8/9/2001

CARNIVORE: WILL IT DEVOUR YOUR PRIVACY?

Perhaps you have written an e-mail that looks something like this:

"Dear David, Have you heard the horrible news? Robert has been picked up again for cocaine. That's another parole violation for him, and I think we'll be losing him at work. I will get back to you on that important project we talked about; I am going to New York this weekend with Ben. Call me on my cell if you need me... (310) 555-2559. Calista"

Can you think of any reason justifying the FBI's access to this email? Assuming that Calista is not under investigation and there is no warrant allowing the FBI to intercept her communications, there simply is no compelling reason. Yet that is exactly what might happen if the FBI's newest cybercrime battling machine, Carnivore, is "tapped" into Calista's ISP.

Introduction

¶1 The Wall Street Journal broke the story of Carnivore a little more than a year ago[1] and since then there has been a swarm of controversy surrounding the program. One of the major reasons for the controversy is that the general public has no firm understanding of the capabilities of Carnivore. There is prodigious misinformation surrounding Carnivore, and the FBI refuses (for proprietary reasons) to release the source code.[2]

What is Carnivore?

¶2 From securities fraud to cyberterrorism, child pornography to espionage, electronic communication has become a major avenue for criminal activity. In response, the FBI developed Carnivore, a surveillance system that monitors electronic communication. With a court order or lawful consent from the Internet Service Provider (ISP), the FBI can tap Carnivore into an ISP's high-speed network. Aptly named Carnivore because of its ability to find the "meat," or criminal activity, in Internet traffic, it can track a user's incoming and outgoing e-mails. Information travels through the Internet in packets of binary code. In the case of e-mail, a single message is broken down into several packets. Every packet contains duplicate information such as, among other things, the address from which the e-mail was sent, the address to which it was sent, and the subject line. Each packet also contains unique information - a section of the e-mail's content.

¶3 Filtering the ISP's network traffic, Carnivore "sniffs" binary code - streams of 0s and 1s - looking for specific information. Detecting this information, Carnivore saves the packets of communication associated with the subject. The rest of the network traffic continues its path, unscathed by Carnivore. From the stored packets, Carnivore collects email content and transactional information, such as the user address, source, destination, date, time, and duration of the message.[3] Carnivore makes the saved, filtered information available to FBI agents. When the FBI attaches Carnivore to an ISP, it swims through a lake full of data searching for a very particular fish.

¶4 Depending on whom you ask, Carnivore is either a sharpened spear aimed directly for the target, or a giant net cast wide across the whole lake. The FBI champions Carnivore as a surgical tool, superior to any commercially available "sniffer."[4] Most commercial sniffers are sufficient for network administration but lack the flexibility and precision to meet legal and evidentiary requirements.

¶5 The FBI can tailor Carnivore's filtering system to collect only information authorized by court order. Carnivore appends each collection by noting the filter configuration during that search, for later reference by federal officials, a court, or defense counsel. Because the FBI can tailor the filtering process to meet the specific parameters of a court order, Carnivore is more flexible and effective than commercial sniffers. For example, if a pen register or trap and trace order authorizes collection of only transactional and addressing information, Carnivore can filter out any content of the message, including the subject line. Commercial sniffers are not sophisticated enough to do that automatically and require human screening of collected content. The FBI argues that this feature minimizes the involvement of FBI personnel in the filtering process and protects the privacy of email users.[5]

¶6 Critics of Carnivore see it in a different light. The technology of e-mail messages, they point out, creates two major privacy concerns. First, does Carnivore give the FBI access to more information than it legally and constitutionally ought to see? While telephone systems clearly distinguish between transactional data (e.g., the number dialed) and substantive data (e.g., the conversation), e-mail systems are not as straightforward. As described above, an e-mail message gets divided into multiple packets of data, each containing a header (the date, time, addresses of the sender and receiver, and subject line) and a piece of the substantive content. Transactional and substantive data are inextricably mixed in these packets.[6] To search substantive content, law enforcement officials must show probable cause and receive a court-ordered warrant. However, to search transactional information, law enforcement officials need no express authorization.

Thus, from a legal perspective, the data packet structure blurs the line between searches that require a warrant and those that do not.

