6 Va. J.L. & Tech. 10 (2001), *at* http://www.vjolt.net
Ó 2001 Virginia Journal of Law and Technology Association

VIRGINIA JOURNAL *of* LAW *and* TECHNOLOGY

UNIVERSITY OF VIRGINIA	SUMMER 2001	6 VA. J.L. & TECH. 10

Carnivore: US Government Surveillance of Internet Transmissions

E. Judson Jennings*

1 Introduction
2 Carnivore Overview
2.1 Carnivore Description
2.2 Technical Issues Unresolved by the Carnivore RFP
2.2.1 Scope of Surveillance
2.2.2 Security
2.2.3 Scalability of Carnivore
2.2.4 Evidentiary Issues With Carnivore
2.3 FBI Solicitation of External Review of Carnivore
2.4 Outside Review of Carnivore by IITRI
2.4.1 IITRI Carnivore Study
3 The Legal Context of Carnivore
3.1 Documents Held by Targets or Disinterested Third Persons
3.1.1 Privacy Protection Act
3.2 Interception of United States Postal Service Mail
3.3 Wiretaps
3.4 Electronic Communications Privacy Act [ECPA] (1986)
3.4.1 Control over Carnivore Applications

1 Introduction

1. Notwithstanding dire predictions, the year 2000 brought few disasters directly caused by technology.[1] The year 2000 did bring from the U. S. Federal Bureau of Investigation official disclosure of a technology project called Carnivore,[2] which enables properly authorized agents to utilize technology to intercept, filter, seize, and decipher digital communications on the information autostrada known as the Internet. Depending upon the precise manner in which this new technology is implemented, Carnivore may entail the compelled disclosure of encryption keys that could not be independently recovered. In any event, Carnivore will certainly intercept many millions of private communications among individuals who have violated no laws, and in many cases will obtain information about such individuals with neither their knowledge nor their consent. Since the Internet is global, many of these individuals will be citizens of other nations who have no physical presence in the United States.

2. In this paper, I will describe the technology of interception, filtering, and seizure, as implemented in Carnivore, in order to develop an appreciation of what is possible. Next, I will examine the pertinent legal principles from the United States, which require an analysis of existing legislation, regulations, and guidelines, as well as of judicial decisions interpreting the Constitution's Bill of Rights. Finally, I will hazard some conjectures about the dangers and benefits that Carnivore presents for both individuals and for governments.

2 Carnivore Overview

3. Carnivore is a computer surveillance device system developed within the FBI that is installed and used together with a tap on the facilities of an Internet Service Provider.[3] The software program copies all data traffic on a particular internet server, and collects information about – and/or the content of – electronic mail or other digital communications to or from the specific users targeted in an investigation.[4] American courts have recognized that the government may, with proper authorization, seize documents, intercept mail,[5] and electronically intercept and record voice communications.[6] The United States Department of Justice has also issued guidelines for the search and seizure of computer evidence.[7]

4. From a theoretical standpoint, Carnivore represents only a small advance in this type of surveillance, in that it extends these techniques to the Internet by enabling authorized investigators to intercept and copy electronic data communications. The apparent similarity between Carnivore and its forebears is, however, superficial. When mail is intercepted, agents must physically separate envelopes or packages with addresses that meet the seizure criteria, and they generally do so at the appropriate local post office.[8] Wiretaps[9] are among the most expensive and labor intensive operations in all of law enforcement; the government must carefully evaluate wiretap projects from the fiscal, tactical and the legal standpoints.[10] Moreover, wiretap agents must, under American law's minimization requirement, monitor all wiretaps in real time and must immediately terminate surveillance of any intercepted communication that does not involve the authorized target.[11]

5. The Carnivore process, unlike its ancestors, is highly automated in several important ways. First, Carnivore necessarily intercepts huge amounts of information from myriad sources unconnected to any investigation: Carnivore monitors and copies virtually all of the data flowing through the channel during the period of surveillance.[12] While the Carnivore software will filter out the vast majority of this information immediately because it fails to meet the surveillance criteria, this filtering is merely optional from a technology standpoint. Moreover, when intercepted information does match the filtering criteria, it is then automatically captured and stored on the Carnivore system, even though the filtering criteria may have been entered in error. Any further removal of irrelevant or improperly seized information depends upon review and decisions by a human agent. [13]

6. Carnivore is an existing system based upon technology – described below – which is not terribly sophisticated. [14] According to a prominent member of the computer security industry, the FBI claims to have used Carnivore in approximately twenty-five investigations prior to August, 2000; the majority of the cases are said to have involved counter terrorism, although drug trafficking and computer hacking were also mentioned.[15] The potential efficacy and pervasiveness of this surveillance technology raises fundamental social concerns, chief among them is whether Carnivore is effective in accurately capturing authorized information while at the same time containing safeguards against the inadvertent collection of unauthorized information, abuse by government agents or private interests, and compromise by detection or manipulation by the targets of the investigation or third party hackers. After the Electronic Privacy Information Center (EPIC) filed suit in July, 2000, under the Freedom of Information Act seeking all government documents discussing Carnivore and its use by the FBI, the agency agreed in August, 2000, that it would provide more information about its existing use of Carnivore, including the data obtained and the details of the investigations. However, this process failed when EPIC objected to the proposed FBI timetable, and the agency sought to have the action dismissed.[16]

7. At the same time, in order to allay, or perhaps deflect, growing public concern, the FBI commissioned a private sector study of Carnivore, which was completed in December, 2000, by the IIT Research Institute and the Illinois Institute of Technology Chicago Kent College of Law [IITRI]. In order to understand why the Carnivore system necessarily entails the elements outlined above, I will examine the Carnivore technology as described in the FBI's solicitation and the IITRI report. This examination will first address only technology issues, and will assume that appropriate legal authorization has been obtained for the operation in question. In subsequent sections, the legal principles affecting the propriety of Carnivore surveillance will be described and analyzed.

2.1 Carnivore Description

8. The efficiency of any complex network is based on topology: there are many routes by which data can travel from one point to another. The flow of traffic improves when data is sent over routes which are the shortest and most lightly traveled, and when retransmission of data due to errors is minimized. The superior efficiency of digital networks like the Internet is in large measure based upon the discovery that network traffic flows much better if each transmission is divided into many small packets, which can follow different routes and be reassembled at the destination.[17] A single communication is broken into many smaller packets, each of which bears a "header," i.e., the information required to properly route, validate, and prioritize that packet.[18]

9. Thus, the Internet is literally built upon computers programmed to read and interpret packet headers. Carnivore is fundamentally based upon a "packet sniffer," which is a computer placed near a switching point on the network and programmed to intercept and examine all of the packets that go by. In order to reduce the potential for delay or disruption of network traffic inherent in this process, Carnivore creates a copy of all of the data that flows through the system at the intercept point, and processes the copy rather than the original.[19] The FBI has taken pains to emphasize the passive and non-intrusive structure of Carnivore.[20] However, as the FBI itself has stated, "Carnivore *chews* all the data on the network, but it only actually *eats* the information authorized by the court order."[21] The FBI contends that Carnivore should be viewed as analogous to a passive wiretap that does not interfere with communications.[22] But a mail seizure or a wiretap touches only upon communications directly involving the target of the investigation,[23] while Carnivore starts by copying everything in the pipe, in much the same fashion as the Echelon program by which the NSA and MI6 monitor all wireless communications. The American Civil Liberties Union has categorized Carnivore as a general search that clearly violates the Fourth Amendment.[24]

10. The Carnivore architecture has been portrayed by the FBI in the following diagram:

[25]

11. As Carnivore creates a full copy of the data stream, the next step in the process is to filter the data so that only packets that are identified as being part of a transmission involving the target are actually copied for review by the investigators. This is accomplished by instructing the computer to examine the information contained in each packet's header to ascertain from whom the packet originated and to whom it is addressed.[26] This function is specified by the FBI solicitation for the external Carnivore review in the form of the following algorithm:[27]

For all Packets sent to port 25				
	If Data starts with "MAIL FROM" or "RCPT TO"[28]			
		Compare the e-mail address against the court-authorized e-mail address		
			If the e-mail addresses match	
				Start collecting this session (IP to/from, port to/from)
				Save the raw packets
Next Packet				

12. The algorithm is simple and straightforward; its power derives from its ability to be executed at great speed for long periods of time without human intervention. The working Carnivore model which the FBI provided to IITRI for evaluation requires only standard, readily available "commercial off the shelf [COTS]" equipment:

    - The computer is a PC with a Pentium III processor, 128 megabytes RAM and a 4-18 gigabyte fixed disk drive.[29]
    - The Operating System (OS) is Windows NT, which is the standard Microsoft product for network servers and workstations.[30]
    - The filtering application software was written in C++, a common and widely used programming language that produces efficient code.[31]
    - The filtered data is written to a Zip drive, which employs removable disks that hold approximately 250 megabytes of data.[32] The FBI anticipates having its agents manually retrieve and replace the removable disks on a daily basis. Captured data can be saved to any valid drive path, so that the use of the Zip drive instead of a much larger fixed disk drive is purely optional.[33]

13. A Carnivore installation, then, consists of a single PC (which may be a laptop). The network cable that links an ISP's hub or switch to another component is unplugged and plugged into a tap hub which routes data to the Carnivore computer.[34] Both the FBI and the IITRI evaluators take pains to emphasize that data is not actually routed away from the ISP's normal pipeline, but is merely copied as it passes the tap point. This emphasis may have either a technical or a legal genesis.

14. From a technical standpoint, the contention is that Carnivore will not disrupt Internet traffic because it never diverts that traffic, but only copies it. At least one large ISP begs to differ; Earthlink reportedly has issued this official stance on Carnivore:

15. > We do not allow the installation of Carnivore on our network because it has the potential to compromise the privacy of our legitimate users and the performance of our network. We have an internal solution which allows us to comply with court orders without the presence of government personnel or equipment in our buildings. The government accepts this solution since they still receive the requested information about the criminal suspect, and we sleep well knowing that our customers are safe from unauthorized surveillance.[35]

16. From a legal standpoint, the FBI may be preparing to argue that Carnivore taps are "passive wiretaps" which do not entail actual interceptions, but merely retrieve electronic data.[36] The significance of that claim, which potentially vitiates the exclusionary rule in Carnivore situations, is discussed below. In any event, the Carnivore system consists entirely of cables, the tap and its hub, and the Carnivore PC with a fixed disk hard drive and a removable disk Zip drive.

