data flowing through computer networks to determine whether it is part of an e−mail message or some other piece of Web traffic. The Carnivore program is operated under the exclusive control of government agents.[22]

9. The Carnivore program has been used pursuant to authority under the Pen Register Statutes.[23] Testimony provided to Congress indicates that Carnivore has been used by the federal government at least 16 times in 2000, including instances in which it has been applied pursuant solely to authority under the Pen Register Statutes.[24]

10. The breadth of information that the government has been seeking to obtain from Internet networks under the authority of the Pen Register Statutes remains unclear. Courts that uphold the Pen Register Statutes' application to Internet-based information, and do not limit its application to the retrieval of "digits" alone, may not be subject to review either because the target is never made aware of the retrieval[25] or the court's decision in the case is kept under seal to prevent alerting the target, who might then cease communications. Testimony provided by attorney Robert Corn-Revere, however, illustrates the argument federal law enforcement authorities have used to extrapolate from the "digits" referred to in the Pen Register Statutes to "letters." According to Mr. Corn-Revere, the federal government, in court papers, asserted that the Pen Register Statutes allow law enforcement access to the "conceptual equivalent of a telephone number" and that, even though e-mail addresses "are commonly referred to by names ... such names are viewed by the computer as numbers."[26] Ultimately, everything traveling through computer components is "digitized" – or reduced to the binary system of zeroes and ones acting as "on" and "off" switches – meaning "to covert to digital form," with "digital" meaning "of or relating to data in the form of numerical digits."[27] Such an argument could, by its internal logic, make words, sentences, and the full substance of electronic communications accessible to the government as "digits" under the Pen Register Statutes.

A. Substantive Differences Between Information Revealed by "Digits Dialed" Over "Circuit-Switched" Telephone Networks and Information Revealed by Addressing Information on "Packet-Switched" Internet Networks

11. As Stewart Baker, former general counsel of the National Security Agency, has stated, "[N]one of the fights with industry have been over whether the FBI can get content; that has always been easily agreed upon. The fights have all turned on the FBI's efforts to get more and more transactional data under the guise of trap and trace orders and the like, I think because, as we have heard, the legal standards for getting that information is quite low."[28]

12. With such concerns in mind, many have questioned whether the "pen register" and "trap and trace" concepts as set forth in the Pen Register Statutes can be readily applied to the online environment without raising privacy concerns. The type of information potentially available from an ISP by a "pen register" greatly exceeds the type of information normally available when one is installed on a telephone line.

13. The nature of information gathering using a "pen register" and "trap and trace" device is different in the online environment compared to traditional telephone systems. Information such as electronic mail is sent over the telephone and other lines ISP's use to connect their data networks to the telecommunications system, but, some have argued, these facts do not convert the facilities of Internet service providers into "telephone lines." A trap and trace device or pen register for Internet−based communications is installed on the data network of an ISP, not on a telephone line, and the information which may be intercepted is not limited to that transmitted over a single subscriber line. Further, the provisions of Pen Register Statutes clearly contemplate making a physical connection to a dedicated telephone line,[29] which envisions a different type of network configuration than exists for Internet−based systems, which have been described as combining both call routing information and content in the same information "packets." The difference between telephone networks, known as "circuit-switched" networks, and Internet networks, known as "packet-switched" networks has been described in one treatise on the subject as follows:

> [T]he Internet is what is known as a packet−switched network. In a *packet−switched network*, there is no single, unbroken connection between sender and receiver. Instead, when information is sent, it is broken into small packets, sent over many different routes at the same time, and then reassembled at the receiving end. By contrast, the telephone system is a circuit−switched network. In a *circuit−switched network*, after a connection is made (as with a telephone call, for example), that part of the network is dedicated only to that single connection.[30]

14. Consequently, the use of pen registers or trap and trace devices to intercept packetized network information raises privacy concerns of a different magnitude than the Supreme Court contemplated when it addressed the constitutional application of pen registers in *Smith v. Maryland* as such information may reveal more than the conceptual equivalent of a telephone number.[31]

15. The Clinton Administration has articulated a goal that federal surveillance law be updated in a manner that makes its application "technology-neutral," meaning in a manner that applies the same rules to gathering the same types of information transmitted through different types of technology.[32] There are concerns, however, that in certain contexts a "technology-neutral" approach may lead to situations in which the surveillance laws become "content-neutral." In other words, in the quest for "technology-neutrality," the focus may become not on whether the information being gathered is content or not content, but rather on whether the information gathered can by obtained by a certain technology, such as that capable of capturing "routing" or "addressing" information that may contain elements of content but which might be gathered from the Internet with a pen register or trap and trace device.