¶7 The FBI claims its complex filtering system enables them to avoid the collection of unauthorized data. Despite assurances that the privacy of targeted users will be protected, it would be easy for the FBI to overstep its mandate when conducting one of these searches. Testifying before the House Judiciary Committee, ACLU leader Barry Steinhardt cautioned, "Carnivore gives the FBI far too much discretion and creates far too great a risk that it will burst through the envelope of the Fourth Amendment and the congressionally imposed restraints."[7]

¶8 The second primary concern is that the e-mail of innocent users, not under investigation, is subject to search. In a process known as "packet switching," e-mail data packets separate from each other at the point of origin and travel independently to the destination e-mail address, each packet taking the most efficient route at the time of transmittal. The entire message reassembles at the destination.[8] With many users sending messages at the same time, a large ISP carries billions of data packets traveling simultaneously. To identify data for a targeted subject, Carnivore must sniff every packet of data that travels on the network. In other words, 99.99999% of the information searched by Carnivore probably belongs to innocent users. The technology of packet switching... means that the data of the innocent are inextricably mingled with the data of the less innocent. A simple search to see if two people are e-mailing each other - which can be approved without a search warrant - requires that Carnivore digest the private correspondence of millions of people. This, of course, horrifies anyone concerned about Big Brother.[9] Privacy advocates are pushing for stricter controls on the use of Carnivore and for requiring greater burdens of cause before the FBI may employ Carnivore.

The Scope of the 4th Amendment - Then, and Now

¶9 In *Weeks v. United States*, the Court holds that police violate a defendant's Fourth Amendment rights by entering his room without his permission or a warrant, and taking possession of his property.[10] After *Weeks*, evidence gathered in violation of the defendant's Fourth Amendment rights is not admissible in court.[11]

¶*10* *Katz v. United States* expands Fourth Amendment protection to include much more than physical effects or mail.[12] The Court holds that "[t]he 4th Amendment protects people, not places."[13] A person's location is less relevant than their activity and subjective expectations. Technological innovations need Fourth Amendment protection to keep up with their rapid pace. The spirit of Fourth Amendment protection includes areas in which a person may have a

justifiable expectation of privacy.

¶11 The *Katz* Court developed a two-part test to determine whether an activity is protected from search. The first part asks whether the individual has exhibited an actual (subjective) expectation of privacy. The second part asks whether that expectation is one that society is prepared to recognize as reasonable. If both parts are answered affirmatively, *Katz* extends the protection of the Fourth Amendment to the individual and activity at issue. After *Katz*, a physical intrusion is not necessary for a search to violate the Fourth Amendment. A violation can occur without police rifling through file cabinets or even entering a house, as long as there is a reasonable expectation of privacy.

¶12 In *United States v. Miller*, the Court holds that there is no realistic expectation of privacy in records that one willingly hands over to a bank.[14] Bank customers know the records will be handled by multiple employees, and perhaps seen by others. Checks, for example, are routinely seen by several parties when used for business. While the records in question were tangible items, Miller did not have possession of them at the time of their seizure. Having given them to a third party like the bank, it became unreasonable for him to expect those records to stay private.

¶*13* *Smith v. Maryland* is the first case involving a pen register.[15] A pen register records the numbers dialed from a telephone. It records only numbers; it is unable to record the substance of the conversation or whether the call connected. The Court holds that people do not have a subjective expectation of privacy in the telephone numbers they dial. They are aware that switching devices receive the numbers and connect them so that they can talk to the correct person. Before the advent of mechanical switching devices, people gave the number to an operator who physically connected the two parties via a switchboard. That, plus the itemized phone bills that show every call a consumer has placed, illustrates that even if a person has an expectation of privacy in the phone numbers he dials, society is not prepared to recognize that expectation as reasonable.