17. Carnivore can be used as either a content wiretap[37] or as a pen trap.[38] The traditional wiretap typically has an actual eavesdrop van parked in the street, and the recorder must be turned off if the call involves someone other than the target. The Carnivore equivalent is the content of all e-mails sent to or received from the authorized target address, or all electronic data flows involving that address, which may consist of data files, program files, messages, or even keystrokes being entered by a hacker.[39] The traditional pen/trap records telephone numbers calling or being called by the target. The Carnivore equivalent records everyone who FTP's a certain file, accesses a certain web page, reads a certain newsgroup, connects to a certain chat room, or transmits keystrokes.[40]

2.2 Technical Issues Unresolved by the Carnivore RFP

18. The purpose of the FBI in issuing the RFP was not to solicit technical information or advice regarding how to build or improve the Carnivore device, but rather to allay concerns about the scope of Carnivore surveillance, the potential for abuse, breaches of security, and interference by hackers. Although the entire project was explicitly given the label "technical review," the IITRI report devotes considerable space to analyzing the practices, policies and controls on FBI personnel,[41] as well as to a discussion of the legal context in which Carnivore operates.[42]

2.2.1 Scope of Surveillance

19. The greatest concern is the scope of a Carnivore operation. Since the initial input to the system is a full copy of all of the data that is flowing past the tap point on the ISP's services, Carnivore is in principle capable of searching through that data in order to find particular names, or key phrases such as "nuclear bomb." The FBI has strenuously rejected this characterization of Carnivore, and maintains that the technology is carefully designed to preclude such a general search. The agency acknowledges that "packet sniffers" which can perform that function are already on the market, but insists that Carnivore has been designed to *automatically* prevent this from happening by structuring the software in a particular way. As the agency states:

20. > [Carnivore] does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user.[43]

21. IITRI, however, reports that although the Carnivore software is normally configured to retain initially only packets which come from or are addressed to a target address before any content based criteria are added, [44] this is not a required parameter: [45]

22. > If IP filtering is not turned on, all packets that pass the other filters are collected regardless of what IP address those packets may have.[46]

23. In fact, Carnivore appears to have an inherent design defect that will be very difficult to overcome, and which if uncorrected will lead to broader seizures. As IITRI reports, Carnivore can be configured to filter for IP packets that involve a particular IP or Mail address and which also contain specified text strings. However, because the address filter is applied at the application level, while the text search is applied at the driver level, a search keyed to a particular email address ignores the text filter. IITRI concludes:

24. > If a court order were to specify that the FBI could only collect e-mail messages of a particular subject [target] that contained a particular text string, the FBI *would not be able to use Carnivore to obtain that data.*[47]

25. If content intercepts must obey the minimization rule, then Carnivore appears incapable of functioning within the bounds of the law.[48]

2.2.2 Security

26. A Carnivore intercept poses two important security risks. The first, of course, is the security of the Carnivore device itself, since clearly both random hackers and investigative targets would have great incentive to monitor and/or sabotage the operation. The second security threat is to the ISP where the system is mounted.

27. Carnivore contains numerous security features, including NIC hardware authentication, and a network isolation device, which together preclude the ISP or a hacker from accessing the device without leaving obvious signs of damage, and which prevent the Carnivore box from transmitting if a hacker compromises the security.[49]

28. Although the system is protected by physical locks, it has a wide open back door. As IITRI reports:

29. > The collection computer is installed without a keyboard or monitor and, in operational use, Carnivore might not be physically accessible to case agents. However, each Carnivore computer is equipped with an off-the-shelf 56-kbps modem allowing it to communicate via a standard analog link.

30. Once Carnivore has been installed at the ISP, it is normally controlled remotely.[50]

31. Dial-up access poses a major security threat. In fact, Intel announced on January 4, 2001, that it was forthwith withdrawing all of its dialup VPN products.[51] One important security function of Carnivore is to maintain a clear separation between the case agent, who manages the overall investigation, and the Technically Trained Agent [TTA], who installs and programs Carnivore. However, IITRI also reports that although the Carnivore user screens employ additional password protection for changing the filter criteria, this password is embedded in the system and can thus be easily hacked.[52]

32. Another security concern is the Carnivore source code. The FBI has refused to release the source code, and in fact did not include it in the IITRI evaluation package. The FBI's reasons for not releasing the source code include concern about hackers, contract restrictions from software vendors, and 18 USC § 2512, which prohibits distribution of devices designed to do communications eavesdropping.[53] Industry spokespersons have rejected these contentions, stating that hackers will face no greater challenge from Carnivore than they have from such other security issues as PGP, anonymous remailers, and anonymizing services.[54]

2.2.3 Scalability of Carnivore

33. Carnivore is routinely characterized as a small part of the FBI surveillance system. The FBI states that as of August, 2000, it had only about two dozen units, stored securely in Quantico, Virginia, except when actually being used for an intercept. One FBI agent has told Congress:

34. > Now . . . it is important that you understand how Carnivore is used in practice. First, there is the issue of scale. Carnivore is a small-scale device intended for use only when and where it is needed. In fact, each Carnivore device is maintained at the FBI Laboratory in Quantico until it is actually needed in an active case. It is then deployed to satisfy the needs of a single case or court order, and afterwards, upon expiration of the order, the device is removed and returned to Quantico.[55]

35. Carnivore is rarely placed on ISP backbones; instead it is placed close to the servers they monitor.[56] Carnivore is designed only for "surgical" taps, not widespread monitoring.[57] Moreover, the system is too small to engage in broad intercepts. However, as with any computer system, this initial prototype could easily be expanded to provide enormous additional capacity without the addition of extensive or expensive resources, and Congress has a responsibility to monitor and potentially audit the Carnivore operation.

2.2.4 Evidentiary Issues With Carnivore

36. The FBI has also reported to Congress that Carnivore is needed to satisfy evidentiary concerns:

37. > Rule 901 of the Federal Rules of Evidence requires that authentication of evidence as a precondition for its admissibility. The use of the Carnivore system by the FBI to intercept and store communications provides for an undisturbed chain of custody by providing a witness who can testify to the retrieval of the evidence and the process by which it was recorded. Performance is another key reason for preferring this system to commercial sniffers. Unlike commercial software sniffers, Carnivore is designed to intercept and record the selected communications comprehensively, without "dropped packets."[58]

38. While Carnivore may satisfy evidentiary requirements regarding the accuracy and integrity of its operation, it cannot address the broader problems inherent in the somewhat uncivilized and uncontrolled community of the Internet. As a practical matter, e-mail can easily be forged, and fraudulent e-mails of this sort are common. Indeed, with a modicum of effort, anyone can originate email from another person. There are Trojan Horse applications, which not only forge e-mail, but make that e-mail "come from" the victim's IP address.[59]

2.3 FBI Solicitation of External Review of Carnivore[60]

39. The FBI's solicitation document, which was released in the summer of 2000, focused on four major areas of concern:

    1. Does the Carnivore system currently used by the agency collect all of the proper data specified in the legal authorization for the interception, while excluding all unauthorized data? [Efficacy 1]
    2. Does Carnivore compromise the operation of the ISP whose facilities host the system? [Disruption]
    3. Does Carnivore reduce the risk that unauthorized data will be collected by FBI personnel? [Efficacy 2]
    4. Is Carnivore sufficiently secure against both improper collection of data by third parties and efforts to interfere with the operation of the system by third parties? [Security][61]

40. The solicitation was ostensibly confined to technical issues. Thus, implicit in the first efficacy issue[62] is the assumption that the interception has been properly authorized, and its precise scope properly defined, in the legal authorization for the operation. Also the first efficacy issue assumes that Carnivore has been fully and properly programmed by the technical personnel responsible for the interception. The nature of this latter assumption flows from a consideration of the second efficacy issue, whether Carnivore reduces the risk of unauthorized collection. This issue clearly recognizes that the system is subject to human as well as machine error, and presents two types of questions. First, does Carnivore contain sufficient checks and audits of the technicians' actions to lower the chance that their inadvertent errors will cause unlawful interceptions? Second, given that Carnivore has some serious flaws, is it an improvement over commercially available packet sniffers that indiscriminately intercept and record internet transmissions?

41. The question of disruption had already surfaced when the Carnivore study was commissioned. At least one ISP had reported that a Carnivore installation had compromised its operations,[63] and the FBI was clearly sensitive to the potentially devastating adverse publicity that would result if one of its operatives completely brought down a network segment. Indeed, the FBI has procedures that grant ISPs the option of furnishing the required information in some other way in order to avoid a Carnivore tap. However, as discussed below, that alternative depends both upon the resources of the ISP and the willingness of the investigators to reveal the precise parameters of the intercept authorization.

42. The final issue, security, voices the hope that law enforcement can somehow stay one step ahead of the hacker community in this area. Given the primitive nature of the tested prototypes and the very limited use of Carnivore up to this point, it seems that the inclusion of the security issue was more an acknowledgment of vulnerability than an expression of confidence. The IITRI report bears out this interpretation.

2.4 Outside Review of Carnivore by IITRI

43. In several press releases the FBI specified that the technical review was to be conducted by a "major university."[64] However, the FBI solicitation included several important restrictions on the information it would make available, the furnishing of full source code, the issues that could be raised in the study, and the right to release the report to the public. These restrictions led several respected institutions to decline to submit proposals, which further inflamed public opinion regarding the integrity and credibility of the project. On September 26, 2000, the FBI announced that it had awarded the technical review project to the Illinois Institute of Technology Research Institute [ITTRI], one of eleven groups that had made submissions.[65] The reaction to the selection by the information technology community was immediate and vociferous. The FBI released the proposal submitted by the IITRI group together with the announcement of their selection, but initially redacted the names of the principal investigators. In only 24 hours, a full version of the report was made public after the FBI's insecure method of censoring PDF files had been breached and the missing names recovered from the published document.[66] There were claims that the principal investigators had close ties with the federal law enforcement and surveillance communities.[67] In addition, Network Ice used the FBI solicitation document together with other information to create Altivore, which it claimed performed all of the functions of Carnivore, and which was published in the public domain.[68]

2.4.1 IITRI Carnivore Study

44. The study was completed on December 8, 2000, and immediately published, with some redaction, on the FBI web site. The scope of the report was carefully circumscribed at the outset:

> In conducting the evaluation of Carnivore, IITRI considered concerns voiced by many parties. However, there are two fundamental concerns IITRI felt it could not address:
>
> (1) the constitutionality of collection performed by Carnivore and
>
> (2) whether or not agents of the government can be trusted to follow established procedures.
>
> The evaluation reveals how Carnivore performs a court-authorized search; it cannot address whether such an authorization should be made. The evaluation also addresses whether weaknesses in the technology, implementation, and procedures associated with Carnivore might facilitate agent error or misbehavior.[69]

45. The reporters also stated that they had minimized their interpretive evaluations, concentrating instead on providing objective data to be reviewed and interpreted by others:

46.