16. On July 31, 2000, the Clinton Administration forwarded to Congress a proposed "Enhancement of Privacy and Public Safety in Cyberspace Act," which includes changes to the federal electronic surveillance laws. One provision of the proposal would amend the definition of "pen register" such that the devices are defined to mean "a device *or process* which records or decodes *dialing, routing, addressing, and signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted*."[33] Currently, "pen register" is defined as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line."[34] The Administration's proposal would greatly expand the reach of a pen register request by changing the current language that restricts such requests to "numbers dialed or otherwise transmitted" to include any "dialing, routing, addressing, and signaling information transmitted." This is language identical to Senate bill S. 2092, introduced by Senator Charles Schumer in the 106th Congress, which also amends the Pen Register Statutes. Such a broad definition, however, significantly alters the intent of the statutes as understood with their terms, which currently limit the type of information that may be collected by a pen register or trap and trace device to information identifying the origin device or destination device of a communication. The phrase "dialing, routing, addressing or signaling information" is broad enough to expand the amount of information that can be sought in ways that are unclear but that are likely to increase the intrusiveness of these devices, which under Supreme Court precedent have not been understood as identifying the parties to a communication or even whether the communication was even completed.[35] Such a definitional change goes significantly beyond simply eliminating an archaic reference to telephone lines.

17. Such a broad definition of what can be captured by pen registers runs the risk that courts will interpret the definition to include, as "routing" information, computer code transmitted to indicate from which part of the Internet a person was requesting information, which could include search terms used to locate, for example, books on certain subjects to be ordered from on on-line bookstore. The Clinton Administration's "Proposed Legislative History" for the Administrations proposal, attached to its proposed legislation transmitted to Congress, states that the Administration's proposed amendments could not be interpreted to reach such "content," stating:

> [T]he amendments clarify that orders for the installation of pen register and trap and trace devices may obtain any non-content information all "dialing, routing, addressing, and signaling information" utilized in the processing and transmitting of wire and electronic communications. Just as today, such an order could not be used to intercept the contents of communications protected by the wiretap statute, such as the subject line of the body of an e-mail message or the search terms typed into a Worldwide Web search engine.[36]

At a June 24, 2000, hearing before the House Constitution Subcommittee, however, one witness presented the following example using a computer printout of a sample Internet Protocol packet showing a search for a book on the Barnes and Noble Web site:

```
1  TIME: 15:02:27.439225 (0.111930)
2  LINK: 00:80:19:42:21:68 -> 00:D0:58:A9:30:52 type=IP
3  IP: 207.226.3.43 -> 208.158.245.141 hlen=20 TOS=00 dgramlen=695 id=6638
4  MF/DF=0/1 frag=0 TTL=255 proto=TCP cksum=79CE
5  TCP: port 1559 -> http seq=3306680833 ack=0184661700
6  hlen=20 (data=655) UAPRSF=011000 wnd=17520 cksum=C1DE urg=0
7  DATA: GET /booksearch/results.asp?WRD=prostate+cancer&userid=4MOT3
```
[37]

18. An important question is whether the portion italicized in line 7 would constitute, under the Clinton Administration's proposal, "routing ... information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." The broad terms of the Clinton Administration's proposal, its "Proposed Legislative History" notwithstanding, includes nothing that would make clear to judges that such terms exclude the sort of "content" that could be included in a line of computer code, such as that in line 7 of the above example of computer code "routing" information on the Internet. The term "addressing information" is also broad. "Addressing" information on the Internet allows each separate piece of information on the Internet to have a unique "address," or location. Such "addressing" information includes Uniform Resource Locators ("URL's"), which might describe the contents of a certain library of information on the Internet, such as a File Transfer Protocol ("FTP") address, as in "ftp://ftp.mentalhealth.com/depression/treatments."[38] An address defining the location of certain content on the Internet, if obtained by the government, would reveal not only the location of such content, but also the precise text that may have been reviewed by an individual[39].

