The Envelope, Please: Problems and Proposals for Electronic Mail Surveillance

The King hath note of all that they intend,
By interception which they dream not of.[1]

Introduction

Consider the envelope, and what it represents in twentieth century America. Perhaps of primary importance is the envelope's two-faceted role in the posting of mail. It provides a convenient display of necessary information for the letter's delivery, and cloaks the letter's contents from all but the recipient. Utility aside, an envelope may symbolize the ceremony of unveiling a secret, as when a ritualistic request for "The envelope, please" creates the usual suspense. An envelope may evoke sentiment, whether romantically sealed with a kiss or ominously addressed with pasted letters and numbers cut from newsprint. It is difficult to imagine a system of correspondence without the folded piece of paper that comprises the physical envelope. But advances in electronic communications portend the demise of the physical envelope and have offered no conceptual equivalent pertaining to electronic mail. A serious practical problem has emerged: how can the electronic letter display "envelope" information without betraying its contents?

Electronic mail is the transmission of letters and messages among computers via telephone lines.[2] The advent of computers in offices and homes has made the electronically sent message a practical alternative to manually delivered mail.[3] Electronic mail entails instantaneous delivery of an electronic message to a recipient's electronic mailbox,[4] avoiding the tedious delay inherent in manual mail delivery.[5] Electronic delivery of messages also provides benefits unavailable with telephone communication: a recipient need not be present to receive the entire message; a

1. W. SHAKESPEARE, THE LIFE OF HENRY V, Act II, Scene 2, at 49 (Harbage ed. 1972).

2. L. TRUDELL, OPTIONS FOR ELECTRONIC MAIL 10 (1984).

3. I. MAYER, THE ELECTRONIC MAILBOX 29-31 (1985); Gerofsky, *Electronic Message Transmission to the Home: Potential Federal Regulatory Conflicts: Congressional Action Needed,* 8 RUTGERS COMPUTER & TECH. L.J. 305 (1981).

4. The "mailbox" may be the recipient's computer terminal, or a file within an electronic mail agency's host computer, depending on the form of electronic mail in use. *See infra* notes 25-36 and accompanying text.

5. I. MAYER, *supra* note 3, at 30-31.

message may be sent to multiple recipients simultaneously; and a recipient may print the message with a printer.[6] Electronic mail services have flourished because of these advantages, and an increasing number of businesses and home computer users rely on electronic mail to send and receive correspondence.[7]

Telephone calls, letters, and electronic mail leave trails of logistical information such as phone numbers dialed, postmarks, and return addresses. Various procedures permit governmental access to these data for use in law enforcement efforts. One such procedure, the mail cover, allows law enforcement agents to collect information displayed by the envelopes of letters. Pursuant to the mail cover procedure,[8] agents may ask the Chief Postal Inspector to compile all information on the outside of a suspect's mail into a record for use by the agents.[9] Since information displayed by an envelope is not an interest protected by the Fourth Amendment, investigative agents may apply mail cover without obtaining a search warrant.[10]

Increasing reliance on electronic mail suggests that an electronic mail cover may be useful for law enforcement purposes.[11] This Note discusses the procedural and constitutional complications attendant to defining and regulating electronic mail cover. First, the Note outlines the development of electronic communications, including electronic mail, and identifies methods which are used to monitor communications. Second, it presents the constitutional analysis which distinguishes a governmental search from a governmental surveillance, and examines the application of this analysis to specific techniques used by government agents to monitor communications. After applying this analysis to electronic mail surveillance, this Note suggests that electronic mail cover should be defined and regulated to prevent governmental misuse, and submits a two-part proposal for electronic mail surveillance. Finally,

6. *Id.* at 15-17. *See also* Rodgers, *Legal Communications Network*, NAT'L L.J., Apr. 16, 1984, at 14, col. 1, *reprinted in* AMERICAN BAR ASSOCIATION, LAWYERS ON LINE: ETHICAL PERSPECTIVES IN THE USE OF TELECOMPUTER COMMUNICATION 114-15 (1986) [hereinafter LAWYERS ON LINE]; Couric, *Electronic Mail Means Instant Delivery*, 71 A.B.A. J. 96 (1985), *reprinted in* LAWYERS ON LINE, *supra*, at 137-39.

7. "Industry sources estimate that five million Americans now use electronic mail, either through the commercial networks operated by such firms as MCI, GTE Telenet and Dialcom or through corporate networks that link geographically dispersed divisions by telephone lines and computer terminals." Tyler, *Electronic Messages and Privacy Rights*, Wash. Post, Jan. 20, 1986, at A17, col. 1. These 5 million Americans generate approximately 250 million messages annually. *Id. See also* Gerofsky, *supra* note 3, at 305.

8. The mail cover is authorized and regulated by 39 C.F.R. § 233.3 (1986). *See infra* notes 43-48 and accompanying text.

9. 39 C.F.R. § 233.3(c), (d) (1986).

10. *See infra* notes 86-94 & 108-117 and accompanying text.

11. See Webster, *Sophisticated Surveillance—Intolerable Intrusion or Prudent Protection?*, 63 WASH. U.L.Q. 351, 353, 364 (1985), for a discussion on the need for electronic surveillance procedures which provide police with proper investigative power to ensure public safety.

this Note discusses constitutional problems likely to arise if an increasingly powerful surveillance device—electronic mail cover—persists unrestrained by the Fourth Amendment's warrant requirement.

I. Electronic Mail Communication

A. The Historical Development of Communications in the United States

The diversity and accessibility of modern communications methods reflect a precedent in the United States for developing intranational and international communications. The importance of providing effective correspondence to early Americans was duly noted by Alexis de Tocqueville, who observed that the strength and success of a general government in the United States depended largely on "that great instrument of intercourse," the post.[12] Failure to construct and maintain postal roads would induce mutual estrangement among the physically scattered colonists, crippling the emergence of federal power.[13] The early Americans did not succumb to physical isolation, however, and instead built postal roads and steamboats to facilitate national delivery of the mails.[14]

The zeal of early Americans for maintaining and improving the post has been sustained in the twentieth century, and has produced a vast array of communications techniques. One of the first contributors to the array, Samuel Morse, after discovering a method to communicate via electricity, introduced his telegraph in 1836.[15] By 1844, refinement of Morse's model provided nearly instantaneous communication between two cities.[16] The success of the telegraph was bolstered by the invention of a "harmonic telegraph," by which a wire could carry various musical pitches at once.[17] The harmonic telegraph was a prototype for a device which transmitted multiple messages over a single telegraph wire.[18] Popular demand for telegraph communication sparked the invention of the telephone in 1876,[19] and radio signal transmission in 1895 provided the first wireless telegraph.[20]

The 1920's and 1930's witnessed the spread of telephones and radios into American homes,[21] followed by "the dawn of the television era" in

12. 1 A. DE TOCQUEVILLE, DEMOCRACY IN AMERICA 404-05 (Bowen rev. 1945). De Tocqueville marvelled at the American propensity for building post roads in unsettled areas. *Id.* at 405 n.79.