> Motivated by a broad concern for privacy, the purpose of this report is to provide the information needed for any individual or organization to make an independent judgment about Carnivore. To this end, IITRI set two objectives: (1) answering the four specific questions posed by the DOJ in its Statement of Work and (2) conveying an understanding of the system and its use.[70]

47. The IITRI conclusions were mixed. On two issues, the report was positive: the evaluators concluded that "the current system of external and internal controls makes it unlikely that either FBI or ISP personnel will use Carnivore carelessly or for improper purposes,"[71] and that "Carnivore cannot place an additional load on the ISP network, nor can it alter or otherwise compromise operations."[72] However, these conclusions must be understood in the context of the testing methods employed. The study did not take place at an actual Internet Service Provider facility, did not utilize an actual electronic surveillance authorization, and did not process actual communications. Rather, the evaluators set up a test bed facility at IIT, which was isolated from the normal network, contained a very small number of PC workstations together with a mail server and hubs, and processed dummy messages generated by a simple script written for the experiment.[73]

48. Although the FBI solicitation had disclosed some basic information about Carnivore, the IITRI report provides the first clear look at the system. Both the FBI and the study team emphasize that Carnivore is built largely with COTS components: Pentium PC,[74] Windows NT,[75] Jaz Zip Drive,[76] and a generic NIC, an application written in C++.[77] Moreover, the full package, which the agency calls "DragonWare suite," is comprised of the Carnivore components, supplemented by two other COTS products: Packeteer, which reassembles individual packets into full messages or files; and CoolMiner, a browser which makes the reassembled files readable.[78]

49. The first impression created by this technical description is that Carnivore is a fairly modest bit of technology, which can perform its functions only if it is strategically placed at specific locations on the Internet, is innocuous and not invasive, and comes away with only small bits of information, enough to fit on a removable disk. However, upon reflection, it becomes apparent that Carnivore is a mere prototype, and could very easily evolve with great speed into a system with enormous capacities for data monitoring. It is disturbing that the IITRI study, with its focus on technical issues, did not consider the strong likelihood that it was looking at the cub rather than the fully mature creature.

50. Moreover, although this study was carefully defined as a technical review both in the FBI solicitation and in the study itself – as quoted earlier – the document contains a substantial discussion of the current FBI procedures for Carnivore.[79] Thus we learn that, consistent with procedures in other technical surveillance situations, an investigation is started and managed by a case agent, who, after determining that electronic surveillance may be needed, contacts the Chief Division Counsel [CDC] and a TTA in the field office.[80] If the Carnivore operation entails electronic wiretapping for content, there are specific approval requirements set forth in the MIOG.[81] If the operation will merely track the source and destination of electronic transmissions, then the case agent need only justify in writing the need for pen-trap surveillance instead of conventional techniques.[82] Thereafter, an application is filed with the court, which then issues two orders. The first authorizes the intercept. The second, containing much less information, orders the ISP to cooperate.[83]

51. When the ISP receives the order, agents will discuss possible ways of obtaining the required information without a Carnivore installation. If those efforts fail, the TTA is responsible for deploying the Carnivore installation. The study notes, somewhat cryptically:

52. > Given that use of Carnivore has been limited, highly trained personnel from FBI Headquarters have, *so far*, played a critical role in the implementation process, *although there is no procedural requirement for their participation.*[84]

53. After the Carnivore system is installed, the TTA must then use the input screens to enter the criteria set forth in the intercept order. These criteria will generally fall into two groups. The first group is the IP address of a particular computer or computers. Although millions of computers may be logged onto the Internet at any one time, each one has a unique numeric address by which it can be identified. Users who access the internet by means of a dialup connection or through a network gateway may have an IP address dynamically assigned for each individual session,[85] which in turn may complicate the process of programming.[86] The second group of Carnivore criteria consists of identifying names in the address fields of communications, such as the "To:" and "From:" fields of an e-mail. This step is vitally important to the integrity of a Carnivore operation. If the agent who enters the criteria into the Carnivore system at this point either deliberately or inadvertently varies the input from that contained in the intercept order, then the data retrieved will not comply with that order or, alternatively, will not fulfill the purposes of the order. As the evaluators note, although the session parameters are saved for subsequent review, "… the potential for human error cannot be discounted – agents must program Carnivore to match the potentially ambiguous information in the court order."[87] The study also describes several "substantial precautions" that are taken to keep ISP personnel away from the hardware. This is important because, as they note:

54. If individuals, despite the precautions, could access the information released by Carnivore, they could reassemble it using readily available software to reveal its contents. [88]

55. Once the system is set up and running properly, the TTA removes himself from the investigation. This is very different from a telephone wiretap. Under agency procedures and the statutory requirements of Title III, a telephone wiretap must be actively and continuously monitored in order to insure that only authorized communications are being intercepted. If an agent hears a telephone conversation that does not involve an authorized target, the recorder must be stopped and restarted only after intermittent periodic surveillance indicates that traffic involving a target has again begun. With Carnivore, "the TTA does not receive any of the information retrieved via Carnivore."[89] Rather, the case agent periodically receives Zip disks containing the intercepted data. Depending upon the amount of data being recorded, a Zip disk could fill up in a matter of hours or even minutes. In any event, it is the case agent who utilizes the DragonWare suite to actually review the data on the disk:

56. On a PC on which DragonWare is installed, the agent determines which information is relevant and which is not. The irrelevant information is deleted immediately and no copies are kept.… *There are no checks of which IITRI is aware to monitor the extent of this second minimization.*[90]

57. Thus, the Emperor has no clothes! While the FBI has claimed that it has designed a system which is carefully programmed to recover exactly the information authorized by a content intercept court order, the reality is quite different. First, the TTA who enters the criteria into the Carnivore software must rigorously and exactly follow the terms of an unambiguous order, or the system will either retrieve unauthorized information or fail to achieve its purpose. Second, fully recognizing that Carnivore will produce only a haystack and not the needles, the FBI's system depends essentially on a case agent who will "immediately" review several hundred megabytes of data,[91] determine which information is "relevant," and permanently discard the rest. Does the term "relevant" apply to the criteria of the order, or to the crime for which the order was obtained, or to any crime? Does it apply to exculpatory information? The study is silent on this point.

58. Finally, IITRI notes that the case agent must determine whether the information is encrypted and, if it is, what to do about it.[92] The tested version of Carnivore does not deal in any way with encrypted data. The FBI has a vision that Carnivore operations will become more productive when there is some legal compulsion upon ISPs and perhaps private individuals to supply encryption key information – the notorious back door – but it is anticipated that the proposal will take a purely legal approach, and will not involve the FBI or other agencies in increasingly futile efforts to decrypt files using technology.

3 The Legal Context of Carnivore

59. Carnivore is an enigma under American law. Both the courts and Congress have invested considerable effort in defining and regulating the recovery and interception of information. When the Fourth Amendment was added to the United States Constitution, the primary concern was that government agents would forcibly enter private homes to search for incriminating documents or contraband. During the nineteenth century, the Supreme Court recognized an extension of this constitutional protection to documents and materials in transit as first class mail. [93] In the twentieth century, both the Court and Congress grappled with the interception of conventional telephone conversations and the use of electronic devices to overhear conversations in private places.[94] Two decades later, these bodies confronted the interception of other (i.e., non-voice) transmissions of data on electronic systems.[95] At about the same time, both the Court and Congress attempted to balance the needs of government investigators against the interests of the news media.[96] And, like all governments, American law distinguishes between domestic investigations and those that involve the national security.[97]

60. When it comes to Carnivore, the first and most difficult task is the selection of an appropriate legal category for the activities that the operation entails, for Carnivore does intercept communications and seize documents. The Carnivore system arguably violates the prohibitions found in the Bill of Rights against unreasonable search and seizure and self-incrimination, and the guarantees of privacy and freedom of speech and the press. The complex and in some respects haphazard evolution of American law in all of these areas has now produced a body of inconsistent and overlapping legal principles which may affect the lawfulness of Carnivore. Since both the courts and the legislature have authority to define constitutional rights, these legal rules are derived from judicial decisions in some cases, and are contained in statutes and regulations in others. In this section we will examine the rules of law that have been applied to the major types of data flow: documents in the custody of a person other than the target of an investigation; documents and material carried as first class mail; verbal conversations carried by telephonic or other wire services; and documents and other data stored in electronic form.

3.1 Documents Held by Targets or Disinterested Third Persons

61. American law compels the delivery of documents to investigators by either subpoena or warrant. A subpoena requires the recipient to deliver documents in his control, and thus affords advance notice and an opportunity to contest the lawfulness of the request. A subpoena by its very nature, however, affords the recipient an opportunity to flee or to destroy, alter, or conceal the evidence. Accordingly, investigators much prefer the search warrant, which authorizes agents to proceed without advance notice and to enter both businesses and private homes to obtain the authorized materials. Since 1972, Federal Rule of Criminal Procedure 41(b) has provided that a search warrant may be issued for the seizure of "evidence" as well as any contraband or the fruits or instrumentalities of a crime.[98] "Evidence" includes any physical item that will aid in apprehending or convicting a person who has committed a crime, regardless of its admissibility at trial. [99] The Supreme Court has held that seizures of items as evidence are subject to a reasonable person standard, and not a test of whether the items are actually evidence after the fact.[100] Records containing information that reveal the criminal operation qualify for seizure,[101] as do records and documents that identify the occupant of a place connected to the crime and regularly used by more than one person,[102] or documents that incriminate co-conspirators.[103] Electronic surveillance is by definition a general search, not limited to specific objects, people, and places as required by the Fourth Amendment.[104]

62. A full content Carnivore operation involves the search for and seizure of documents in electronic form. Since the documents are in the custody of the ISP, such seizures are subject to federal regulations governing warrants directed to a disinterested third person.[105] These regulations require authorization by a government attorney for any application for a search warrant for documentary materials believed to be in the private possession of a disinterested third party, and also provide that no application for such a warrant should be made "unless it appears that the use of a subpoena, summons, request, or other less intrusive alternative means of obtaining the materials would substantially jeopardize the availability or usefulness of the materials sought."[106] The regulations also restrict the use of a search warrant to obtain materials in the custody of third persons if they contain information protected by certain evidentiary privileges (e.g. attorney-client, physician-patient, clergy[107] or psychologists[108]) unless the application has been approved by a United States Attorney or an appropriate Deputy Attorney General[109] and "[a]ccess to the documentary materials appears to be of substantial importance to the investigation or prosecution for which they are sought."[110] The regulations also contain the minimization requirement that "[a] search warrant authorized under paragraph (b)(2) of this section shall be executed in such a manner as to minimize, to the greatest extent practicable, scrutiny of confidential materials."[111] When such materials are likely to be found among the materials seized, a reliable third person should first review them to remove the privileged documents not subject to seizure. This task may be done by a judge in camera, a special master appointed by the court, or an independent team of prosecutors not involved in the investigation.[112]

3.1.1 Privacy Protection Act

63. In 1967, the Supreme Court held in *Warden v. Hayden* that a search warrant could be issued to seize evidence of a crime. [113] In 1978, the United States Supreme Court held in the controversial case of *Zurcher v. Stanford Daily* that prosecutors could constitutionally seize evidence from a third party news organization. [114] In response, Congress enacted the Privacy Protection Act (PPA), which attempted to strike a balance between these two fiercely competing interests.[115] Congress noted its aim in passing the statute in the following provision of the PPA:

64. The purpose of this statute is to limit searches for materials held by persons involved in First Amendment activities who are themselves not suspected of participation in the criminal activity for which the materials are sought, and not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation.[116]