¶14 Today, cases like *Kyllo v. United States* illustrate the judicial recognition that as our technology changes, so will our definition of "search."[16] Even if the government refrains from physically touching a person's belongings, the Supreme Court has recognized that the taking of information may amount to the same kind of illegal search. "Where . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is

presumptively unreasonable without a warrant."[17]

¶15 Recent legislation in this area includes the Communications Assistance for Law Enforcement Act of 1994, 47 U.S.C. §1001. This Act, know simply as "CALEA," requires that communications providers implement certain technologies to enable them to assist law enforcement agencies with authorized searches. However, CALEA does not apply to "information services" like Internet Service Providers and email.[18]

Legal Analysis of Carnivore

¶16 Law enforcement agencies are not required to demonstrate probable cause when using a pen register (to record a telephone subscriber's outgoing telephone numbers) or trap and trace device (to record incoming telephone numbers).[19] The FBI developed Carnivore in order to emulate these devices for electronic communications.[20] Relying on *Smith* and subsequent congressional legislation, the FBI asserts that Carnivore's pen-mode should be subject to the same minimal legal restraints as these other devices.[21]

¶17 In *Smith*, the Court holds that if law enforcement conduct infringes upon an actual and reasonable expectation of privacy, it is a search under the Fourth Amendment.[22] Applied to telecommunications, the Court holds that there is no reasonable expectation of privacy for the digits of incoming and outgoing telephone calls.[23] This holding "serves as justification for the relatively low standard governing privacy protections for pen register and trap and trace devices."[24] As Alan Davidson, Staff Counsel for the Center for Democracy and Technology, commented, this approval standard is "so low as to be nearly worthless."[25]

¶18 The FBI asserts that obtaining e-mail addresses using Carnivore's pen-mode is similar to obtaining telephone numbers using a pen register or a trap and trace device.[26] Because the use of pen registers and trap and trace devices does not constitute a search under the Fourth Amendment, the FBI argues that the use of Carnivore's pen-mode does not constitute a search.[27] Evaluating Carnivore's constitutionality requires consideration of the FBI's analogy that e-mail addresses are like telephone numbers. If the analogy is accurate, it may not be necessary to examine the issue further; it is likely that the use of Carnivore will be found constitutional. If this analogy is *inaccurate*, a higher legal standard must be followed and Carnivore deserves a fresh review under *Katz*.

¶19 It is likely that the analogy is inaccurate because the operation of Carnivore in the online environment differs in significant ways from the operation of the pen register and trap

and trace device in traditional telephone systems. Although e-mail is often sent over telephone lines, Carnivore is installed on an ISP's data network, not a telephone line. Information that Carnivore can intercept is not limited to a suspected criminal's private telephone line, as with traditional devices. Instead, Carnivore searches an ISP's entire network, which includes the e-mail of thousands of the ISP's customers. This gives the FBI access to a much larger scope of information than available from a single phone line. Intentional or accidental collection of unauthorized communication by FBI personnel poses a potential threat to Fourth Amendment rights. IIRTI's independent review of the Carnivore system revealed serious concerns about the accountability of FBI agents using Carnivore. IITRI found that:

> "it is not possible to determine who, among a group of agents with the password, may have set or changed filter settings. In fact, any action taken by the Carnivore system could have been directed by anyone knowing the Administrator password. It is impossible to trace the actions to specific individuals." [28]

¶20 When the information-collecting capacity of the pen register is magnified by thousands, as Carnivore does, the full potential to track who communicates with whom becomes clear and such monitoring is seen for what it is: an invasion of privacy.

¶21 It is clear that the statutes governing the pen register and trap and trace device are intended to cover the physical connection to a telephone line and not connection to the Internet. Call routing information is separated from content in a telephone line, but the two are combined in packets used for e-mail transmission over the Internet. As a result, the privacy concerns raised in Carnivore are greater than those contemplated in *Smith*. First, the process by which individual e-mail addresses and telephone numbers are collected is significantly different. Pen registers do not copy the content of communications.[29] "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."[30] Carnivore's pen-mode, on the other hand, first copies everything that concerns the target, including the content of the target's communications, before each character of the content is replaced with an "X."[31] The content of communications clearly carries a reasonable expectation of privacy; does another person have to read the content to violate the sphere of "content?" What if, for example, private papers are taken, copied, and then put back without ever having been read? Is this not an invasion of privacy? If one agrees that it is, and the expectation of privacy in e-mail communication is reasonable, then it appears that Carnivore violates the protection afforded by the Fourteenth Amendment.