13. *Id.* at 404-06.

14. *Id.* at 405 n.80.

15. G. BROCK, THE TELECOMMUNICATIONS INDUSTRY 55-56 (1981).

16. *Id.* at 56.

17. *Id.* at 89.

18. *Id.*

19. *Id.* at 90.

20. R. THOMAS, TELECOMMUNICATIONS FOR THE EXECUTIVE 3 (1984).

21. *Id.* at 1-5.

the 1950's.[22] Technologies of the nineteenth and twentieth centuries have coalesced into a sophisticated, interwoven telecommunications environment.[23] The transmission of vocal and electronic data via telephone networks and satellites enables instantaneous exchange of information around the world.[24]

B. Electronic Mail

One method of exchanging information rapidly—electronic mail—uses computers and telephone lines to transmit correspondence.[25] Electronic mail represents a synthesis of written correspondence and telecommunications.[26] There are two basic arrangements which provide for sending mail electronically. One method links the correspondents' computers through telephone lines which transmit messages directly among computers and correspondents. This arrangement requires that each electronic correspondent have access to a computer with a word processor,[27] modem,[28] and communications software to orchestrate the trans-

22. Wilson, *The Pay Cable TV-Sports Broadcasting Nexus,* 8 COMM. & LAW 43, 45 (1986). It is currently estimated that 98% of American homes have television sets. *TV of the Future at D.C. Preview,* San Francisco Chron., Feb. 10, 1987, at 58, col. 1.

23. R. THOMAS, *supra* note 20, at 3. *See also* Geller & Brotman, *Electronic Alternatives to Postal Service,* in COMMUNICATIONS FOR TOMORROW: POLICY PERSPECTIVES FOR THE 1980'S, at 320-22 (G. Robinson ed. 1978) [hereinafter COMMUNICATIONS FOR TOMORROW].

24. Telephone networks permit electronic communication via narrowband transmission. This provides the means of electronic mail arrangements currently in use. A different form of electronic mail is provided by the broadband transmission of satellites. One satellite system in development will provide two-way voice, data, and image service through small antennas located on the subscriber's premises. This Note does not address the consequences of surveillance of broadband transmission since it is not currently cost effective compared to the earthbound economy provided by narrowband (telephone line) transmission. R. THOMAS, *supra* note 20, at 118-19. For a discussion of probable future additions to the telecommunications array, see *id.* at 113-22.

25. Detailed explanations of electronic mail are provided by I. MAYER, *supra* note 3, and L. TRUDELL, *supra* note 2.

26. The advantages of electronic mail are numerous. *See generally* LAWYERS ON LINE, *supra* note 6, at 114-15. For a discussion of the usefulness of electronic message transmission within a law office, see *id.* at 137-39. One particular electronic message system—ABA/NET—offers an electronic mail network for lawyers which allows the transmission of an electronic message among subscribing offices across the country within 15 minutes. For a discussion of the ABA/NET facility, see Shuey, *The Expansion of Telecommunications in the Law Office,* 14 COLO. LAW. 1419, 1419-20 (1985).

27. A word processor is a computer program which provides the capacity to write at the computer, and to save, edit, and print the document. *See* R. THOMAS, *supra* note 20, at 91; *see also* J. DEKEN, THE ELECTRONIC COTTAGE 333-35 (1980).

28. A modem is a device which enables the transmission of electronic data among computers using telephone lines. R. THOMAS, *supra* note 20, at 67. For an explanation of the technology by which telephone lines transmit computer data, see G. BROCK, *supra* note 15, at 266-68.

mission of messages among the computers.[29] The sender[30] types a message (the "letter") into the computer and specifies the recipient.[31] The communications software links the sender's terminal directly to the recipient's terminal over telephone lines accessed by each correspondent's modem.[32] The recipient need not be present to receive the message; the software can record the full communication to be read subsequently.[33]

In the alternative electronic mail arrangement, a correspondent subscribes to the services provided by an electronic mail agency.[34] Equipment necessary for this communication includes a computer and word processor, telephone, modem, and a subscription to an electronic mail service. The electronic mail service provides a central computer which holds electronic messages en route between correspondents. The sender types a message into the word processor, indicating the letter's destination, and the modem transmits the message over a phone line to the electronic mail agency's host computer. There the message may be directly routed to the addressee's computer or held until the addressee electronically collects the message from the host computer.[35] Some services will print the electronic message and send it off via the United States Postal

29. For example, MCI Corporation markets a computer-to-computer electronic mail system which enables the sender to type a message at her computer and transmit it directly to another registered MCI Mail user. Elman, *Mail Messaging's Sticky Legal Issues*, PERSONAL AND PROFESSIONAL, vol. 2, no. 3, at 30 (1984), *reprinted in* LAWYERS ON LINE, *supra* note 6, at 127.

30. The distinction between "sender" and "recipient" blurs in some electronic mail arrangements. For example, the ostensible sender may be calling to retrieve mail from another's computer. Or electronic mail may be sent and received in a single telephone transmission in which the caller deposits her message and picks up the message left by another correspondent. The form of delivery and pick up depends on the options provided by the communications software, and the arrangement selected by the correspondents. For a detailed survey of the variety of electronic mail configurations, see I. MAYER, *supra* note 3, at 49-153.

31. There may be multiple recipients to whom the message is sent simultaneously. LAWYERS ON LINE, *supra* note 6, at 138.

32. *Id.*

33. Gupta, *Living in a Legal Village,* BARRISTER, Winter 1984, at 64, *reprinted in* LAWYERS ON LINE, *supra* note 6, at 126.

34. A representative electronic mail agency service is that offered by MCI Corporation. The service provides a depository for electronic mail, which computer users may use to communicate and transmit text over the phone between computers. The sender calls the service and places the message at any time of day or night in MCI's central computer, where it is stored until the recipient retrieves it. LAWYERS ON LINE, *supra* note 6, at 127. Other communications carriers offering electronic mail services are: Tymshare (OnTyme), GTE Telenet (Telemail), ITT (DialCom), CompuServe, and The Source. L. TRUDELL, *supra* note 2, at 53.

35. The recipient picks up her mail by connecting with the mail service through her computer, modem, and identification number. She may display the message on her terminal or print it on a printer. L. TRUDELL, *supra* note 2, at 18-19. Some services offer arrangements whereby a subscriber may send an electronic message to the agency, where it is then printed, put into an envelope, and delivered by the United States Postal Service (or private mail carrier) to the recipient. LAWYERS ON LINE, *supra* note 6, at 139.