65. The statute protects journalist work product, defined as original work in the possession of anyone who intends to publish it.[117] The statute also protects "documentary materials," broadly defined, which are possessed in connection with a purpose to issue a public communication, such as a newspaper, book, or broadcast.[118] Such materials may not be seized unless they constitute the fruits or instrumentalities of crime, there is danger of physical injury, or the person possessing the materials probably committed a crime [other than that of possessing or withholding the materials themselves].[119] In addition, documentary materials may be seized upon obtaining a warrant where the magistrate determines that there is reason to believe giving notice would result in destruction or alteration of the material, or that a court order for the materials has been disobeyed and there is reason to believe further delay would threaten the interests of justice.[120] According to the latest Computer Seizure guidelines from the Department of Justice (DOJ):

66. [T]he use of personal computers for publishing and the Word Wide Web has dramatically expanded the scope of who is 'involved in First Amendment activities.' Today, anyone with a computer and access to the Internet may be a publisher who possesses PPA-protected materials on his or her computer.[121]

67. The PPA does not provide for the suppression of evidence seized in violation of its terms, and the Supreme Court has not determined whether the Constitution so requires.[122] However, the latest DOJ guidelines indicate a serious concern for civil and criminal liability, even when the seizure of PPA protected materials is incidental and unintentional.[123]

3.2 Interception of United States Postal Service Mail

68. The Fourth Amendment by its terms applies to the right of the people to be secure against unreasonable searches and seizures "in their persons, houses, papers, and effects."[124] Implicit in this constitutional doctrine is the notion that persons may have a reasonable expectation of privacy in certain situations even when they are not physically within this protected enclave. Moreover, the American Constitution also confers the privilege against self-incrimination, which entails a related value, that is, the right to refuse to cooperate with criminal investigators.[125] Finally, the First Amendment broadly protects freedom of speech and of the press, both of which depend heavily upon the ability to use postal systems and resources. Taken together, these constitutional doctrines led the United States Supreme Court to hold in 1878 that documents in transit as first class mail in the postal system retain their private character under the Fourth Amendment so as to require the government to secure a warrant before they could be seized. In *Ex parte Jackson*, the Court noted that the very essence of creating different classes of United States mail items was to preserve and demarcate the Fourth Amendment rights of mail patrons to be secure in the privacy of their papers:[126]

69. The right to designate what shall be carried necessarily involves the right to determine what shall be excluded. The difficulty attending the subject arises, not from the want of power in Congress to prescribe regulations as to what shall constitute mail matter, but from *the necessity of enforcing them consistently with rights reserved to the people, of far greater importance than the transportation of the mail*. In their enforcement, a distinction is to be made between different kinds of mail matter, – between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined. Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, *as if they were retained by the parties forwarding them in their own domiciles*. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation,

> particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household. *No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail;* and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution.[127]

70. Thus, in *Jackson* the court divided government mail surveillance into two categories for constitutional purposes.[128] Content seizures entail breaking the mail seal, examining and perhaps copying the contents and, in most cases, resealing and delivering the parcel to the target. The Supreme Court held these seizures of first class mail to be subject to the warrant requirement of the Fourth Amendment. Mail covers, on the other hand, merely monitor mail, recording sender and recipient address information on the outside of the envelope, without breaking the seal. The law requires only that a law enforcement agency furnish a request which specifies a reasonable ground to believe that the mail cover is necessary to obtain information regarding the commission or attempted commission of a crime.[129]

3.3 Wiretaps[130]

71. The United States Supreme Court long resisted extending the constitutional doctrines it applied to first class mail to private telephone communications. In 1927, the Court held that the constitution provided no protection for the interception of information by a wiretap, since no property was seized. In *Olmstead v. United States*, [131] the Supreme Court, in a controversial and widely criticized decision, declined to extend the doctrine of *Jackson* and its progeny to this new technology. In his dissent, Justice Brandeis warned that the Court was ignoring a growing threat to fundamental rights: "The progress of science in furnishing the government with means of espionage is not likely to stop with wire-tapping."[132]

72. The Court ultimately repudiated the rationale of *Olmstead* in 1967, when it held in *Katz v. United States*[133] that the interception of a telephone conversation originating in a public telephone booth violated the Fourth Amendment. Just one year later, Congress entered the fray – and largely obviated the need for the Supreme Court to pursue the constitutional analysis – by enacting stringent statutory restrictions on wiretaps in Title III of the Omnibus Crime Control & Safe Streets Act of 1968 – widely known simply as Title III. Most of the judicial decisions issued thereafter dealt with questions of statutory interpretation rather than Constitutional protection. [134] Title III permits electronic surveillance by government investigators only under court order, and requires that records be maintained to show the quantity and nature of such activities.[135] Title III was written before the era of the Internet, and was primarily concerned with actual "aural interception" of telephone conversations and with the use of electronic devices to intercept private conversations in real time. The Act prohibited such interceptions by either government officials or private citizens, and provided stringent remedies for violations: civil liability, criminal liability, and a very strong exclusionary rule barring the use of either the intercepts or *any evidence derived from them in any trial.*[136] Title III, as amended by the ECPA,[137] extends to "oral communications," defined as: "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."[138]

73. Title III does not extend to ordinary eavesdropping on an oral conversation, but only to the "interception" of such a communication by use of the specified devices.[139] The FBI descriptions of Carnivore take great pains to avoid calling its activities interceptions, by indicating that the system does not in any way interfere with transmission, that only copies of transmissions are used.[140] The Zip drive clearly holds stored communications, but this portion of Title III includes no exclusionary rule.

74. Title III as originally enacted also regulates pen-trap surveillance, which is limited to tracking the origin and destination of calls involving the target.[141] This type of surveillance is regulated for electronic communications, both ongoing and stored, by the ECPA. Since these intercepts merely record the numbers from which or to which calls or messages were transmitted, the privacy concerns are less severe, and accordingly the restrictions on the use of these techniques are less stringent.[142] Just as mail surveillance can entail either the actual seizure and examination of contents or merely tracking source and destination by examining the parcel, so too telephonic interceptions fall into two major groups: actual wiretaps, which intercept and record conversations; and pen register or trap & trace operations, which merely record the origin and/or destination of calls involving specific telephone numbers.[143]

75. A federal judge must authorize a full content wiretap.[144] The judge must be satisfied from the application that there is probable cause to believe that an individual has committed or is about to commit any of a large number of designated crimes.[145] Although the FBI and others have characterized Carnivore as applying to only a few very serious crimes such as terrorism, kidnapping, drug trafficking, and child pornography, the statutory list of predicate crimes in Title III, even for content interception wiretaps, is extensive and includes: labor organization payments, bribery, concealment of assets, juror influence, and currency transactions.[146]

76. The judge must also be satisfied that normal investigative procedures are not adequate to secure the evidence sought,[147] and that there is probable cause to believe that the facility or place from which the interception is to be made is either controlled by or is being used in connection with the commission of the predicate offense. [148] Particular communications concerning the predicate offense will be obtained through the proposed interception.[149]

77. The order authorizing the wiretap must itself contain specific information concerning the identity of the target, [150] the communications facilities, the type of communications targeted, the predicate offense, the authorized agency for interception and the duration of the operation.[151] Title III also includes a minimization principle: the duration of a wiretap is limited to the shorter of 30 days or the time required to implement the operation; the wiretap must be interrupted immediately whenever an intercepted communication is outside the scope of the order.[152] Finally, Title III requires that intercepted communications be fully recorded whenever possible, in a manner which protects the recording from editing or alteration.[153] The recordings must be submitted to the judge immediately after the operation is completed, and the judge must retain them under seal for at least ten years, allowing copies to be made and used as necessary.[154] Finally, the target of a wiretap order must be notified within ninety days after the wiretap order terminates of the fact of the order, its date, and whether communications were intercepted.[155]

78. When Title III was enacted, the telephone business in the United States was largely under the control of the Bell Telephone/AT&T monopoly; however, following the breakup of this monopoly during the 1980s, the industry became populated with many new companies armed with a variety of burgeoning new technologies for both voice and data communications. [156] In response to these developments, Congress enacted legislation in 1994 requiring telecommunications carriers and manufacturers to build wiretap capabilities into every communications systems.[157]

3.4 Electronic Communications Privacy Act [ECPA] (1986)

79. The advent of the modern computer era can be traced to the introduction of the small, inexpensive, and powerful personal computer, or PC, in the 1970s.[158] Although the Internet was just barely getting off the ground as a universal public resource, it was obvious in the early 1980s that Title III was not an adequate statutory foundation to regulate the staggering possibilities that the computer brought to the field of electronic surveillance. Since the Court had stepped out of the fray after Katz, letting Congress take the initiative, Congress accepted the challenge and commissioned a technical review of Title III with a view toward reform. [159] It was on this basis that Title III was extensively amended in 1986 by the Electronic Communications Privacy Act, (ECPA) which included important amendments to the existing provisions of Title III governing wiretaps – most notably by adding the new term "electronic communications" and regulating them in several existing parts of Title III, as well as by adding an entirely new section regulating access to electronically "stored communications."[160] ECPA also extended Title III to cover private telephone networks as well as common communications carriers.[161] A separate statute governs child pornography.[162]

80. The advent of ECPA did not create a uniform scheme for surveillance under the law. Currently, the unlawful seizure of the contents of first class mail or of telephone conversations is both a tort and a crime. More importantly, evidence so seized is subject to the exclusionary rule, precluding its use as evidence at trial. Moreover, while a seizure of first class mail is subject to the general requirements for search warrants set forth by the Supreme Court under the Fourth Amendment, wiretap warrants are subject to the enhanced requirements of Title III.