19. In similar contexts, courts have held that if a device is simply capable of gathering content, whether or not it is used to obtain content in any given instance, it may not be considered a "pen register" under the Pen Register Statutes and may be subject to use only when more stringent standards than those set out in the Pen Register Statutes have been met by the government. In *Brown v. Waddell*, the court held that a device used by the government to intercept numbers appearing on a target's digital display pager was not a "pen register" because digital display pagers are capable of receiving a series of numbers that are not telephone numbers, but combinations of numbers used to transmit "coded messages of unlimited substantive content."[40] As the court made clear, "[t]hat a digital display pager programmed to receive numeric transmissions 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 by clone pager–is what makes the interception subject to the [wiretap] authorization requirements of [18 U.S.C.] 2516 and 2518. That the interceptions made in this case did include some such coded messages is relevant only in demonstrating the capability, not in determining whether the interception was legally authorized."[41]

20. New York courts have also held that law enforcement must meet more stringent showings than that required for authorization to use a pen register device when such devices may also be used to gather information other than telephone numbers identifying incoming and outgoing calls. In *People v. Bialostok*, the Court of Appeals of New York held that a pen register having the capacity to monitor telephone conversations would be treated as an eavesdropping device requiring a warrant, stating:

> The traditional pen register was, to a large extent, self-regulating. Neither through police misconduct nor through inadvertence could it reveal to anyone any information in which the telephone user had a legitimate expectation of privacy. The same is not true of the device used here. This is a technology that has the *capacity*, through willful use or otherwise, to intrude on legitimately held privacy, and it is the warrant requirement, interposing the Magistrate's oversight, that provides to citizens appropriate protection against unlawful intrusion. Thus, we hold the devices employed here were subject to the warrant requirement and installation of them without one was unlawful.[42]

B. Issues Raised Under the Communications Assistance to Law Enforcement Act

1. The Court of Appeals for the District of Columbia's Decision in *United States Telecom Association v. Federal Communications Commission*

21. The convergence of information that can be characterized as both "addressing" information and content was recently illustrated in a federal appeals court decision. On August 15, 2000, the United States Court of Appeals for the District of Columbia held that the Federal Communications Commission ("FCC"), in issuing a challenged Order, failed to comply with the Communications Assistance to Law Enforcement Act's ("CALEA")[43] requirement that it "protect the privacy and security of communications not authorized to be intercepted."[44] In its decision, the Court of Appeals expressed concerns that authority under the Pen Register Statutes not extend to "digits" that convey "content," clearly indicating that it would have the same concerns that authority under the Pen Register Statutes not extend to "letters" that convey "content," such as the sender's name in the e-mail address "john.smith@home.com." This decision lends support to the notion that a higher showing on the part of the government should be required when it seeks to gain access to an e-mail address under the Pen Register Statutes or under any authority granted in the future.[45]

22. The Order challenged in *United States Telecom Association v. Federal Communications Commission* had been interpreted by the government as allowing it access to so-called "postcut-through dialed digit extraction" under the authority of the Pen Register Act.[46] As the Court of Appeals explained:

> This [postcut-through dialed digit extraction] capability requires carriers to electronically monitor the communications channel that carries audible call content in order to decode all digits dialed after calls are connected or "cut through." Some post−cut−through dialed digits are telephone numbers, such as when a subject places a calling card, credit card, or collect call by first dialing a long−distance carrier access number and then, after the initial call is "cut through," dialing the telephone number of the destination party. Postcut−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.[47]

The Court of Appeals continued:

> The government contends that a law enforcement agency may receive all post− cut−through digits with a pen register order, subject to CALEA's requirement that the agency uses "technology reasonably available to it" to avoid processing digits that are content. 18 U.S.C. 3121(c). No court has yet considered that contention, however, and it may be that a Title III warrant [issued after a showing of probable cause] is required to receive all post−cut−through digits. The Commission therefore had a statutory obligation to address how its Order, which requires the capability to provide all dialed digits pursuant to a pen register order, would "protect the privacy and security of communications not authorized to be intercepted." 47 U.S.C. 1006(b)(2). The Commission spoke of law enforcement's need to obtain post−cut−through dialed digits and of the cost of providing them, but it never explained, as CALEA requires, how its rule will "protect the privacy and security of communications not authorized to be intercepted."[48]

23. Because the challenged Order required carriers to make available all postcut−through dialed digits −− those that convey content as well as telephone numbers – the Court of Appeals vacated those portions of the Commission's challenged Order allowing law enforcement access to "postcut-through dialed digit extraction" under the authority of the Pen Register Statutes. The Court of Appeals' concerns that authority under the Pen Register Act not extend to "digits" that convey "content," indicates it would have the same concerns that authority under the Pen Register Statutes not extend to letters that convey content, such as the sender's name in the e-mail address "john.smith@home.com."[49]