Service, which facilitates sending electronic messages to recipients who do not have electronic mail capacity. If the recipient is not an electronic mail user, delivery of out-of-town correspondence is nonetheless expedited because the sender's message is instantaneously transmitted to the host computer closest to the letter's destination, where it may be printed for pick up by or delivery to the recipient.[36]

Each electronic mail arrangement has advantages and idiosyncracies. Directly transmitted electronic mail ("terminal-to-terminal" mail) is instantly deliverable, but requires both correspondents to have access to electronic mail equipment and compatible electronic mail software. In contrast, a recipient of electronic mail sent through an agency ("terminal-via-agent" mail) does not need electronic mail equipment, since the agency may print the electronically received message and provide for delivery or pick-up. Cost is an additional consideration.[37] Permutations of these two arrangements are possible,[38] but the variations are based on either a terminal-to-terminal or a terminal-via-agent set-up.[39]

II. Techniques and Procedures for Monitoring Communications

Advances in technology which have facilitated the convenient, efficient exchange of information have concurrently produced sophisticated methods for monitoring the exchange of information.[40] The assortment of methods employed by government agents to watch a suspect's commu-

36. LAWYERS ON LINE, *supra* note 6, at 138-39.

37. There are many rapidly changing variables which affect the cost of an electronic mail arrangement. For both types of electronic mail, these variables include the cost of the computer equipment, word processor, and modem. Direct electronic mail requires purchase of a communications software package; indirectly transmitted mail requires subscription to an electronic mail agency. Both forms of electronic mail entail transmission of data over telephone lines, and the cost to use phone lines to transmit electronic data is calculated similarly to conventional phone use: length of communication and distance are controlling. For electronic mail sent via agency, costs increase if the recipient is not a subscriber, and vary according to whether the United States Postal Service, Western Union, or other private delivery services are involved. *Id. See also* I. MAYER, *supra* note 3, at 31-39.

38. For example, a correspondent may use her computer to transmit a message to a telex service, which forwards the message to the recipient by teletype. I. MAYER, *supra* note 3, at 16-17. Or a facsimile service may be used by one correspondent, whereby a printed report is electronically photocopied and transmitted over phone lines to an electronic mail recipient. For an explanation of facsimile and its integration with electronic mail transmission, see L. TRUDELL, *supra* note 2, at 137-39.

39. It is possible to send electronic mail through satellite hookups, using broadband transmission, rather than through narrowband transmission provided by telephone networks. Satellite transmission, however, requires equipment which ordinarily is unnecessarily expensive and elaborate for the average electronic mail user. *See supra* note 24.

40. For a brief listing and explanation of a variety of electronic surveillance techniques which have emerged, see Landever, *Electronic Surveillance, Computers, and the Fourth Amendment—The New Telecommunications Environment Calls for Reexamination of Doctrine,* 15 U. TOL. L. REV. 597, 602 (1984).

nication mirrors the assorted mediums of communication. Governmental monitoring of a communication may occur at two levels: intercepting a communication's message, or acquiring information as to its logistics. The following survey of investigative techniques illustrates that the distinction between content and logistics creates different procedures applicable to a single communication.

A. Monitoring Mailed Communications

Letters and other mailed material contain written information which may interest law enforcement agents in their surveillance of communications. A posted letter's envelope supplies information needed for delivery and enfolds the letter's message. Two ways to monitor mail result: collection of data from the envelope, and collection of data from the letter itself. There is no specific method which permits law enforcement agents to open mailed material and record its content. Instead, since monitoring the content of mail comprises a governmental search,[41] the pertinent procedure is supplied by the fourth amendment search warrant requirement: police must show probable cause for suspecting the subject of the search, and must specifically describe the thing to be searched.[42] The warrant requirement severely inhibits substantive mail searches, but mail search may be used by police under circumstances which satisfy the Fourth Amendment's procedural requirements.

Although no specific procedure governs the search of a letter's content, there is a defined method which regulates governmental access to a letter's envelope information: the mail cover. Law enforcement agents may use mail cover to collect all information discernible from the outside of a suspect's mail.[43] The Chief Postal Inspector's statutory authority to compile such a record[44] is circumscribed by the requirement that the

41. More than a century ago, the Supreme Court disallowed governmental opening of first class mail without a search warrant:

> 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.

Ex parte Jackson, 96 U.S. 727, 733 (1877).

42. U.S. CONST. amend. IV.

43. 39 C.F.R. § 233.3(c)(1) (1986):

> "Mail cover" is the process by which a record is made of any data appearing on the outside cover of any class of mail matter . . . in order to obtain information in the interest of (i) protecting the national security, (ii) locating a fugitive, or (iii) obtaining evidence of commission or attempted commission of a crime.

44. The statutory scheme authorizes the Chief Postal Inspector, or her designee, to order mail covers:

> When written request is received from any law enforcement agency wherein the requesting authority stipulates and specifies the reasonable grounds that exist which demonstrate the mail cover is necessary to (A) protect the national security, (B) lo-

requesting agency apprise the Postal Inspector of a legitimate reason to institute the surveillance.[45] Information obtainable pursuant to mail cover is only that which appears on the envelope or covering of the suspect's mail; government agents may not open the mail.[46] Mail cover surveillance initially may be applied for up to thirty days.[47] This period may be extended upon the request of law enforcement agents, after showing the Postal Inspector that the original reason for the surveillance remains.[48]

B. Monitoring Telephone Communications

Governmental monitoring of spoken telephone communication may take two forms: surveillance of the logistics of a telephone connection, or interception of a conversation's content. Access to a conversation's content is effected with a wiretap, which directly intercepts the transmission of telephone communication from phone lines.[49] Explicit regulation of governmental wiretapping is codified in the Omnibus Crime Control and Safe Streets Act of 1968,[50] which requires police to obtain a search warrant prior to installing a wiretap.[51]

There are several techniques available to law enforcement agents which provide surveillance of the logistics of a telephone connection. Pursuant to one technique, law enforcement agents may examine records maintained by telephone companies for billing purposes.[52] This information is needed to calculate long distance (toll) call charges; the records list the long distance numbers dialed, what time the calls were placed, and the length of the calls.[53] When law enforcement agents are interested in a suspect's local phone usage, which may not have been recorded by the suspect's phone company, surveillance of those calls may be implemented with electronic devices. One such device is the pen register.[54]

---

cate a fugitive, or (C) obtain information regarding the commission or attempted commission of a crime.

Id. at § 233.3(d)(2)(ii).

45. No showing of probable cause is required. *Id.*

46. "No person in the Postal Service . . . may break or permit breaking of the seal of any matter mailed as first-class mail without a search warrant." *Id.* at § 233.3(g)(1). Pursuant to mail cover, however, any second, third, or fourth class mail may be opened and examined without a search warrant. United States v. Choate, 576 F.2d 165, 168 n.1 (9th Cir.), *cert. denied*, 439 U.S. 953 (1978).

47. 39 C.F.R. § 233.3(g)(4) (1986).

48. *Id.* at § 233.3(g)(4)-(5).