81. ECPA added a new category of "electronic communications," which includes any communications that are *"not* carried by sound waves and cannot be fairly categorized as containing the human voice."[163] Electronic communications thus include many transmissions by such devices as computers, digital-display pagers, and fax machines.[164] This now seems to have been a terrible idea. We are rapidly learning that the Internet is about the free and flexible transmission of information – a.k.a. content – in a wide variety of formats. Indeed, when the Internet fulfills one of its broadband dreams – becoming a voice as well as a data network – the distinction between oral and electronic transmissions for purposes of search and seizure is simply untenable. It has been pointed out that ECPA failed to address the technology problems in a coherent way, and that Title III should be revamped to abolish the different standards for telephone, email, and voice mail, and conflicting treatment of messages that are intercepted, accessed, or acquired. In short, "[E]mployee communications should be protected regardless of whether the message is transmitted or remains in storage."[165]

82. ECPA also modified the Title III definition of "intercept," which had applied only to actual aural eavesdropping of wire or oral communications, and extended it to include other means of acquiring wire, oral, or electronic communications.[166] Additionally, ECPA created a new category of stored electronic communications,[167] restricting both the *interception* of electronic communications,[168] and the *disclosure of and access to* stored electronic communications.[169] Access to stored electronic communications is governed by 18 U.S.C. § 2703, which distinguishes between data stored for less than 180 days and data stored longer. The rationale for the distinction is that the older material more closely resembles other ordinary business records, which traditionally have been obtained through the use of document subpoenas and warrants as outlined above. Accordingly, these older materials can be obtained by a search warrant *without notice* to the customer or subscriber, or by an administrative subpoena, grand jury subpoena, trial subpoena, or order under § 2703(d) [with notice to customer or subscriber].[170] Data stored for less than 180 days is treated more protectively, and access to such material requires a warrant issued under the Federal Rules of Civil Procedure or "an equivalent state warrant."[171]

83. The stored communication provisions of ECPA apply only to data, which is in *"temporary intermediate* storage of a wire or electronic communication incidental to the electronic transmission thereof or any backup of this communication."[172] The DOJ has taken the position that the act covers e-mails temporarily on the ISP server as part of an e-mail transmission process:

84. > Once the recipient accesses and retrieves the e-mail, however, the communication reaches its final destination. If a recipient then chooses to retain a copy of the accessed communication on the provider's network, the copy stored on the network in no longer in "electronic storage" … the copy is simply a remotely stored file.[173]

85. The legal issues involved in Carnivore intercepts are greatly exacerbated by a significant difference in these two statutes. The *interception* provisions, which are codified together with the wiretap provisions, have a strong exclusionary rule: under 18 U.S.C. § 2515, any evidence that is obtained by, or *derived from* an illegal intercept of a "wire or oral communication" is inadmissible at trial.[174] Improper *access* to and retrieval of stored data in violation of 18 U.S.C. § 2701, on the other hand, can be redressed only by an action for damages or by a criminal prosecution;[175] that statute contains no exclusionary rule.

86. The difficulties that flow from this dichotomy are illustrated in *United States v. Smith*,[176] a securities prosecution that originated when an informant guessed a co-worker's password and used it to unlawfully retrieve, forward to herself, record, and furnish to another co-worker an incriminating telephone voice mail message left by the defendant, which the co-worker then delivered to prosecutors together with an account of the crime.[177] The tape recording of the voice mail message falls within the definition of 18 U.S.C. § 2510(1) and therefore is subject to the exclusionary provision of § 2515. [178] However, it also falls within the definition of stored communication in § 2701, and is therefore also subject to the exclusive remedy provision of § 2708.[179] The government argued that an intercept occurs only if the conversation is overheard as it takes place in real time.[180] By analogy, the government could also argue that even full content Carnivore operations are not intercepts, because the content is read only later after being stored on the Zip drive. The court in *Smith* rejected this argument because wire communications are defined in § 2510(1) to include stored communications. The court noted that the definition of electronic communication in § 2510(12), on the other hand, includes only the "transfer of signs, signals, writing, images, sounds, data, or intelligence."[181] The court concluded: "Consequently, in cases concerning electronic communications … it is natural to except non-contemporaneous retrievals from the scope of the Wiretap Act."[182]

87. The Court then reconciled the statutory provisions by holding that an *intercept* entails actually acquiring the contents of a communication, while *access* involves "being in position to acquire the contents of a communication,"[183] so that "an exclusion provision in the Stored Communications Act [which covers access without content seizure] is unnecessary."[184] The Court concluded that when the employee retrieved and recorded the voice mail there was an intercept subject to the wiretap exclusionary rule of § 2515, so the tape was properly suppressed.[185]

88. The stored communications provisions apply to anyone who provides an electronic communications service or remote computing services to the public.[186] The terms are somewhat ambiguous, and it appears that a single ISP may qualify as either or both of them, depending not just upon the identity of its client, but also upon the nature of the services provided and even whether an e-mail has been opened and then stored on the ISP's resources. However, the computer seizure guidelines take the position that this distinction is often immaterial:

89. > As a practical matter, however, agents do not need to grapple with these difficult issues in most cases. Instead, agents can simply draft the appropriate order based on the information they seek, [such as] an order compelling Local ISP to divulge all files in [the target's] account except for those in 'electronic storage.' In plain English, this is equivalent to asking for all of [the target's] opened e-mails and stored files.[187]

90. The DOJ manual for search and seizure of computers to obtain electronic evidence does not even mention Carnivore.[188] Conversely, the IITRI Report does not discuss the Electronic Communications Privacy Act.[189] However, in *Smith* it was held that the retrieval of a stored voicemail message could constitute a content intercept subject to the exclusionary provision of Title III. The conclusion that governing law is not a seamless web is inescapable. Clearly Congress must define the governing law by distinguishing on a functional basis between the retrieval of content and the monitoring of traffic to learn who is communicating with whom. In addition, there must be a further distinction between retrieval of content that is in the process of being carried over the Internet, which should include temporary storage of that content on Internet resources, as opposed to files and documents which are truly stored in the same manner as documents. A rigorous and workable definition will present a great challenge, but so much has happened in the technology world since the last study was done in 1985 that clearly it is time for a fresh start.

3.4.1.1 Control over Carnivore Applications

3.4.1.1 Control over Carnivore Applications

91. The FBI's characterization of Carnivore is based upon a fundamental contradiction. In order to appease public concern about the use of Carnivore as a giant electronic dragnet, the FBI proffers the system as a small and simple box made up of off the shelf components assembled in a clever way to prevent abuses and sabotage.[190] But at the same time, the FBI claims that Carnivore is ferociously controlled by both agency procedure (only two dozen units, centrally stored, must involve both case agents and TTAs, deployed only as a last resort) and legal restrictions (very few crimes are covered, highest level approvals required for application, rigorous requirements for the warrant, close controls over the operation and its results).[191] Yet if the first set of claims is true, then Carnivore could easily become a part of every agent's toolbox: just a laptop and the tap. Thus, it becomes useful to look more closely at the legal restrictions that actually affect Carnivore's operation.

3.4.1.2 Predicate Felonies

92. Title III restricts wiretaps to designated felonies, as discussed above. The FBI has repeatedly asserted that Carnivore operations have been [and implied that they will be] restricted to an even narrower group of felonies, typically terrorism, narcotics trafficking, child pornography, and kidnapping.[192] However, an application for interception of electronic communications can be predicated upon *any* Federal felony offense.[193] The FBI has stated that it substantially follows the Title III wiretap requirements when performing Carnivore investigations.[194] Even if these provisions are followed, the scope of potential Carnivore use is much broader than the FBI has indicated.

3.4.1.3 Persons Authorized to Make Applications

93. Under the statute as amended, a federal official who is at or above the rank of Assistant United States Attorney[195] and any principal prosecuting attorney of a state or political subdivision thereof[196] may authorize the making of an application to a Federal Court to authorize intercepts by an investigative or law enforcement officer "when such interception may provide or has provided evidence of *any* Federal felony."[197] The Department of Justice has reported that, notwithstanding the broad language of the ECPA, the agency and Congress "agreed informally" when the statute was enacted that the Department would for a three-year period continue to require Department approval for all applications for interceptions of electronic communications. Thereafter, the agreement was rescinded insofar as it applied to digital-display paging devices, which are now the subject of a series of cases. The DOJ maintains that it continues to apply the Department approval requirements to other electronic communications, and maintains an Electronic Surveillance Unit in its Office of Enforcement Operations.[198] However, the agency's Criminal Resource Manual makes it clear that this unit does not have operational control over the authority of a particular official to make an electronic communications intercept application, but merely has attorneys who are "available to provide assistance concerning both the interpretation of Title III and the review process necessitated thereunder."[199]

3.4.1.4 Contents of Application & Standard for Issuance

94. The Fourth Amendment provides that: "No Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched and the persons or things to be seized*."[200]

95. Generic classifications in a warrant are acceptable only when a more precise description is not possible.[201] In *Application of Lafayette Academy, Inc.*,[202] the court struck a warrant authorizing the seizure of computer tapes, disks, operation manuals, tape logs, tape layouts, and tape printouts that were evidence of criminal fraud and conspiracy. The test is pragmatic; if large numbers of documents fit the criteria for seizure, then the warrant may include all of them.[203] It appears that in those situations agents are justified in seizing large numbers of documents, whether in file cabinets or on computer disks and tapes, for processing off site. Where, however, the warrant narrowly specifies the documents to be seized, then the removal of a much larger quantity of documents which contains the ones specified has been held invalid.[204]

96. The FBI claims that Carnivore can satisfy the specificity requirements through a combination of measures. First, the warrant itself will limit the scope of the intercept.[205] Second, Carnivore minimizes the seizure by immediately filtering out and ignoring all data packets that don't meet the specified criteria for sender, recipient, or content.[206] Third, intercepted documents that do not satisfy the search warrant criteria are deleted by the case agent.[207] However, Carnivore does not actually behave in the way the FBI claims it does. It is true that the search warrant can specify an Internet address or addresses that may be collected.[208] However, the intercept can extend to any transmission either from or to the target address, so that, for example, the several thousand members of a discussion group will have their messages intercepted just because they are written to or from a group member who is also a target. Moreover, IITRI has documented that whenever a Carnivore operation attempts to combine addresses with content criteria (i.e., text string searches), the string search criteria is ignored and all documents are kept.[209] The only remedy for this drastic over-inclusion is the *case agent*, who, under current FBI procedures, has sole access to the information which is kept and stored to the Zip disks, and who will remove those Zip disks from the Carnivore computer, and then "immediately" review their contents and delete the information that does not fit the requirements of the warrant.[210] Unless the courts treat Carnivore searches as *sui generis*, it is difficult to reconcile these described procedures with the decisions that have analyzed the specificity requirements in more traditional contexts.

3.4.1.5 Cooperation of ISP

97. The FBI describes Carnivore as a system which is attached to the resources of an ISP, which generally means a firm that offers Internet services to the public for a fee, such as Yahoo or AOL.[211] However, the ECPA amendments to Title III define, not an ISP, but rather an "electronic communications system" to mean "any service which provides to users thereof the ability to send or receive wire or electronic communications."[212] That term may be constructed to cover private firms, universities, and indeed all institutions that are connected to the Internet.

Conclusion

98. The FBI developed and deployed Carnivore without public disclosure until an ISP official disclosed that it had resisted a Carnivore assistance request. Shortly after that disclosure, as public concerns increased, the FBI ordered an independent technical review to confirm its assertion that Carnivore was constructed and operated in a manner that fully complies with existing law and the Constitution. However, the existing law is a hodgepodge of overlapping and inconsistent provisions regulating traditional mail, telephone wiretaps and bugs, electronic communications, and news media activities, which cannot sensibly be read to provide a coherent legal context for authorizing and regulating Carnivore activities. Unless Congress rapidly adopts legislation addressed specifically to Carnivore, there is a grave risk that the important privacy principles developed by the Supreme Court and Congress to protect more traditional forms of communication, i.e. "snail mail" and telephone voice communications, will be dormant vestiges of an earlier age while government surveillance of meaningful activities in the internet era goes largely unchecked.

---

* Professor of Law, Seton Hall University School of Law. © 2001. All Rights Reserved. The author wishes to thank Deborah Freier, Seton Hall Law School '01 for her diligent research assistance.