24. Also, the nature of information gathered using a "pen register" and "trap and trace" device is different in the online environment compared to traditional telephone systems, and the Court of Appeals made clear in its decision that simply because information may be delivered in "packets" containing source and destination information, as well as content, the government is not relieved from abiding by the higher procedural safeguards that protect content.[50]

2. The Federal Communications Commission's Implementation of the Communications Assistance to Law Enforcement Act as Applied to Packet-Switched Networks

25. The difficulties raised by attempts to separate non-content "transactional" information from information containing content in "packet-switched" networks was addressed by the FCC in its rulemaking proceeding implementing CALEA. The Commission found that interception of packet−mode communications raises significant technical and privacy concerns because call routing information and content are both contained in the packets.[51] In particular, while 18 U.S.C. 3121(c) currently provides that "a government agency authorized to install and use a pen register under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing," according to the FCC, interception of packetized information potentially allows the government to "receive both call identifying information and call content under a pen register."[52] Consequently, the FCC requested that the Telecommunications Industry Association deliver a report to it that would address this issue no later than September 30, 2000.[53]

26. On September 29, 2000, the experts selected by the Telecommunications Industry Association delivered their report of the results of their Joint Expert Meetings ("JEM") to the FCC, as requested in the CALEA Order. The JEM did not address legal issues, but only the technical issues related to the technology used to separate information in packet-switched networks, including the FBI's Carnivore program.[54]

27. The cover letter accompanying the report to the FCC summarized the difficulties encountered by the joint experts in producing their report in light of the absence of a clear legal framework in which to discuss what types of information were appropriately obtained pursuant to an order under the Pen Register Statutes, and which types were not. The letter states:

> The JEM participants were frequently frustrated by the fact that there was no clear, legal framework (either in the statute or from the Commission's decisions) in which to base their evaluations. For example, it is ambiguous how the term "call-identifying information" applies (if at all) to packet data. Without clearer guidance of what constitutes "call-identifying information" for packet data, industry cannot accurately report on the technical impact and feasibility of making such information available to law enforcement.[55]

28. Regarding Carnivore, the JEM Report concluded that the program presented several problems regarding its ability to filter information in packet-based networks. First, concluded the JEM Report, "Carnivore has not been proven effective, as yet, in cases where the subject's communications are part of a high bandwidth transmission."[56] Second, the JEM Report states that while

> Carnivore ... constitutes a potential technical solution for separating content from packet information, ... numerous industry concerns were raised about the introduction of government-provided product into the service provider network. Concerns were acknowledged regarding (a) potential liability for failure of the product, (b) uncertain impact on the network, (c) terms and conditions to obtain the product from government, (d) administrative and operational impacts from constant upgrades to the filter, (e) scalability, (f) privacy, (g) certification or testing of the product, and (h) uncertainty about the scope of the filter (i.e., whether the filter produces information that is coextensive with call identifying information and who establishes the criteria for separation).[57]

29. Finally, the JEM Report contains a discussion of problems entailed in creating an industry standard for the separation of information in a packet-switched network to obtain the type of transactional information that would be requested under the authority of a pen register or trap and trace order. The JEM Report states:

> Relevant Pen Register or Trap and Trace information may be located in different layers of the protocol depending on the specific service used and the application of the packet ... The variability of applications therefore makes it difficult for a service provider to extract such information. New services (and therefore application layer protocols) are developed on a continual basis within the IP [Internet protocol] environment making isolation of Pen Register or Trap and Trace information within an IP data field even more complicated. If a separation capability were to be developed, maintaining accurate and up-to-date separation capabilities (i.e., filtering capabilities) will require rapid, continuous development which will be highly resource intensive. This process does not lend itself to the current standards development process due to the process' sometimes lengthy, consensus driven nature. It is also expected that the industry resources for this work would be significantly greater than the resources that are currently committed for surveillance standards development.[58]

The JEM Report ultimately concludes, "[T]here is no reliable method for determining the Pen Register and Trap and Trace information when monitoring a packet stream."

IV. Conclusion

30. Applying the Pen Register Statutes to information transmitted over "packet-switched" Internet networks pose two distinct problems. First, there are inherent difficulties in separating content from non-content in communications transmitted over packet-switched Internet networks. Second, recent efforts to make the Pen Register Statutes "technology-neutral" by incorporating broad language to describe the objects to which pen register and trap and trace devices may be attached demonstrate the difficulties entailed in selecting words – such as "routing" and "addressing" – that clearly limit the types of information that can be obtained in Internet networks to information that does not contain content. Consequently, new legislation should be enacted that imposes higher standards for access to Internet-based information characterized as "transactional" in nature when the risk is high that content as well as non-content may be disclosed to the government.