49. J. CARR, THE LAW OF ELECTRONIC SURVEILLANCE § 1.1(a) (1986).

50. 18 U.S.C. §§ 2515-2518 (1968).

51. *Id.*

52. J. CARR, *supra* note 49, at § 3.3(a).

53. *Id.*

54. The pen register is defined as:

A device connected to a telephone instrument or line that permits the recording of telephone numbers dialed from a particular telephone instrument. "Pen register"

The pen register is installed at a central telephone facility,[55] and records all numbers dialed on a telephone by monitoring the electrical impulses created by dialing the phone.[56] The pen register also records the time a call is placed and the number of rings at the telephone number dialed.[57] It does not overhear oral communications and does not indicate whether the calls are actually completed.[58] Government use of the pen register is regulated: agents must provide the telephone company with reasonable grounds for using the pen register,[59] and the surveillance may last for thirty days,[60] after which an extension may be granted.[61]

Two additional electronic techniques provide surveillance similar to that of the pen register: a diode device and a dialed number recorder. In contrast to a pen register's list of outgoing calls, a diode reveals information from incoming phone calls—the phone numbers of those who dial into a suspect's telephone.[62] The dialed number recorder provides information from both incoming and outgoing telephone communications: the numbers dialed out of a suspect's phone, the origin of incoming calls, and the duration of calls.[63] No explicit procedure regulates governmental use of diodes or dialed number recorders, but courts have held that the pen register procedure controls governmental installation of these devices.[64]

These techniques—mail search, mail cover, wiretapping, examining toll records, pen register, diode, and dialed number recorder—are tools which supply government agents with the technical capacity to monitor communications. Raw technical ability, however, is circumscribed by constitutional limits, and the availability of each technique depends on its categorization under the Fourth Amendment.

---

also includes decoder devices used to record the numbers dialed from a touch-tone telephone. "Pen register" does not include equipment used to record the numbers dialed and duration of long-distance telephone calls when the equipment is used to make such records for an entire telephone system and for billing or communications management purposes.

32 C.F.R. § 42.6(h) (1986).

55. United States v. Giordano, 416 U.S. 505, 549 n.1 (1974) (Powell, J., concurring in part and dissenting in part).

56. United States v. New York Tel. Co., 434 U.S. 159, 161 n.1 (1977).

57. *Id.*

58. *Id.*

59. 32 C.F.R. § 42.7(b) (1986).

60. *Id.* at § 42.7 (a)(1)(iv)(2).

61. *Id.*

62. J. CARR, *supra* note 49, at § 3.2(c)(2)(C).

63. *Id.*

64. *See infra* notes 128-131 and accompanying text.

III. Fourth Amendment Restraints on Governmental Monitoring of Communications

The ease with which a specific procedure may be applied to monitor communication depends on whether the activity comprises a governmental search under the Fourth Amendment.[65] This determination serves to identify the limits on procedures used by police to collect data. If the procedure is a search, it is permissible only pursuant to a valid search warrant issued by a judicial magistrate upon a proper display of probable cause and descriptive detail.[66] A procedure which is not a search, but rather a surveillance, is available to law enforcement agents without judicial supervision or approval. If an electronic mail cover is to be permitted without a search warrant, its procedure must be carefully defined to avoid being judicially labelled as a search. Of critical importance, therefore, is to identify the analysis courts use in distinguishing search from surveillance, and extend it to proposals for electronic mail cover. An understanding of this analysis begins with a survey of the constitutional principles derived from the Fourth Amendment.

A. The Historical Purpose and Scope of the Fourth Amendment

The Fourth Amendment to the Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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.[67]

The Framers included the Fourth Amendment in the Bill of Rights largely because of perceived abuses of the "writs of assistance" used by colonial officials in Massachusetts.[68] A writ allowed colonial officials to search a suspect's home for smuggled goods.[69] The English Parliament

65. *See infra* notes 75-94 and accompanying text.

66. U.S. CONST. amend. IV. A few governmental actions are deemed to be searches, but nonetheless permitted without search warrants in strictly defined circumstances. One significant example is the power of police to "frisk," or carry out a superficial search for weapons on the person of a suspect. Terry v. Ohio, 392 U.S. 1 (1968). Another exception to the warrant requirement is a search incident to arrest. Chimel v. California, 395 U.S. 752 (1969). Additionally, objects in plain view of an officer who has a right to be in that position of view may be seized and introduced into evidence without a search warrant. Harris v. United States, 390 U.S. 234 (1968). A warrantless search may be sustained where the court finds it to have been impossible or unwise to first obtain a warrant. This is the "exigent circumstances" exception, and it applies in cases where police are in "hot pursuit" of a suspect, or where evidence is likely to be destroyed prior to obtaining a search warrant. Warden v. Hayden, 387 U.S. 294 (1967).

67. U.S. CONST. amend. IV.

68. J. STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES 647-48 n.c (5th ed. 1891).

69. *Id.* at 649.

approved the writs, which permitted general searches unrestricted in scope.[70] In addition, prior to 1763,[71] colonial officials could acquire general arrest warrants which authorized apprehension of unnamed and undescribed suspects.[72] To curtail the inherent abuse of writs of assistance and general warrants, the Framers desired an explicit proscription of general searches and arrests, and codified that desire in the Fourth Amendment.[73]

The original purposes of the Fourth Amendment—to inhibit abusive police practices and to proscribe governmental intrusion into the inner recesses of an individual's life[74]—have endured uncompromised by dramatic social changes in the United States over the course of two centuries. In contrast, the scope of the Fourth Amendment has proven to be vulnerable to mercurial influences, such as changing mores and idiosyncratic judicial analyses. For example, a basic tenet of the Fourth Amendment—protection against indiscriminate and unreasonable police searches—remains resolute, while opinions on how to achieve this policy fluctuate. This flux reflects judicial ambivalence in identifying which interests are guarded by the Fourth Amendment, and the Supreme Court accommodates this ambivalence by redefining the term "search." When it recasts the definition of search, the Court revises the scope of the Fourth Amendment, because a governmental activity which is not a search is not caught within the Fourth Amendment's protective web. Significant to developing a procedure for electronic mail cover, therefore, is to incorporate restrictions which prevent its electronic surveillance from becoming an electronic search. Ascertaining appropriate restrictions for electronic mail surveillance entails understanding the current definition of search, as historically derived from cases which have influenced the Fourth Amendment's scope.

B. The Scope of the Fourth Amendment Today: The Definition of Search

One of the earliest decisions of significance in deriving the current definition of a search was *Boyd v. United States*.[75] The Court in *Boyd* designated property interests as the beneficiaries of fourth amendment protection: a government surveillance which did not infringe an individual's property interest was not a search and could be implemented without a search warrant.[76] Numerous subsequent Court decisions relied on

70. *Id.* at 648-50.

71. In 1763, the use of general arrest warrants was judicially disapproved. *Id.* at 649.

72. *Id.* at 650.