[1] Perhaps this is because the new millennium began only on January 1, 2001.

[2] Carnivore was revealed to the public eye in April 2000, when an executive from Earthlink, a major ISP, disclosed FBI efforts to install a Carnivore tap on its system.

[3] Such cooperation will be, the FBI believes, legally mandated, in the same manner as CALEA currently requires telephone carriers to cooperate on wiretaps.

[4] *See* STEPHEN P. SMITH et al., ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE [IITRI], INDEPENDENT REVIEW OF THE CARNIVORE SYSTEM (2000) [hereinafter IITRI CARNIVORE REPORT].

[5] As described in Part 3, the investigators may if properly authorized open and read the mail or examine its contents, and then resume delivery without alerting the recipient of the intervention; alternatively, investigators may simply examine the outside of the letter or parcel and record information, such as addresses.

[6] *See infra* Part 3.

[7] COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, UNITED STATES DEPARTMENT OF JUSTICE, SEARCHING & SEIZING

COMPUTERS & OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2001) [hereafter DOJ COMPUTER SEARCH GUIDELINES].

[8] *See* United States v. Gering, 716 F.2d 615 (9th Cir. 1983). *See generally* 39 C.F.R. § 233.3(d)(2) (2001).

[9] The term wiretap encompasses two very different activities. The familiar sense of the term, described here, entails actual monitoring and recording of ongoing conversations. The American legal requirements for wiretaps are more stringent than those for search warrants. However, telephone surveillance may be limited to capturing the telephone numbers called from a specific telephone [a pen register] or to a specific telephone [trap and trace]. The American legal requirements for this type of surveillance are much less strict. The legal issues will be discussed at the conclusion of this paper.

[10] *See infra* Part 3, at 20. *See generally* ANTHONY ALBERTI, WIRETAPS: A COMPLETE GUIDE FOR THE LAW ENFORCEMENT AND CRIMINAL JUSTICE PROFESSIONAL (1999) (establishing in excruciating detail the complex equipment and procedural requirements for a wiretap operation under Florida law); DICK LEHR & GERARD O'NEILL, BLACK MASS: THE IRISH MOB, THE FBI, AND A DEVIL'S DEAL (2000) (recounting the seamy saga of FBI corruption and mob informants in Boston, and providing some particularly compelling descriptions of the dangerous, expensive, difficult, and often frustrating efforts to wiretap and bug career criminals who were fully aware that they were ongoing surveillance targets).

[11] *See infra*, Part 3.

[12] IITRI CARNIVORE REPORT, *supra* note 5, § 3.4.1, at 3-10.

[13] *Id*. § 3.2.3, at 3-5.

[14] Robert Graham, *Carnivore FAQ 2.4*, *available at* http://www.robertgraham.com/pubs/carnivore-faq.html (last modified January 2001) [hereinafter *Carnivore FAQ*]. Robert Graham is the TCO of Network Ice, a prominent marketer of network security devices such as firewalls. A freeware program called TCP_DUMP has been said to be capable of performing the same packet sniffing functions as Carnivore. Black Ice Defender, a commercially available product, includes "packet logging" to monitor traffic and save it to disk just like carnivore, and the results can be displayed with the freeware program Ethereal. There are numerous products on the market more advanced than Carnivore.

[15] *Carnivore FAQ*, *supra* note 15, at 1.3. According to this source, the FBI also claims actual Carnivore intercepts were required in only ten percent of cases where court authorization had been obtained. In all of the other cases, the ISP was able to provide the information sought in less intrusive ways.

[16] Electronic Privacy Information Center, *Report on FOIA Litigation*, *available at* http://www.epic.org/privacy/carnivore/default2.html (last modified August 9, 2001).

[17] Packet technology provides for faster transmission and easier recovery from failed transmissions of individual packets, which failures are quite common but almost never fatal.

[18] The many routing devices that the data packet encounters on its trip need only examine the header in order to select the next route or to take other appropriate action, and this ability to ignore the rest of the data packet provides even greater speed.

[19] IITRI CARNIVORE REPORT, *supra* note 5, § 3.4.1 at 3-10 (Carnivore can presently operate only upon a 10/100Base-T Ethernet cable, and uses a Shomiti Systems, Inc. Century Tap).

[20] *Id.* § 3.4 at 3-10 (Carnivore merely records IP packets, and does not assemble packets into higher level protocols. Nor does Carnivore entail the installation of an IP stack. "The packets are treated strictly as data.").

[21] *Carnivore FAQ*, *supra* note 15, at 1.3.

[22] *See* Oversight Hearings on "Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program," Before the House Comm. on the Judiciary, Subcomm. on the Constitution, 106th Cong. (2000) (statement of Donald M. Kerr, Assistant Director, Federal Bureau of Investigation), July 24, 2000, a*vailable at* http://www.house.gov/judiciary/kerr0924.htm.

[23] As discussed below, this characterization conceals a fundamental policy problem. American law generally provides that if one party to a communication is an authorized target, the interests of the innocent parties to that communication have no right to object to the monitoring or seizure of *their* speech or data.

[24] *See infra,* Part 3.

[25] *See* FBI, *Carnivore Large Chart*, *available at* http://www.fbi.gov/hq/lab/carnivore/carnlrgmap.htm (last visited Sept. 6, 2001).

[26] The RFP algorithm deals with this in an oversimplified way, as if every communication were from one person to another. In reality, there are e-mail cc's and forwards, newsgroups, listservers, and other complicating factors.

[27] Robert Graham, *Carnivore – Detailed Analysis*, Slide Presentation Toorcon '00 San Diego, Slide 26 (2000), *available at* http://www.robertgraham.com/slides/00toorcon. An algorithm is a functional description of a process, frequently recursive, that a computer program will perform.

[28] This is only one example of several criteria, as discussed below.

[29] A very basic workstation often used to perform simple tasks such as word processing.

[30] This is not to be confused with the current Microsoft Workstation OS, Windows 2000 Professional.

[31] IITRI was not given the full source code, but did conduct some tests and line counts. The FBI cited contractual restrictions from the software vendor as a reason for not furnishing the full source code. However, given that limitation an evaluator can merely verify that the program can perform designated functions, and cannot certify that there are not other functions included in the program.

[32] This is roughly 200 times the capacity of the universal 3.5 inch floppy drive.

[33] IITRI CARNIVORE REPORT, *supra* note 5, § 3.4.4.3, at 3-17.

[34] *Id*. § 3.4.1, at 3-11 (noting several technical limitations on the current Carnivore, including the inability to work on full-duplex or non-Ethernet configurations).

[35] Mary Youngblood, Earthlink Abuse Team Manager, August 10, 2000. Reported by *StopCarnivore.org*, *available at* http://www.stopcarnivore.org/carnfreeisps.htm (on file with the Virginia Journal of Law and Technology).

[36] "[Carnivore] is connected as a passive collection device and does not have any ability to transmit anything onto the network." Kerr Statement to House Subcomm., *supra* note 23, at 7.

[37] The original meaning comes from physical attachment of a recording device to capture the full contents of a telephone conversation. This was the central focus of the original Title III enactments in 1968. Although technology has greatly expanded the kinds of data monitored, both investigators and legal principles impose enhanced requirements when full content interceptions are required.

[38] When the technology consisted of "plain old telephone service [POTS]," investigators employed two different techniques to track telephone numbers. Trap & Trace, used for inbound calls, often involved a lengthy manual trace of circuits to identify the caller, and unless a conversation lasted several minutes, the trace was lost. Caller ID makes this seem primitive, but the term remains. Conversely, a Pen Register for outbound calls was simply a device placed on the telephone line which counted the dial pulses, which were then manually converted into the telephone number being dialed.

[39] In simple situations, the target has a fixed and known IP address in the Internet format aaa.bbb.ccc.ddd. However, if the target is part of a local enterprise network, or uses dialup services to access the network, a different IP address may be dynamically assigned for each session. Carnivore has the ability to handle these situations by retrieving pertinent DHCP information from the TACAS/RADIUS for a specified user account. Neither the FBI proposal nor the IITRI report discuss the ability of Carnivore to tackle internet traffic that employs Virtual Private Network [VPN] technology such as Intel's SHIVA which is designed to prevent interception.

[40] Kerr Statement to House Subcomm., *supra* note 23, at 6.

[41] IITRI CARNIVORE REPORT, *supra* note 5, §§ 3.3 at 3-6, 4.2 at 4-2.

[42] *Id*. § 3.1 at 3-1.

[43] Kerr Statement to House Subcomm., *supra* note 23.

[44] Packets may be selected based upon an actual fixed or dynamic IP address, or upon the "To:" or the "From:" address of a POP3 or SMTP e-mail message.

[45] IITRI CARNIVORE REPORT, *supra* note 5, § 3.4.4.1.1 at 3-14.

[46] *Id.* § 3.4.4, at 3-13.

[47] *Id.* § 3.6.12, at 3-28 (emphasis added). *See also id*., § 3.6.11 at 3-27 (The report also points to another inherent problem affecting this function. Since only packets containing the text string would pass the filter, any packet from that same message which passed the tap *before* the text string showed up would already have been discarded, thus preventing the message from being displayed, since "CoolMiner needs the entire set of e-mail protocol packets in order to display properly.").

[48] *See infra,* Part 3.

[49] *Carnivore FAQ*, *supra* note 15, at 1.4.

[50] IITRI CARNIVORE REPORT, *supra* note 5, § 3.4.3, at 3-12.

[51] *See* Intel, *Announcement* (Jan. 4, 2001), *available at* http://www.support.intel.com/support/si/dial/access/30840.html.

[52] IITRI CARNIVORE REPORT, *supra* note 5, § 3.4.4, at 3-13.

[53] *Carnivore FAQ*, *supra* note 15, at 2.7.

[54] *Carnivore FAQ*, *supra* note 15, at 2.8 (citing Graham's belief that the FBI could keep the source code, but run Carnivore in a test lab and publish the results and the test files).

[55] Kerr Statement to House Subcomm., *supra* note 23.

[56] See Carnivore FAQ, supra note 15, at § 4.8.

[57] *See id*.

[58] Kerr Statement to House Subcomm., *supra* note 23. It has been noted that these concerns are further served by the FBI decision to design Carnivore so no TCP/IP stack is loaded. Robert Graham, Network Ice, Presentation Toorcon, San Diego 2000 slides 17-20, *at* http://www.robertgraham.com/slides/00toorcon.

[59] *See Carnivore FAQ*, *supra* note 15, at § 2.9.

[60] IITRI CARNIVORE REPORT, *supra* note 5, § 1.1, at 1-2.

[61] *Id*. § 1.2.1, at 1-6.

[62] Essentially, does a properly programmed Carnivore intercept, contain an amount of information which is "just right", neither missing authorized information nor retrieving unauthorized information?

[63] Ted Bridis, Neil King, Jr., & Nick Wingfield, *Earthlink Just Says No to FBI's Carnivore*, ZD NEWS, (July 14, 2000), at http://www.zdnet.com/zdnn/stories/news/0,4586,2603945,00.