---

[1] Attorney, Alexandria, Virginia

[2] 277 U.S. 438, 474 (1928) (holding that tapping of wires leading from defendants' residences to chief office from which alleged conspiracy was directed did not constitute unlawful ‹search or seizure› under the Fourth Amendment) (Brandeis, J., dissenting)

[3] *See id*. at 472−474.

[4] As stated in a recent White House Working Group Report, "[r]egulation tied to a particular technology may quickly become obsolete and require further amendment. In particular, laws written before the widespread use of the Internet may be based on assumptions regarding then−current technologies and thus may need to be clarified or updated to reflect new technological capabilities or realities.›› The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet, Report by the President›s Working Group on Unlawful Conduct on the Internet (March 2000) (hereinafter ‹Report›) at 13.

[5] *See* 18 U.S.C. 3121 *et seq*.

[6] 18 U.S.C. 3127(3); 3127(4).

[7] 18 U.S.C. 3123(a).

[8] *Id*.

[9] As long as the application contains an assertion that the information sought is relevant to the investigation, a court will authorize the installation of a pen register and will not conduct an independent judicial inquiry into the veracity of the attested facts. 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) (The judicial role in approving use of trap and trace devices is ministerial in nature.). The resulting order may authorize use of a pen register for up to sixty days and may be extended for additional sixty−day periods. *See* 18 U.S.C. 3123(c). The court order also orders the provider not to disclose the existence of the pen register to "any ... person, unless or until otherwise ordered by the court." 18 U.S.C. 3123(d)(2).

[10] See Hearing Transcript, ‹‹Fourth Amendment Issues Raised by the FBI›s ‹Carnivore› Program›› (July 24, 2000) at 17-19 (testimony of Dr. Donald Kerr, Director, Lab Division, Federal Bureau of Investigation, Larry Parkinson, General Counsel, Federal Bureau of Investigations, and Kevin Digregory, Deputy Associate Attorney General, Department of Justice).

Testimony provided to the House Subcommittee on the Constitution contains the following exchanges:

> Mr. [Charles] CANADY [Chairman, House Constitution Subcommittee]: ... When you are using the pen register or trap and trace authority, would you ever obtain any letters or information other than those that make up an e-mail address such as JohnSmith@home.com? In other words, have you ever or would you ever make a request under the pen register or trap and trace authority that included the capture of words or sentences other than the e-mail address?
>
> Mr. KERR [Director of the FBI›s Lab Division]: The answer from our side in terms of how we set it up is that if it is a pen register order, we only get the address, and we capture nothing else.

Id. at 17.

This point was reiterated by Larry Parkinson, General Counsel for the Federal Bureau of Investigations:

> Mr. PARKINSON: I might also say that even the subject line we consider to be content, and that would require full Title III. It is just the addressing information, and that is solely just as in the telephone context, the numbers dialed, the numbers received.
>
> Mr. CANADY: Because it is your understanding that your legal authority is limited to the e-mail address, and of course it has been your practice, it is your practice and has been your practice, only to obtain the e-mail address when you are using the trap and trace or the pen register authority?
>
> Mr. KERR: In the electronic communications context, yes, that is correct.

Id. at 17.

[11] United States v. New York Telephone Company, 434 U.S. 159, 167 (1977) (emphasis added).

[12] Attorney General›s Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations at II(C)(1).

[13] *Id.* The Guidelines further elaborate that ‹‹[t]he standard of ‹reasonable indication› is substantially lower than probable cause ... However, the standard does require specific facts or circumstances indicating a past, current, or impending violation. There must be an objective, factual basis for initiating the investigation; a mere hunch is insufficient.›› *Id*. (Emphasis added.)

The Department of Justice currently encourages, but does not require, that this standard be met when pen register requests are made for electronic addressing information. The Computer Crime and Intellectual Property Section of the Department of Justice (CCIPS), in January, 2001, issued its update of guidelines on the search and seizure of computers and electronic evidence. ORIN S. KERR, U.S. DEPT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2001) *available at* http://www.cybercrime.gov/searchmanual.htm [hereinafter CCIPS GUIDELINES]. While the previous version of these Guidelines, issued in 1994, did not include a sample model of a request for a court order for electronic addressing information pursuant to a request under the Pen Register Act, the current version does. In one paragraph of the Guidelines sample pen register application, a bolded and bracketed note addressed to Justice Department attorneys who will be filing such applications regards the evidentiary standard of required relevance to an ongoing criminal investigation. It states, "[a]lthough not required by law, CCIPS recommends the inclusion within the application of specific and articulable facts that support this conclusion." CCIPS Guidelines, App. D.