73. A. PUTNEY, UNITED STATES CONSTITUTIONAL HISTORY AND LAW § 240 (1985).

74. P. DIONISOPOULOS & C. DUCAT, THE RIGHT TO PRIVACY: ESSAYS AND CASES 15 (1976).

75. 116 U.S. 616 (1885).

76. *Id.* at 627.

the *Boyd* analysis.[77] Of particular note are two cases in which the Court considered the fourth amendment status of electronic eavesdropping. The first of the two, *Olmstead v. United States*,[78] held that a wiretap which had not physically intruded upon the defendant's premises was not a search because "the Constitution does not forbid [wiretapping] unless it involves actual unlawful entry into a house."[79] The *Boyd* physical intrusion requirement disqualified the surreptitious *Olmstead* wiretap as a search, and electronic eavesdropping accomplished without physical intrusion required no search warrant.

Conversely, applying *Boyd* to hidden microphone eavesdropping in *Silverman v. United States*,[80] the Court concluded that a search had occurred because a microphone used by the police had been placed in an outside wall of the defendant's premises.[81] The *Boyd* test of physical intrusion was met by the *Silverman* microphone which had physically intruded upon a protected area—the defendant's premises—and therefore comprised a search constrained by the warrant requirement.[82] This vestige of *Boyd*—that the Fourth Amendment protected only interests with physical dimension—survived until the Court "discarded fictional and procedural barriers rested on property concepts" in *Warden v. Hayden*.[83]

Shortly after *Warden*, the Supreme Court bestowed further judicial insight as to the elusive definition of a "search." In *Katz v. United States*,[84] law enforcement agents suspected the defendant of violating a federal statute[85] by using a telephone to transmit illegal bets. The defendant habitually used a particular phone booth, and government agents placed a wiretap on the outside of the phone booth to record the defendant's conversations in the booth. The agents had not obtained a search warrant prior to the wiretapping, and in his appeal to the Supreme Court, the defendant alleged that application of the wiretap constituted a governmental search, allowable only pursuant to a valid search warrant. The Court agreed with the defendant's assertion, holding that a search does not require a physical intrusion because "the Fourth Amendment protects people, not places."[86] *Katz* completely reformulated the scope of the Fourth Amendment: while incorporating *Warden* to extend the Fourth Amendment's scope beyond physical interests, *Katz* denied

77. *See, e.g.*, Stoner v. California, 376 U.S. 483 (1964); Chapman v. United States, 365 U.S. 610 (1961); United States v. Jeffers, 342 U.S. 48 (1951); Adams v. New York, 192 U.S. 585 (1904).

78. 277 U.S. 438 (1928).

79. *Id.* at 452.

80. 365 U.S. 505 (1961).

81. *Id.* at 512.

82. *Id.*

83. 387 U.S. 294, 304 (1967).

84. 389 U.S. 347 (1967).

85. 18 U.S.C. § 1084 (1976).

86. 389 U.S. at 351.

fourth amendment protection to "[w]hat a person knowingly exposes to the public, even in his own home or office."[87]

Justice Harlan, in his concurring opinion in *Katz*,[88] composed a two-part analysis to determine when a surveillance becomes a search which is restricted by the warrant requirement. First, the person subjected to the alleged search must have *actually* expected her interest to be treated by others as if it were private.[89] Second, if the subject did harbor such an expectation of privacy, her expectation must have been objectively reasonable.[90] Justice Harlan's formulation has provided courts with a paradigm for determining whether a governmental activity comprises a fourth amendment search. The consistency with which cases since *Katz* have invoked Harlan's two-part test is testimony to its endurance as a practicable standard.[91] The paradigm may thus be summarized: a governmental procedure is a search if it intrudes on an interest which the suspect actually and reasonably expected to be treated by others as private[92] to the suspect. If the suspect harbored no conscious expectation of privacy as to the infringed interest, or if the suspect's expectation of privacy was not reasonable, then the interest is not protected under the Fourth Amendment, and any governmental intrusion on the interest does not comprise a fourth amendment search.[93] This analysis is invoked by courts to examine the constitutionality of particular governmental procedure,[94] and a consensus from these holdings will illuminate the constitutional status of electronic mail cover.

---

87. *Id.*

88. *Id.* at 361 (Harlan, J., concurring).

89. *Id.*

90. *Id.*

91. "In determining whether a particular form of government-initiated electronic surveillance is a 'search' within the meaning of the Fourth Amendment, our lodestar is *Katz*." Smith v. Maryland, 442 U.S. 735, 739 (1979). *See also* Rakas v. Illinois, 439 U.S. 128, 143 & n.12 (1978); United States v. Brock, 667 F.2d 1311, 1319-20 (9th Cir. 1982).

92. A different privacy analysis is used by Justice Douglas to identify a constitutional "right to privacy" for individuals. Griswold v. Connecticut, 381 U.S. 479, 483, 486 (1965). *Griswold*'s "right to privacy," derived from six constitutional Amendments, *id.* at 484-85, is not interchangeable with *Katz*'s "zone of privacy," 389 U.S. at 350-51, which derives from the Fourth Amendment. Although the right to privacy is the fundamental interest protected by the Fourth Amendment, *id.* at 351, "[t]he Fourth Amendment cannot be equated with a general right to privacy, since Fourth Amendment protections extend beyond privacy interests." *Id.* at 350. *See also Brock*, 667 F.2d at 1319 n.7; Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 359 (1974).

93. *See* Note, *The Impact of* Smith v. Maryland *on the Law of Pen Registers*, 1 ANTIOCH L.J. 65, 70-71 (1981) [hereinafter Note, *Pen Registers*].

94. *See infra* notes 95-117 and accompanying text.

IV. Methods of Monitoring Communications Without a Search Warrant

A. Pen Registers and Tracing Devices

In *United States v. New York Telephone Co.*,[95] the Supreme Court held that a pen register does not violate the Fourth Amendment because it is not a search. The Court explained this conclusion by noting that only insignificant information is revealed by the pen register:

> Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.[96]

The information obtained by the pen register was sufficiently trivial to disqualify it from any reasonable expectation of privacy, and thus did not comprise an interest protected by the Fourth Amendment under the second part of the *Katz* test.