¶22 When replacing e-mail characters with Xs, Carnivore records the length of each field in a target's e-mail, including the subject heading and the body of the message itself, as a string of Xs.[32] Knowledge of the entire length of an e-mail is analogous to knowledge of the entire length of a telephone call, the latter being permissible under the pen-trap statute. However, knowledge of the lengths of individual fields in an e-mail has no pen-trap equivalent.[33] The length of each individual field can, to a certain degree, reveal the nature of the communication. Letters contained in an e-mail address also reveal more information than the digits in a telephone number.[34] Not only are the identities of the corresponding parties often revealed (*e.g.*, "john.doe@email.com"), but e-mail addresses can also reveal an individual's affiliation with an organization (*e.g.*, "john.doe@law.duke.edu" or "john.doe@aclu.org").

¶23 Since a person's expectation of privacy is likely to increase as more information about that person is collected, the potential for a "search" also increases.[35] Moreover, Internet and telephones naturally carry different expectations of privacy. The recording of transactional information by telephone companies is a central reason the Supreme Court in *Smith* holds that there is no expectation of privacy in telephone numbers dialed and received. In the context of the Internet, there is no such recording of transactional information. ISPs merely provide an access point to an untended pipeline.

¶24 Although the FBI tries to re-assure skeptics that Carnivore will not be used to retrieve more information than is authorized because of its internal procedures, system safeguards, and the potential for civil and criminal penalties stemming from its misuse, Fourth Amendment principles require that the government's promises not be accepted without scrutiny.[36] As Barry Steinhardt, Associate Director of the ACLU, has pointed out, the FBI has failed in recent years to respect the agreements it has made with Congress to impose limitations on its own law enforcement capabilities.[37]

¶25 There is some indication that courts are moving toward a higher legal standard for electronic communications. The United States Court of Appeals for the District of Columbia recently held that the Fourth Amendment protects dialed digits that convey content.[38] This decision supports the assertion that e-mail addresses convey content protected by the Fourth Amendment. Taking this protection into account, Carnivore should be subject to a heightened legal standard.

Conclusion

¶26 Returning very briefly to the e-mail excerpt discussed in the Introduction, one must consider the reasons for the FBI's access to that email. Compelling reasons are difficult to find. The writer obviously had an expectation of privacy, as she discussed her work, travel plans, and even revealed her private phone number. Courts would likely find that her expectation is reasonable, at least as reasonable as Katz's expectation of privacy in a public phone booth. Should the FBI have access to all of this personal information simply because she used the word "cocaine" in her email?

¶27 If Carnivore is tapped into her ISP, and programmed to search e-mail text for the word "cocaine," it is not only possible that the FBI will read her e-mail, it is guaranteed. IIT's independent tests proved that Carnivore can successfully search the text of e-mails for specified keywords.[39] Keep that in mind next time you share the news of the day, be it domestic terrorism or celebrity drug use, with friends and family. The intended recipient may not be the only person reading your e-mail.

Authors: :Joseph Goodman

Angela Murphy

Morgan Streetman

Mark Sweet

Footnotes

1. Neil King, Jr., *FBI's Wiretaps to Scan E-Mail Spark Concern*, Wall St. J., July 11, 2000, at A3.

2. IIT Research Inst., *Independent Technical Review of the Carnivore System, at* http://cryptome.org/carnivore-rev.htm#1 (last visited August 7, 2001).

3. 3 *See Carnivore Diagnostic Tool: Statement of the Rec. Before the Senate Comm. On the Judiciary*, (2000) [hereinafter FBI Statement] (statement of Donald M. Kerr, Assistant Director, Laboratory division, Federal Bureau of Investigation), *available at* http://www.fbi.gov/congress/congress00/kerr090600.htm. (last visited August 7, 2001).

4. Id.

5. Id.

6. *Alan Charles Raul*, Should You Fear the Carnivore?, *Business 2.0, Nov. 2000.*, at http://www.business2.com/articles/mag/0,1640,8545,00.html(last visited August 7, 2001).