[14] *Id.* at II(B)(5).

[15] The American Bar Association has also issued an ethics opinion in which it concluded that «[a] lawyer may transmit information related to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct [Model Rule 1.6(a), «Confidentiality of Information,» requiring that information related to client representation be kept in confidence] because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The same privacy accorded U.S. and commercial mail ... applies to Internet e-mail.» ABA Formal Ethics Opinion 99-413 (March 10, 1999).

[16] *See* United States v. Maxwell, 42 M.J. 568, 576 (1995) (holding that "appellant clearly had an objective expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password. Similarly, he had an objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords."), *rev'd on other grounds*, 45 M.J. 406 (C.A.A.F. 1996). *See also* Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591, 1603 (1997) ("Cyberspace communication should be protected with a password to establish a reasonable expectation of privacy.").

[17] *See* United States v. Chan, 830 F.Supp. 531, 534 (N.D.Cal. 1993) ("In contrast to the transmitter of a message to a pager, the possessor of the pager has control over the electronically stored information. The expectation of privacy in an electronic repository for personal data is therefore analogous to that in a personal address book or other repository for such information."); United States v. Lynch, 908 F.Supp. 284, 287 (D.V.I. 1995) (holding that pager user "had a reasonable expectation of privacy in the contents of the pager's memory"); United States v. Reyes, 922 F.Supp. 818, 833 (S.D.N.Y. 1996) (holding the same).

[18] ABA Formal Ethics Opinion 99-413 (March 10, 1999) (concluding that "[l]awyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure"). It is unclear whether the model pen register application included in the CCIPS Guidelines anticipates government access to passwords under a pen register order in certain circumstances. The model pen register application states: "Applicant requests that the Court issue an Order authorizing the installation and use of a pen/trap device to capture the packet header and mail header information (but not the subject lines of e-mails) associated with the transmission of communications and other data (including transfers of information via the World Wide Web, electronic mail, telnet, and the file transfer protocol) to and from the account [Jdoe@isp.com] ...." CCIPS GUIDELINES, App. D. Both telnet and file transfer protocol transfer requests may require the inputting of passwords to gain access to servers, thereby implicating a stronger claim to a reasonable expectation of privacy under the Fourth Amendment, and they also may require the inputting of particular Web site addresses, such as, for example, "mentalhealth.com." Telnet provides a means of using the resources of a distant computer. As described by a leading Internet handbook, "[S]ome [telnet systems] might require that you choose a username and a password that you will use the next time you log in." GRALLA, HOW THE INTERNET WORKS (1999) at 175. File transfer protocols are the most popular means of downloading files on the Internet. Some ftp sites are private, allowing only certain people with the proper account number and password to enter. Id. at 179.

[19] One of the key protections established by Congress when it passed the Wiretapping Protection Act, 18 U.S.C. 2510-22, in 1968 was the «minimization rule.» Minimization means that law enforcement is not supposed to record non−relevant communications. At the time the Electronic Communications Privacy Act («ECPA»), 18 U.S.C. 2510-21; 2701-18; 3121-26, was enacted, it was assumed that this was impossible in the e−mail context because law enforcement would receive all communications to and from a target and read each one to determine if it was relevant. In 1986, the Senate Judiciary Committee expressly addressed this concern and suggested that minimization should be conducted by the initial law enforcement officers who review the intercepted communications. The committee stated, "those officials would delete all non−relevant material and disseminate to other officials only the information which is relevant to the investigation." S. Rep. No. 99−541, at 31 (1986). The FBI's Carnivore program may allow such «minimization» to occur automatically, without requiring anyone to first manually screen the electronic communications.

[20] *See* T. Bridis, N. King, Jr., *Carnivore E-Mail Tool Won't Eat Up Privacy, Says FBI,* WALL ST. J. (July 20, 2000) at A28.

[21] J. Schwartz, *FBI Internet Wiretaps Raise Issues Of Privacy; New System Tracks Suspects*, WASH. POST (July

12, 2000) at E1. This coincides with a recent increase in applications for government interceptions of communications generally, and particularly in requests for electronic, rather than telephone, wiretaps. The 1999 Wiretap Report, issued annually by the Administrative Office of the U.S. Courts pursuant to 18 U.S.C. 2519, reports that the number of federal intercept applications increased 94 percent between 1989 and 1999. See Administrative Office of the U.S. Courts, 1999 Wiretap Report (May 2000), at 5. In 1999, there were 601 federal intercept orders issued, and 749 orders issued at the state and local level. Id. at Table 7. Prior to 1998, the most common method of surveillance was the telephone wiretap. Currently, the most common form of surveillance is the electronic wiretap, which includes eavesdropping on devices such as digital display pagers and e-mail accounts. Id. at 10.