New York Telephone emphasized the distinction between the means of communication, which law enforcement agents may monitor without a warrant, and the constitutionally protected purport of a communication. The Court in *Smith v. Maryland*[97] found this distinction equally compelling. In *Smith*, the Court held that installation and use of a pen register at a telephone company's office to record numbers dialed by the defendant was not a search and violated no expectation of privacy.[98] The Court distinguished the pen register from a wiretap,[99] which records the *substance* of a communication.[100] The pen register gathered only "non-substantive" information, to which no objective expectation of privacy attached.[101] Therefore, the pen register did not intrude on a protected private area under the *Katz* test and was not a search within the meaning of the Fourth Amendment.[102] Another factor which influenced the *Smith* holding was that the defendant *voluntarily* disclosed phone numbers he dialed to the phone company whenever he dialed a phone number.[103] Voluntary disclosure[104] precluded recognition of any reason-

95. 434 U.S. 159 (1977).
96. *Id.* at 167.
97. 442 U.S. 735 (1979).
98. *Id.* at 745-46.
99. A wiretap intercepts the communication transmitted over the telephone wires, and may not be applied by law enforcement agents without a search warrant. J. CARR, *supra* note 49, at § 1.1(a).
100. 442 U.S. at 741.
101. *Id.* at 743-45.
102. *Id.* at 745-46.
103. *Id.* at 743-44.

able expectation of privacy with regard to those numbers.

Unlike the federally regulated pen register procedure,[105] a governmental procedure for installing a diode device, or trace, to record numbers from incoming phone calls has not been defined. But the judicial analysis of this technique employs the pen register analysis:

> [T]he same rules applicable to pen registers also control the installation of other mechanical or electrical devices designed to trace incoming calls. The equipment used in tracing phone calls is similar to a pen register in that it does not accomplish an "aural acquisition" within the meaning of [the Safe Streets Act]. Traces, like pen registers, neither hear nor monitor contents.[106]

Furthermore, the dialed number recorder, distinguished from the pen register by its capacity to trace both incoming and outgoing calls, nevertheless acquires no "contents" of conversation, and is therein analogous to the pen register for purposes of procedural guidance.[107]

B. Mail Cover

The Supreme Court has declined to consider the constitutionality of the mail cover.[108] Its refusal to address the issue, however, is attributed to the similarity between the mail cover and the pen register under a fourth amendment search analysis.[109] Federal courts which have ruled on the mail cover consistently invoke the Supreme Court's analysis of the pen register as set forth by *New York Telephone* and *Smith*.[110] In *Vreeken v. Davis*,[111] the Tenth Circuit Court of Appeals examined the constitutionality of mail cover, analogizing mail cover to the pen register. The court found the pen register analysis from *Smith* to be determinative:

---

104. The Court contended that an individual who voluntarily conveys numerical information to the phone company assumes the risk that the company would reveal the information to the police. *Id.* at 744. But Justice Marshall, in dissent, provides a compelling argument criticizing the legitimacy of the "voluntary disclosure" rationale: "[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." *Id.* at 750 (Marshall, J., dissenting).

105. The pen register is defined in 32 C.F.R. § 42 (1986). *See supra* notes 54-61 and accompanying text.

106. Michigan Bell Tel. Co. v. United States, 565 F.2d 385, 388 (6th Cir. 1977).

107. State v. Miller, 449 A.2d 1065, 1067 (Del. Super. Ct. 1982).

108. *See, e.g.*, United States v. Choate, 576 F.2d 165 (9th Cir.), *cert. denied,* 439 U.S. 953 (1978); United States v. Bianco, 534 F.2d 501 (2d Cir.), *cert. denied,* 429 U.S. 822 (1976); United States v. Leonard, 524 F.2d 1076 (2d Cir. 1975), *cert. denied,* 425 U.S. 958 (1976); United States v. Balistrieri, 403 F.2d 472 (7th Cir. 1968), *cert. denied,* 402 U.S. 953 (1971).

109. *See, e.g.*, Vreeken v. Davis, 718 F.2d 343, 347 (10th Cir. 1983); United States v. Choate, 576 F.2d at 175-77.

110. *See, e.g.*, cases cited *supra* notes 108-109.

111. 718 F.2d 343 (10th Cir. 1983).

> [T]he mail cover at issue in the instant case is indistinguishable in any important respect from the pen register at issue in *Smith*. The mail cover did not include an examination of the contents of any mail . . . . Courts that have addressed the question have uniformly upheld the constitutionality of mail covers on this reasoning.[112]

The mail cover in *Vreeken* did not disturb the letters' contents, but revealed only nonsubstantive information which could be granted no reasonable expectation of privacy. The *Vreeken* court thus concluded that the Supreme Court decision in *Smith* compelled a holding that mail cover was not a search and its use did not violate the fourth amendment warrant requirement.[113]

The Ninth Circuit considered the mail cover in *United States v. Choate*.[114] The opinion relied on the *Katz* privacy formulation,[115] and found no reasonable expectation of privacy pertaining to the envelope of a letter: "[L]ike any other reasonable citizen, [the defendant] could expect no privacy as to the outside of his incoming mail, . . . [the] 'lack of privacy' is not significant enough to be constitutionally impermissible when [mail cover] does not concern the substance of a communication and fits within regulatory restrictions."[116] The information voluntarily supplied on an envelope is not protected by the Fourth Amendment because no justifiable expectation of privacy exists for envelope information.[117]

Judicial analyses of mail cover, pen register, and tracing devices have concluded that those procedures do not intrude on fourth amendment interests because they reveal only voluntarily submitted information as to the means of a communication.[118] The means of a communication is not substantive information, and surveillance of that information by law enforcement agents is not within the ambit of fourth amendment protection.[119] Repeated judicial emphases distinguish the

---

112. *Id.* at 347-48.

113. *Id.* at 348.

114. 576 F.2d 165 (9th Cir.), *cert. denied*, 439 U.S. 953 (1978).

115. *Id.* at 174-75.

116. *Id.* at 181.

117. *Id.* at 176-77.

118. *See, e.g., Smith*, 442 U.S. at 743-45; *New York Telephone*, 434 U.S. at 166-67; *Vreeken*, 718 F.2d at 347-48; *Choate*, 576 F.2d at 177.

119. The dissents in *Choate*, 576 F.2d at 201-02 (Hufstedler, J., dissenting), and *Smith*, 442 U.S. at 747-48 (Stewart, J., dissenting), criticized the wisdom of this leniency. The criticisms are reiterated by commentators who have examined the holdings in those cases. *See* Note, *Mail Covers and the Fourth Amendment:* United States v. Choate, 12 LOY. L.A.L. REV. 201, 209-16 (Dec. 1978); Note, *Pen Registers, supra* note 93, at 68-76; *see also* Note, *Invasion of Privacy: Use and Abuse of Mail Covers*, 4 COLUM. J.L. & SOC. PROBS. 165, 170 (1978) (in which the author promulgates abolition of a procedure permitting mail surveillance without a search warrant). These analyses persuasively criticize the judicial refusal to categorize the pen register and mail cover as fourth amendment searches requiring search warrants. But one commentator suggests that permitting such procedures without search warrants actually safe-

content of a communication—substantive information—from the *means* of a communication—logistical information.[120] The means of communication, but not the content, may be monitored without a search warrant, because logistical information merits no fourth amendment protection, and governmental examination of logistical data is therefore not a search. Whether a governmental monitoring is a search thus pivots on determining whether the procedure reveals the content of a communication to law enforcement agents.