7. The Fourth Amendment and Carnivore Before the House Judiciary Committee Subcommittee on the Constitution, *106th Cong., at* www.house.gov/judiciary(2000) (last visited August 7, 2001) *(statement of Barry Steinhardt, Assoc. Dir. Am. Civil Liberties Union).*

8. *Raul*, supra *note 4.*

9. Id.

10. *232 U.S. 383 (1914).*

11. *Olmstead v. United States*, 277 U.S. 438, 462 (1928).

12. 389 U.S. 347 (1967).

13. *Id.* at 351.

14. 425 U.S. 435 (1976).

15. 442 U.S. 735 (1979).

16. 121 S. Ct. 2038 (2001).

17. *Id.* at 2046.

18. 47 U.S.C. §1001(8)(C)(i), §1002(b)(2)(A); *U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 455 (D.C. Cir. 2000).

19. 50 U.S.C. §1801-1811.

20. *See Fourth Amendment Issues Raised by the FBI's Carnivore Program: Oversight Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong., *at* http://www.house.gov/judiciary/davi0724.htm (2000) (last visited August 7, 2001) (testimony of Alan B. Davidson, Staff Counsel for the Ctr. For Democracy and Tech.).

21. *See Carnivore Diagnostic Tool: Statement of the Rec. Before the Senate Comm. on the Judiciary*, (2000) [hereinafter *FBI*] (statement of Donald M. Kerr, Assistant Director, Laboratory division, Federal Bureau of Investigation), *available at* **http://www.fbi.gov/congress/congress00/kerr090600.htm.** (last visited August 7, 2001).

22. *Smith v. Maryland*, 442 U.S. 735, 739 (1979).

23. *Id* at 743.

24. Johnny Gilman, Comment, *Carnivore: The Uneasy Relationship Between the Fourth Amendment and Electronic Surveillance of Internet Communications*, 9 CommLaw Conspectus 111, 118 (2001) (citations omitted).

25. *See Fourth Amendment Issues Raised by the FBI's Carnivore Program: Oversight Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong., *at* http://www.house.gov/judiciary/davi0724.htm (2000) (last visited August 7, 2001) (testimony of Alan B. Davidson, Staff Counsel for the Ctr. For Democracy and Tech.).

26. *See Carnivore Diagnostic Tool: Statement of the Rec. Before the Senate Comm. on the Judiciary*, (2000) [hereinafter *FBI*] (statement of Donald M. Kerr, Assistant Director, Laboratory division, Federal Bureau of Investigation), *available at http://www.fbi.gov/congress/congress00/kerr090600.htm*. (last visited August 7, 2001)

27. *Id.*

28. IIT Research Inst., *Independent Technical Review of the Carnivore System*, *at* http://cryptome.org/carnivore-rev.htm#1 (last visited August 7, 2001).

29. *See Smith*, 442 U.S. at 741.

30. *Id.* citing *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977).

31. IIT Research Inst., *Independent Technical Review of the Carnivore System*, *at* http://cryptome.org/carnivore-rev.htm#1 (last visited August 7, 2001).

32. *Id.*

33. *Id.*

34. *See The Fourth Amendment and Carnivore Before the House Judiciary Committee Subcomm. on the Constitution,* 106th Cong., at www.house.gov/judiciary (2000) (last visited August 7, 2001) (statement of Barry Steinhardt, Assoc. Dir. Am. Civil Liberties Union).

35. *See Smith*, 442 U.S. at 741.

36. *See The Fourth Amendment and Carnivore Before the House Judiciary Comm. Subcomm. on the Constitution,* 106th Cong., at www.house.gov/judiciary (last visited August 7, 2001) (2000) (statement of Barry Steinhardt, Assoc. Dir. Am. Civil Liberties Union) (the Fourth Amendment is built on the premise that "the Executive cannot be trusted with carte blanche authority when it conducts a search").

37. *See id.* (discussion of CALEA's implementation process and the FBI's attempts to gain capabilities under CALEA that it specifically promised Congress it would not seek).

38. *See United States Telecom Association v. Federal Communications Commission*, 227 F.3d 450 (D.C. Cir. 2000).

39. IIT Research Inst., *Independent Technical Review of the Carnivore System, at* http://cryptome.org/carnivore-rev.htm#1 (last visited August 7, 2001).