[22] *See* Neil King, Jr. and Ted Bridis, *FBI's Wiretaps to Scan E-Mail Spark Concern*, WALL ST. J. (July 11, 2000) at A3.

[23] *See* Testimony of Dr. Donald Kerr, Hearing of House Subcommittee on the Constitution on ‹‹Fourth Amendment Issues Raised by the FBI›s ‹Carnivore› Program›› (July 24, 2000), at 13 (‹‹A number of those [applications of Carnivore] were simply pen registers and some involved full content.››).

[24] *See id.* (‹‹[Carnivore] has been used in 6 criminal cases and 10 national security cases [to date]. A number of those were simply pen registers and some involved full content.››). Congress recently enacted legislation that requires future public reporting of the numbers of pen register or trap and trace orders directed at ISP›s by the Department of Justice. Under 18 U.S.C. 3126(4), the Attorney General must report annually to Congress the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice, which reports must include information concerning ‹‹the number and nature of the facilities affected,›› presumably requiring an indication of when such devices are installed at ISP›s, as opposed to telephone companies.

[25] The Pen Register Statutes do not provide for the notification of those information regarding whom has been disclosed pursuant to an order issued under the Pen Register Statutes.

[26] Written Testimony of Robert Corn-Revere to House Constitution Subcommittee (April 6, 2000), at 25. This interpretation of federal authority under the pen register and trap and trace statutes was reiterated by David Green, Deputy Chief, Computer Crime and Intellectual Property Section of the Computer Crimes Division of the Department of Justice, at the April 6, 2000 hearing before the Subcommittee on the Constitution:

> Mr. CANADY: ... Does the Pen Register Act apply to e-mail or other Web-based communications? If so, what are the things to be recorded that identify the numbers dialed _ that is, language from the Pen Register Act _ or identify the originating number of the device from which communication is transmitted?
>
> Mr. GREEN: We do view e-mail as subject to a pen register and trap and trace. In fact, we use it all the time in investigation of hacking cases, child porn cases, Internet fraud cases ...
>
> Mr. CANADY: ... Do you think the Pen Register Act is sufficient to deal with the current technology or not?
>
> Mr. GREEN: ... One, the _ certainly the language of the Pen Register _
>
> Mr. CANADY: Identify the number dialed?
>
> Mr. GREEN: Right.
>
> Mr. CANADY: You are extrapolating from that to the e-mail address?
>
> Mr. GREEN: And that has raised litigation concerns and certainly we would want that _ if the law is amended, we would want that to be clarified.

Oversight Hearing (Transcript) on ‹‹The Fourth Amendment and the Internet,›› (April 6, 2000), at 30-32 (emphasis added).

[27] Webster's Ninth New Collegiate Dictionary.

[28] Oversight Hearing (Transcript) of the House Constitution Subcommittee on "The Fourth Amendment and the Internet," (April 6, 2000), at 60.

[29] 18 U.S.C. 3127(3) defines the term ‹pen register› as a device which records or decodes information ‹on the telephone line to which such device is attached.›

[30] PRESTON GRALLA, HOW THE INTERNET WORKS, 13 (1999) (emphasis in original).

[31] 442 U.S. 735 (1979) (holding that the use of pen registers does not constitute a "search" within the meaning of the Fourth Amendment)

[32] *See* Proposed Legislative History, at 3 (stating that the proposed legislation "seek[s] to make the [Pen Register Statues] technology-neutral by removing words such as 'numbers ... dialed' that do not apply to the way that pen/trap devices are used, for instance, to trace communications on computer networks").

[33] Enhancement of Privacy and Public Safety in Cyberspace Act (emphasis added) at 17.

[34] 18 U.S.C. 3127(3).

[35] United States v. New York Telephone Company, 434 U.S. 159, 167 (1977) ("Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.").

[36] Proposed Legislative History, at 32-33.

[37] Example 3, attached to Written Testimony of Alan Davidson, Staff Counsel, Center for Democracy and Technology, provided to House Constitution Subcommittee in advance of Hearing on ‹Fourth Amendment Issues Raised by the FBI›s ‹Carnivore› Program› (July 24, 2000).