V. Governmental Surveillance of Electronic Mail

A. The Importance of a Procedure for Electronic Mail Cover

By monitoring a suspect's electronically sent messages, law enforcement agents might acquire information useful in efforts to ferret out crime.[121] Existing technology provides the capability to monitor electronic mail, but no procedure applies to prohibit the abuses indigenous to electronic surveillance methods.[122] The legislative reluctance to provide the needed procedure portends undesirable results, such as police misuse of electronic mail cover, which is judicially countered with excessive restraint. Faced with a flagrant governmental abuse of unregulated electronic mail surveillance, an alarmed court might respond by attaching a warrant requirement to any form of electronic mail surveillance. This result would eradicate what might have been a useful and inoffensive police procedure under proper regulation.

Legislative neglect in regulating electronic mail cover and the lack of judicial precedent in this area force inquiries on the law of electronic mail cover to draw principles from scattered but comparable surveillance procedures. This Note relies on such an approach to formulate proposals for regulating electronic mail cover. Two procedures are needed to ac-

---

guards the privacy of the contents of communications. If the showing of cause for a pen register is the same as that required for a wiretap, governmental agents would always request the more information-laden wiretap. C. FISHMAN, WIRETAPPING AND EAVESDROPPING § 28 (1978). Professor Fishman argues that civil liberties and privacy are less vulnerable when a pen register is permitted without a search warrant because the availability of the pen register may discourage governmental monitoring of the contents of a conversation, when surveillance of the means of the conversation would suffice for the particular law enforcement objective at hand. *Id.* If an electronic mail cover is to resemble a pen register, *see infra* text accompanying notes 127-136, Professor Fishman's argument merits consideration by those who would require a search warrant for its installation.

120. The courts apply various labels to differentiate the information which comprises the "content" of a communication from that which reflects the "means." The category of information deriving from the content or purport of a communication is labelled "substantive," "private," or "personal." The category of information which reflects the means of communication is labelled "nonsubstantive," "commercial," or "logistical." These terms are used interchangeably throughout this Note.

121. *See* Webster, *supra* note 11, at 353, 364.

122. Landever, *supra* note 40, at 600.

commodate the alternative methods of sending electronic mail. The first procedure supplies surveillance of mail which is sent directly from computer to computer. The second technique applies to the surveillance of letters which are sent through an electronic mail agency. The best means of implementing surveillance differs for the two forms of electronic mail.

B. A Proposal for Covering Directly Transmitted Electronic Mail

Attempted surveillance of electronic mail which is transmitted directly between two computers, independently of an electronic mail intermediary, threatens to lay bare the contents of the entire communication because nothing in the transmission separates content from logistical information—the mail is simply sent from one computer to another, over telephone lines. To extract "envelope information"—identities of sender and recipient, time, date, origin, and destination—from a direct transmission would entail interception of the entire transmission and expose its content. This interception would not provide an acceptable mail cover because the judicial refusal to extend fourth amendment protection to information acquired through ordinary mail cover is premised on the mail cover's disclosure of only the means of communication, not the content.[123] Electronic mail cover which intercepted the content of communication would resemble a wiretap's interception of spoken telephone conversation, which is not available without a search warrant.[124]

The possibility of using a wiretap to effect electronic mail cover is further derogated by recent congressional legislation. The Electronic Communications Privacy Act of 1986[125] amended the wiretap law[126] to protect electronically transmitted nonvocal messages in the same manner as telephone conversations are protected. The amendment requires government agents to obtain a search warrant before using a wiretap to intercept the content of an electronic message. This requirement sensibly updates the wiretap law to protect the content of the phone call, whether the content is electronically sent text or spoken conversation.

1. The Pen Register as Prototype

The Electronic Communications Privacy Act prohibits electronic mail surveillance from acquiring any information—even ostensibly "envelope" information—from the electronic transmission itself. The source of envelope information for direct electronic mail must be found elsewhere. The only logistical trail created by directly transmitted electronic mail is the telephone number used by a correspondent to transmit the

123. *See Vreeken*, 718 F.2d at 347-48; *Choate*, 576 F.2d at 177-78; *see also supra* notes 111-117 and accompanying text.

124. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2515-2518 (1968).

125. Pub. L. No. 99-508, 1986 U.S. CODE CONG. & ADMIN. NEWS (pamphlet 10).

126. *See supra* note 124.

message over phone lines. The pen register is thus an appropriate model for an electronic mail cover of terminal-to-terminal correspondence which is not a search. The surveillance provided by a pen register in the context of electronic mail is no different from the pen register used in the context of telephone communications. Consequently, the judicial analysis of the pen register which permits its installation without a search warrant[127] may be extended to allow pen register surveillance of the phone numbers dialed by a computer modem without a search warrant.

2. Suggested Restrictions

A lurking concern with using the pen register as a model for covering direct electronic mail is that data obtained through the pen register and conventional mail cover are conceptually opposite. By disclosing information from envelopes addressed to a suspect, manual mail cover provides government agents with information as to a suspect's *incoming* correspondence. Manual mail cover surveillance thus identifies the senders of communication to a suspect. In contrast, a pen register records the phone numbers dialed from a suspect's telephone and provides government agents with information as to a suspect's *outgoing* phone calls. Pen register surveillance thus identifies the intended *recipients* of communication from a suspect. This concern should not prove constitutionally problematic, to this electronic mail cover, though, since Fourth amendment principles applicable to pen registers have been extended to diode devices which trace the origin of incoming phone calls.[128] Since it reveals phone numbers of those who call the suspect's telephone, the diode device is analogous to mail cover in that both procedures acquire data from communication directed to a suspect. The diode device does not collect any substantive information, and may be installed by law enforcement agents without a search warrant.[129] Additionally, the dialed number recorder, which records information from both incoming and outgoing telephone communications,[130] does not intercept a communication and therefore is not subjected to the search warrant requirement.[131] These holdings indicate that surveillance of communication may acquire logistical information from both parties involved; the direction of communication is not of constitutional import.

Three devices—pen register, diode, and dialed number recorder—are able to elicit logistical information that comprises the relevant "envelope" data for terminal-to-terminal electronic mail. Consequently, this electronic mail cover procedure may take three forms: (1) surveillance of

127. Smith v. Maryland, 442 U.S. at 741-42.
128. J. CARR, *supra* note 49, at § 3.2(c)(2)(C).
129. Michigan Bell Tel. Co. v. United States, 565 F.2d 385, 388 (6th Cir. 1977).
130. J. CARR, *supra* note 49, at § 3.2(c)(2)(C).
131. State v. Miller, 449 A.2d 1065, 1067 (Del. Super. Ct. 1982).

outgoing phone numbers dialed by a computer modem via the pen register; (2) surveillance of *incoming* calls received by a modem via the diode; and (3) two-way surveillance of a modem's activity via the dialed number recorder. A reasonable approach is to draft a procedure which permits electronic mail cover by means of any one of the three devices, while requiring the requesting agent to specify which form of surveillance is most appropriate for the law enforcement objective at hand.