[64] Mary Jo Foley, *Congress Isn't Swallowing Carnivore*, ZD NEWS, (July 24, 2000), *at* http://www.zdnet.com/zdnn/stories/news/0,4586,2606899,00.html.

[65] IITRI CARNIVORE REPORT, *supra* note 5, § 1.1 at 1-2 .

[66] John Young, editor of the http://www.cryptome.org, published the full report, *at* http://www.cryptome.org/carnivore-mask.htm.

[67] *See* Robert Lemos, *Carnivore Review: A 'Stacked Deck?'*, ZD NEWS (Oct. 4, 2000), *at* http://www.zdnet.com/zdnn/stories/news/0,4586,2636879,00.html.

[68] The Altivore Web Site (http://www.networkice.com/altivore/) is devoted to an ongoing development of this product and to discussions of the technical and social issues of electronic surveillance on the Internet and elsewhere.

[69] IITRI CARNIVORE REPORT, *supra* note 5, § 1.1 at 1-2

[70] *Id*. § 1.2, at 1-5. The evaluators also decided to eschew any detailed pursuit of minor bugs, a sensible decision in light of the fact that Carnivore is a work in progress: Version 1.3.4 (sp3) was evaluated, but at the time of the study, Version 2 was already being written. It may be recalled that two of the most successful PC applications in history [MS Word and WordPerfect] reached their pinnacle of [non GUI] success in Versions 5.0 and 5.1, respectively.

[71] IITRI CARNIVORE REPORT, *supra* note 5, § 3.3.3, at 3-9.

[72] *Id*. § 4.3.2, at 4-9.

[73] *See also id*. § ES.4 at xi (claiming the setup "mimics the typical installation of an ISP," but notes that the "tap was placed on a subnetwork containing traffic from the target but as little other traffic as possible."); *id.*§ at 2-3 (describing the test bed). To be sure, the study was undertaken under severe time constraints: the evaluators had barely three months from award to submission. This time constraint dissuaded other groups from even bidding on the job.

[74] IITRI CARNIVORE REPORT, *supra* note 5, § 3.4.2, at 3-11.

[75] *Id*. § 3.4.4.3, at 3-17.

[76] *Id*. § 3.4.2, at 3-12.

[77] *Id*. § 2.3, at 2-2.

[78] *Id*. § 2.4, at 2-3.

[79] *Id*. § 3.2.1, at 3-3 ff.

[80] *Id*. § 3.2.1, at 3-3.

[81] *Id*. § 3.2.1, at 3-4.

[82] *Id*. (The justification is initialed by a supervisor and kept in the pen-register control file).

[83] *Id*.

[84] *Id.,* § 3.2.2, at 3-4 [emphasis added].

[85] *Id.,* § 3.2.2, at 3-5 (Dynamic Host Configuration Protocol [DHCP] or Remote Access Dialup User Services [RADIUS]).

[86] *Id*. § 3.2.2, at 3-5.

[87] *Id*. § 3.2.2, at 3-5.

[88] *Id*. § 3.2.2, at 3-5.

[89] *Id*., § 3.2.3, at 3-5.

[90] *Id*., § 3.2.3, at 3-5 (emphasis added).

[91] To clarify: 250 words per page is 2000 bytes per page is 500 pages per megabyte is 50,000 pages per hundred megabyte Zip disk.

[92] See IITRI CARNIVORE REPORT, *supra* note 15, § 3.2.3, at 3-5.

[93] Ex Parte Jackson, 96 U.S. 727, 732-733 (1878); Olmstead v. United States, 277 U.S. 438 (1927).

[94] Katz v. United States, 389 U.S. 347 (1967). *See also* 18 U.S.C. § 2510 et seq., § 3121-3127 (1986) (In regulating surveillance of telephone systems, the law fundamentally distinguished full content interception (wiretap) from pen/trace monitoring (source and destination of telephone calls involving a targeted number). We can extend by analogy this precept to the opening and reading first class mail in transit as opposed to retrieving information such as addresses from the envelope).

[95] Electronic Communications Privacy Act of 1986, amending various sections of 18 U.S.C. § 2510 et seq. and adding provisions regulating stored communications, 18 U.S.C. § 2701 et seq.

[96] Zurcher v. Stanford Daily, 436 U.S. 547, 565 (1978). *See also* The Privacy Protection Act (PPA), 42 U.S.C. § 2000aa (2001).

[97] *See generally* The National Security Surveillance Act [NSSA], S. 743, 94th Cong. (1975).

[98] FED. R. CRIM. P. 41(b). *See also* 28 C.F.R. § 59.4 (1981) (Attorney General Guidelines for federal officers who wish to obtain documentary materials from disinterested third parties). *See generally* Warden v. Hayden, 387 U.S. 294 (1967) (rejecting the doctrine that a search warrant could not authorize the seizure of "mere evidence").

[99] *See generally* Federal Guidelines for Searching & Seizing Computers (United States Department of Justice 1994) at 30. The Guidelines were rewritten in January 2001: DOJ COMPUTER SEARCH GUIDELINES, at 36. *See generally* United States v. Gawrysiak, 972 F. Supp. 853 (D.N.J. 1997), *aff'd.* 178 F.3d 1291 (3d Cir. 1999).

[100] Andresen v. Maryland, 427 U.S. 463 (1976). *See also* United States v. Truitt, 521 F.2d 1174 (6th Cir. 1975).

[101] Andresen**,** 427 U.S. at 463.

[102] United States v. Whitten, 706 F.2d 1000, 1009 (9th Cir. 1983), *cert. denied*, 465 U.S. 1100 (1984).

[103] United States v. Santarsiero, 566 F. Supp. 536, 544 (S.D.N.Y. 1983).

[104] *Big Brother in the Wires, Wiretapping in the Digital Age* (ACLU), 1998, at 4, *available at* http://www.aclu.org/issues/cyber/wiretap_brother.html.

[105] See 28 C.F.R. § 59.4 (2000).

[106] 28 C.F.R. § 59.4(a)(2). *See also* 28 C.F.R. § 59.4(c) (2000) (delineating several factors to be considered in making this judgment, including whether advance notice might lead to concealment, destruction, or alteration of the documents; whether a suspect has access to them; whether there is a close relationship of friendship or loyalty between suspect and custodian; and whether the custodian is subject to threats or reprisals. The list concludes with this admonition: "The fact that the disinterested third party possessing the materials may have grounds to challenge a subpoena or other legal process is not *in itself* a legitimate basis for the use of a search warrant.") [emphasis added].

[107] *See 28* C.F.R. § 59.4(b)(1).

[108] *See* 28 C.F.R. § 59.4(b)(5). *See also* Jaffee v. Redmond, 518 U.S. 1 (1996) (In defining the scope of the counseling privilege, the Supreme Court separately discusses materials held by psychiatrists, psychologists, social workers, nurses, and the like. One of the more notorious violations of the Watergate era was the unlawful search of a psychiatrist who was treating Daniel Ellsberg, the former government employee who played a crucial role in the publication of the Pentagon Papers).

[109] *See* 28 C.F.R. § 59.4(b)(2) (allowing a narrow exception for emergency applications approved by "the appropriate supervisory official of the Department of Justice" provided the Deputy Attorney General is notified within 72 hours).

[110] 28 C.F.R. § 59.4(b)(1).

[111] 28 CFR § 59.4(b)(4).

[112] *See* DOJ COMPUTER SEARCH GUIDELINES, *supra* note 8, at 35. *See also* DeMassa v. Nunez, 747 F.2d 1283 (9th Cir. 1984) (authorizing the use of a special master to help search a computer containing privileged information).

[113] 387 U.S. 294 (1967).

[114] 436 U.S. 547 (1978).

[115] *See* 42 U.S.C. § 2000aa (1980).

[116] S. Rep. 874 96th Cong. 2d Sess. 11 (1980).

[117] *See* 42 U.S.C. § 2000aa-7(b).

[118] *See* 42 U.S.C. § 2000aa(b).

[119] *See id*.

[120] *See id*.

[121] DOJ COMPUTER SEARCH GUIDELINES, *supra* note 8, at 30.

[122] *See* 42 U.S.C. § 2000aa-6(a),(d),(e); Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997).

[123] DOJ COMPUTER SEARCH GUIDELINES, *supra* note 8, at 30. The department is particularly disturbed by the holding that the secret service was liable for inadvertent seizure of PPA material in Steve Jackson Games, Inc. v. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd on other grounds*, 36 F.3d 457 (5th Cir. 1974).

[124] U.S. CONST. amend. IV.

[125] U.S. CONST. amend. V (No person "shall be compelled … to be a witness against himself …").

[126] 96 U.S. 727 (1878).

[127] *Id*. at 732-733 (1878) (emphasis added).

[128] Jackson actually creates two dual classifications. The first, between first- and fourth-class mail, does not concern us here. The second distinguishes breaking the seal and examining the contents from mere outward examination, which in turn justifies the distinction between the warrant requirement for opening mail and less stringent requirements for mail covers. *See* United States v. Van Leeuwen, 397 U.S. 249 (1970) (upholding detention and external inspection of first class mail based upon justifiable suspicion that fell short of probable cause). *See generally* 39 U.S.C. §§ 404, 3623 (outlining the Postal Service's specific powers).

[129] 39 C.F.R. § 233.3(e)(2) (1982); *see generally* United States v. Gering, 716 F.2d 615,618-620 (9th Cir. 1983) (applying the reasonable grounds standard).

[130] Omnibus Crime Control & Safe Streets Act of 1968, 18 U.S.C. § 2510-2522 (1968), *repealed by* The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522 (1986).

[131] 277 U.S. 438 (1928).

[132] *Id*. at 571 (Brandeis, J., dissenting).

[133] 389 U.S. 347 (1967) (recognizing that the Fourth Amendment protects persons in situations where they have a reasonable expectation of privacy even though the seizure might not constitute a trespassory taking).

[134] 18 U.S.C. §§ 2510-2522 (1986) (mandating that state statutes governing electronic surveillance be at least as restrictive as the Federal law partially preempting state law).

[135] The requirements include the number of taps authorized, their purpose, number of conversations and people overheard, and how many intercepts led to arrests and convictions. *See generally* BRUCE SCHNEIER & DAVID BANISAR, THE ELECTRONIC PRIVACY PAPERS 9-38 (1997).

[136] 18 U.S.C. § 2511(1) (1986) (regarding prohibition); 18 U.S.C. § 2520 (1986) (regarding damages); 18 U.S.C. § 2521 (1986) (regarding injunctions); 18 U.S.C. § 2511(4) (1986) (regarding criminal penalty); 18 U.S.C. § 2515 (1986) (regarding preclusion of evidence). As to suppression of evidence derived from illegal taps, see, e.g., United States v. Smith, 155 F.3d 1051 (9th Cir. 1998).

[137] The Electronic Communications Privacy Act, *supra* note 92.