[38] The Federal Wiretap Act defines "interception" as an "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device." 18 U.S.C. 2510(4). Subsection 2510(8) in turn defines "contents" as "any information concerning the substance, purport, or meaning of [the] ... communication." 18 U.S.C. 2510(8).

[39] The CCIPS Guidelines model pen register application states: "Applicant requests that the Court issue an Order authorizing the installation and use of a pen/trap device to capture the packet header and mail header information (but not the subject lines of e-mails) associated with the transmission of communications and other data (including transfers of information via the World Wide Web ... [and] telnet ...) to and from the account [Jdoe@isp.com] ...." It is unclear whether such a pen register request anticipates government access to all addresses of particular Web sites visited by a suspect, or only to any Web site address that might be necessary in locating e-mail addresses associated with Web-based e-mail accounts, such as those made available by the hotmail service. Further, the use of services such as telnet requires that communications be directed at a particular Web site address rather than an e-mail address.

[40] 50 F.3d 285, 294 (4th Cir. 1995)

[41] *Id*. at n.11.

[42] 594 N.Y.S.2d. 701, 705 (N.Y. 1993). In People v. Kramer, 683 N.Y.S.2d. 743, 749 (N.Y. 1998), the Court of Appeals of New York elaborated that ‹Bialostok should be understood and applied as a more fact specific, adaptable legal guidepost for sophisticated modern technologies. It should require scrutiny and examination of the pen register technology as used in a given investigation and situation. The appropriate judicial assessment [regarding whether or not a warrant should be required for the use of a particular device] should include not only the capacity of the device used to intercept, hear and record communication, but the manner in which it does so and its susceptibility to evasion of statutory, precedential, and even constitutional protections.›

[43] 47 U.S.C. 1006(b)(2). Congress responded to technological developments in the telecommunications field by enacting the Communications Assistance for Law Enforcement Act of 1994. *See* Pub. L. No. 103−414, 108 Stat. 4279 (codified at 47 U.S.C. 1001−1010 and various sections of 18 U.S.C. and 47 U.S.C.). CALEA requires telephone companies to ensure that new technologies, and some old technologies, do not impede law enforcement interception of communications. *See id.* at 1006(a)(2). The legislation mandates that carriers must take steps to ensure that the broad technological trends in the industry do not eliminate law enforcement access to communications of targeted individuals.

[44] See United States Telecom Association v. Federal Communications Commission, 2000 WL 1059852 (D.C.Cir.), at *12.

[45] Government interceptions of the contents of communications, for example, require an intercept order issued pursuant to strict requirements. See 18 U.S.C. 2518(3) (requiring for a court order that ‹‹(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular [enumerated] offense ..; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; (d) ... there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person››).

[46] 2000 WL 1059852 (D.C.Cir.) at *12.

[47] *Id*. at *12.

[48] *Id*.

[49] It is unclear whether the CCIPS Guidelines model pen register application anticipates government access to passwords pursuant to a pen register order in certain circumstances. *See* commentary in note 15, supra.

[50] *See id.* at *16 (“[N]othing in the Commission's treatment of packetmode data requires carriers to turn over call content to law enforcement agencies absent lawful authorization. Although the Commission appears to have interpreted the [challenged standard] as expanding the authority of law enforcement agencies to obtain the contents of communications ... the Commission was simply mistaken ... CALEA authorizes neither the Commission nor the telecommunications industry to modify either the evidentiary standards or procedural safeguards for securing legal authorization to obtain packets from which call content has not been stripped, nor may the Commission require carriers to provide the government with information that is ‘not authorized to be intercepted.’”).

[51] *See* Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, Third Report and Order, 14 FCC Rcd. 16794, 16819 (“CALEA Order”) (adopting technical requirements for wireline, cellular, and broadband PCS carriers to comply with assistance capability requirements prescribed by CALEA).

[52] *Id.* at 16820.

[53] CALEA Order, at 16820.[53]

[54] *See* Report to the Federal Communications Commission on Surveillance of Packet-Mode Technologies, Joint Experts, Committee TR 45, Telecommunications Industry Association (September 29, 2000) (‹‹JEM Report››), at 10-11.

[55] Cover Letter, Matthew J. Flanigan, President, Grant Seiffert, Vice President, Government Relations, Telecommunications Industry Association, to William E. Kennard, Chairman, Federal Communications Commission (September 29, 2000), at 3 (‹‹Letter››).

[56] JEM Report, at 12.

[57] *Id*. at 12-13.

[58] Id. at 16.