[138] *Id*. at § 2510(2).

[139] *Id*. at § 2510(4) (setting out the means by which a prohibited intercept occurs). *See also id*. § 2511(1). However, such eavesdropping by police, if conducted in a private place, would violate the Fourth Amendment under *Katz*.

[140] *See supra* Part 2.

[141] *See* 18 USC **§** 2511(2)(h) (1986).

[142] 18 U.S.C. §§ 3121-3124 (1994).

[143] All of these terms are mired in the earliest vestiges of electronic communication, when conversations could be intercepted only by physically tapping into a wire or planting a bug, and when source and destination information could be obtained only by tapping a telephone line and counting the clicks or pulses which coded the numbers being dialed, or by manually tracing an incoming call through switches to attempt to ascertain the source number. These technologies, in addition to raising the spectre of "Big Brother," were extremely expensive and time consuming, more than a little dangerous, and often frustratingly unproductive. *See generally* ALBERTI, *supra* note 11; DICK LEHR & GERARD O'NEILL, *supra* note 11.

[144] 18 U.S.C. § 2516(1). The United States Constitution provides for the appointment of Federal Judges to serve on good behavior [i.e., for life unless impeached for high crimes or misdemeanors, U.S. CONST., art. III, § 1]. However, federal judicial functions are also performed by magistrates, who are essentially judicial assistants, and by specialized judicial officers deciding administrative disputes, bankruptcy, and other proceedings. None of these judges serves pursuant to Article III and, more importantly, none can authorize a full content wiretap. Title III does authorize emergency action in a few narrowly defined circumstances, but judicial authorization must be obtained within 48 hours. *See* 18 U.S.C. § 2518(7).

[145] 18 U.S.C. § 2518(3)(a).

[146] *See* 18 U.S.C. § 2516.

[147] 18 U.S.C. § 2518(3)(c) (requiring the applicant to attest that normal investigative procedures have been tried and have failed, or appear unlikely to succeed if tried, or in the alternative appear too dangerous).

[148] 18 U.S.C. § 2518(3)(d) (the characterization of this provision has been simplified for this paper, and is subject to certain exceptions for highly sensitive investigations as set forth in 18 U.S.C. § 2518(11)).

[149] 18 U.S.C. § 2518(3)(b).

[150] Section 2518(11) of the statute now authorizes a "Roving Wiretap," which allows the FBI to eavesdrop on many people as long as they only pay attention to the suspect.

[151] 18 U.S.C. § 2518(4).

[152] 18 U.S.C. § 2518(5). Wiretaps may, upon formal written application demonstrating specific cause, be extended once for thirty days, subject again to minimization. There is also a provision for after-the-fact minimization where the intercepted communications are either in a foreign language or in code and no contemporaneous translator is available. While the reference to "code" obviously emanates from the use of innocuous words to describe money and contraband, surely the FBI will seek to apply a similar doctrine to encrypted files and communications. *Id*.

[153] 18 U.S.C. § 2518(8)(a).

[154] *Id*.

[155] 18 U.S.C. § 2518(8)(d). The target may in turn move for disclosure of the intercepted communications. The motion is addressed to the discretion of the court. The statute also provides for and regulates the manner in which a defendant or other party may learn of the full contents of the wiretaps before trial and move to suppress part or all of the portions being offered into evidence. 18 U.S.C. § 2518(9), (10).

[156] *See generally* Steve Coll, *The Deal of the Century: The Breakup of AT&T*, (Athenum 1986).

[157] The Communications Assistance for Law Enforcement Act of 1994, Pub. L. 103-414, 108 Stat. 4279 (codified in scattered sections of 18 U.S.C. and 47 U.S.C.).

[158] The default clock setting on the X86 Intel chipset which drives the DOS/Windows Microsoft line was January 1, 1980, and that seems as good a date as any.

[159] OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 18 (1985), *discussed in* Thomas R. Greenberg, Comment, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219. 231 (1994).

[160] 18 U.S.C. § 2701.

[161] 18 U.S.C. § 2510(1), (18). See also S. REP. NO. 99-541, at 12. (1986), *reprinted in* 1986 U.S.C.A.A.N. 3555, 3566.

[162] 42 U.S.C. § 13032.

[163] S. REP. NO. 99-541, *supra* note 156, 3568.

[164] *See* 18 U.S.C. § 2510(12).

[165] Thomas R. Greenberg, Comment, *E-Mail & Voice Mail: Employee Privacy & the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 252 (1994).

[166] 18 U.S.C. § 2510(4). ECPA also continued and expanded the exceptions under which an employer may monitor employee telephone calls through the use of a telephone extension without violating the statute, provided it is done in the ordinary course of business and is a result of a necessary activity or of protecting the provider's rights or property. However, employers may not deliberately eavesdrop on employees' personal conversations without some business purpose. The storage provisions authorize disclosure to law enforcement agents if "the contents were inadvertently obtained and appear to pertain to the commission of a crime." 18 U.S.C. § 2702(b)(6).

[167] 18 U.S.C. § 2510(12) (applicable only to electronic communications transmitted on a system that affects interstate or foreign commerce).

[168] 18 U.S.C. § 2516(3).

[169] 28 U.S.C. § 2701(a)(2)-(c)(3) (emphasis added).

[170] DOJ COMPUTER SEARCH GUIDELINES, *supra* note 8, at 46.

[171] 18 U.S.C. § 2703(a).

[172] 18 U.S.C. § 2510(17) [emphasis added].

[173] DOJ COMPUTER SEARCH GUIDELINES, *supra* note 8, at 48.

[174] *See* 18 U.S.C. § 2515 (providing that "[w]henever any wire … communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial").

[175] 18 U.S.C. § 2708 (stating explicitly that these "are the only judicial remedies and sanctions for violations of [the Stored Communications Act]").

[176] 155 F.3d 1051 (9th Cir. 1998).

[177] After listening to the message, the informant electronically forwarded it to her own voice mailbox, then played that message from her home telephone and recorded it using a handheld tape recorder. The subsequent investigation stemmed from her delivery of the tape to yet another co-worker, who in turn delivered it to the United States Attorney, together with his interpretation of the names mentioned in the message and identifying the defendant as the speaker.

[178] 28 U.S.C. §2510(1) (defining wire communication as any aural transmission by wire, and "any electronic storage of such communication"). *See also* 18 U.S.C. § 2510(17) (defining "electronic storage" to include "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"); *but cf.* Smith, 155 F.3d 1051,1056 (discussing conflicting excerpts from the legislative history of the statutes).

[179] *See* Greenberg, *supra* note 160 (for the same analytical model).

[180] *See* United States v. Turk, 526 F.2d 654 (5th Cir. 1976) (holding that replaying a previously recorded conversation does not constitute an interception). See also, ECPA, *supra* note (including stored information in the definition of wire communications).

[181] Smith, 155 F.3d at 1057. *See also* Steve Jackson Games v. Secret Service, 36 F.3d 457 (5th Cir.1994); Wesley College v. Pitts, 974 F. Supp. 375 (D. Del. 1997); Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996); U.S. v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996).

[182] Smith, 155 F.3d at 1057.

[183] *Id*. at 1058. *See also* 18 U.S.C. § 2510(4) (defining intercept, but not access).

[184] Smith, 155 F.3d at 1059.

[185] The court ultimately sustained the conviction. *See* 18 U.S.C. § 2515 (prohibiting the use of evidence derived from the unlawful seizure, and construing "evidence derived therefrom" under the Fourth Amendment). Chandler v. United States, 125 F.3d 1296 (9th Cir. 1997). Although 18 USC § 2515 has no clean hands exception allowing the government to use evidence if it was not a party to the unlawful seizure, the attenuated basis exception set forth in Wong Sung v. United States, 371 U.S. 471 (1963) applied in view of the minimal role the voice mail actually played in the development of the case.

[186] 18 U.S.C. § 2711(2).

[187] DOJ COMPUTER SEARCH GUIDELINES, *supra* note 8, at 85.

[188] DOJ COMPUTER SEARCH GUIDELINES, *supra* note 8.

[189] IITRI CARNIVORE REPORT, *supra* note 5.

[190] This is a summary of what I have reported earlier in this article. *See, e.g.*, *supra* ¶¶ 13-15 (as to simplicity of the system) and 48-55 (as to FBI controls).

[191] *See id*.

[192] *See supra* at ¶ 75.

[193] United States Attorney's Manual, ch. 8-7.110, 28 U.S.C. § 2516(3).

[194] *See supra* at ¶ 50 (as to FBI procedures).

[195] 18 U.S.C. § 2516(3) (referring to FED R. CRIM. P. 54(c) to define the term "attorney for the government").

[196] 18 U.S.C. § 2516(2) (mandating that the state attorney must have authority under a state statute to seek authorization for electronic communications intercepts, and the state judge must conform to both the applicable state statute and to federal law).

[197] 18 U.S.C. § 2516(3) [emphasis added].

[198] *See* IITRI CARNIVORE REPORT, *supra* note 5, at **§** 5.2.

[199] United States Attorney Manual, *supra* note 184, at ch. 9-7.010.

[200] U.S. CONST. amend. IV [emphasis added].

[201] *See, e.g.,* In Re Grand Jury Subpoenas, 926 F.2d 847 (9th Cir. 1991).

[202] 610 F.2d 1 (1st Cir. 1979).

[203] United States v. Offices Known as 50 State Distributing Co., 708 F.2d 1371 (9th Cir. 1983). *See also* United States v. Bentley, 825 F.2d 1104 (7th Cir.), *cert. denied*, 484 U.S. 901 (1987).

[204] *See* United States v. Tamura, 694 F.2d 591 (9th Cir 1982) (holding that because most of the documents seized were outside the scope of the warrant, the seizure was improper).

[205] *See* IITRI CARNIVORE REPORT, *supra* note 5, at **§** 3.3.1.1.

[206] *See id*. at **§** 3.4.4.1.

[207] *See supra* Part 2.1.4.

[208] As pointed out in Part 2, that address may be an IP address [fixed or dynamic] or an e-mail address. In reality, it is likely that the target will have several such addresses associated with his name, so even this criteria may become dangerously broad. *Id*.

[209] *See id*. at **§** 3.4.2.

[210] *See id.* at **§** 3.2.2.

[211] An ISP, short for internet service provider, is a company that provides access to the Internet. For a monthly fee, the service provider gives you a software package, username, password and access phone number. Equipped with a modem, you can then log on to the Internet and browse the World Wide Web and USENET, and send and receive e-mail. In addition to serving individuals, ISPs also serve large companies, providing a direct connection from the company's networks to the Internet. ISPs themselves are connected to one another through *Network Access Points (NAPs)*. ISPs are also called *IAPs (Internet Access Providers)*. See Internet.com, *Webopedia*, *available at* http://www.webopedia.com/TERM/I/ISP.html (last visited Aug. 28, 2001].

[212] 18 U.S.C. § 2510(15); United States Attorney Manual, *supra* note 184, at ch. 9-7.