Additional restrictions on an electronic mail cover which is patterned after the pen register should reflect restraints imposed by the pen register procedure. The specifications which limit the duration of pen register surveillance and require law enforcement agents to provide reasonable cause for the pen register serve to safeguard the procedure's constitutionality. Pen register surveillance over an unlimited length of time might be sufficiently intrusive so as to garner fourth amendment protection.[132] A procedure for surveillance of electronic mail by means of a pen register should include similar provisions limiting duration and availability so that it does not invade fourth amendment interests.[133]

3. *Phone Company Compliance*

Successful surveillance by means of a pen register requires cooperation from the telephone company which provides the suspect's phone service. The extent to which a phone company may be forced to cooperate in pen register surveillance has been litigated and resolved in the government's favor: the phone company must comply because "[t]he assistance of the phone company . . . [is] essential to the fulfillment of the purpose for which the pen register . . . [is] ordered. Without the company's assistance, pen registers cannot be effectively employed."[134] A court may also require a phone company to provide its toll records when the law enforcement agent needs to examine a record of long distance calls previously made by the suspect.[135] Although an unwilling phone company may be forced to comply, it is not forced to pay: where the company is compelled to assist with the installation of a pen register, it stands to be reimbursed for the expenses incurred.[136]

C. A Proposal for Covering Indirectly Transmitted Electronic Mail

In contrast with transmitting electronic mail directly over phone lines to another computer, routing a message through an electronic mail

132. *See supra* notes 54-61 and accompanying text.

133. The procedural restrictions placed on the pen register are discussed *supra* notes 59-61 and accompanying text.

134. *New York Telephone*, 434 U.S. at 175-76.

135. *See* Reporters' Comm. for Freedom of the Press v. American Tel. & Tel. Co., 593 F.2d 1030 (D.C. Cir. 1978), *cert. denied*, 440 U.S. 949 (1979); *see also* J. CARR, *supra* note 49, at § 3.3(a).

136. *See, e.g.*, Michigan Bell Tel. Co. v. United States, 565 F.2d at 389.

agency in a sense cleanses the trail left by the communication because the message is sent to the recipient indirectly. No direct logistical link betrays the communication because a correspondent who subscribes to a mail agency does not dial the recipient's phone number, and the sender's modem does not access the recipient's phone line. Applying a pen register to monitor indirectly transmitted electronic mail would not reveal the phone numbers of intended recipients, but rather the phone number of a mail service's host computer. Despite its utility in covering directly transmitted electronic mail, the pen register fails as a model for covering mail sent through an electronic mail service because phone numbers between senders and mail companies, or between mail companies and recipients, contain little useful information.

1. Covering Electronic Mail Sent by Agency: Access to Commercial Records

The source of information which sustains manual mail cover surveillance is the display provided by a letter's envelope. Comparable to that display is the data examined by surveillance of direct electronic mail by means of pen register recordation of the phone numbers dialed among communicating computers. But a surveillance of indirect electronic mail, sent through an agency, requires a different source of envelope information. The presence of a third party—an electronic mail agency—will provide the source needed for covering indirect electronic mail. The appropriate form of this surveillance is access to the information from a company's commercial records of transactions with its customers. The propriety of permitting governmental access to commercial records without search warrants has been debated in a variety of contexts: the consensus is that law enforcement agents are not required to obtain search warrants prior to obtaining information from commercial records.[137] These holdings emphasize that business records are not sufficiently private or personal in nature to be protected by the Fourth Amendment. The commercial information compiled by electronic mail agencies is sufficiently similar to the information sought in these cases to permit law

137. *See, e.g.*, Whalen v. Roe, 429 U.S. 589 (1977) (the public interest in regulating dangerous drugs outweighs any individual privacy interest in reporting all prescriptions to the state since no personal, private business, or political confidences are involved; these reports may be obtained by law enforcement agents without a search warrant); Fisher v. United States, 425 U.S. 391, 401, 414 (1976) (tax documents are not "private papers" and may be examined by law enforcement agents without search warrants); California Bankers Ass'n v. Shultz, 416 U.S. 21, 35, 52-53 (1974) (individual bank depositors have no fourth amendment interest in bank records and copies of their bank accounts—such records and copies may be examined by law enforcement agents without search warrants); Brown v. Johnston, 328 N.W.2d 510, 512-13 (Iowa), *cert. denied*, 463 U.S. 1208 (1983) (public libraries must make their circulation records available to law enforcement agents without search warrants).

enforcement agents access to electronic mail records without a search warrant.

2. Suggested Restrictions

If electronic mail cover of indirectly transmitted mail is to be effected by governmental access to a mail company's commercial records, it will be important to define the permissible extent of that access. A mail company may record much more than "envelope" information. Reliability is crucial to a mail service that receives and transmits electronic data. Meticulous and detailed record-keeping by the company indicates reliability to customers, provides evidence in case of dispute with a customer, facilitates accuracy in billing customers, and establishes a general database of information for use by the company. Furthermore, because of the vulnerability of electronic data to loss or damage within the computer, an electronic mail company might adopt a policy of duplicating and storing all correspondence that it handles. To permit police unlimited access to a mail company's records on a suspected customer might impermissibly broaden the scope of surveillance. To protect the integrity of this electronic mail cover as a nonsubstantive surveillance, its procedure should explicitly limit governmental access to proper logistical information—time and date, length, and destination of transmission—and explicitly forbid examination of additional commercial or substantive data. In addition, this electronic mail cover should be procedurally limited in duration, reflecting limits placed on manual mail cover surveillance.[138] A procedure which permits sufficiently restricted access to information from a mail company's commercial files will provide a workable and constitutional mail cover for indirectly transmitted electronic mail, and will be available to law enforcement agents without a search warrant.

3. Electronic Mail Company Compliance

Conventional mail cover gathers data from a public agency: the United States Postal Service. In contrast, all electronic mail services currently in operation are private. The Federal Postal Service withdrew from electronic mail enterprise after a failed attempt to enter the electronic mail market.[139] Successful mail cover of correspondence sent via private electronic mail agencies will require assistance and cooperation from the companies in supplying the necessary information from their

138. The procedural restrictions placed on manual mail cover are discussed *supra* notes 45-48 and accompanying text.

139. The United States Postal Service briefly dabbled in electronic mail by developing a system called "E-COM," but it dropped that project in 1984. *See Computer Mail Effort Abandoned,* N.Y. Times, June 6, 1984, at D15, col. 1; *see also* I. MAYER, *supra* note 3, at 65. The problems confronting the Postal Service in undertaking an electronic mail delivery system are discussed in L. TRUDELL, *supra* note 2, at 136-37.

records. Assistance and cooperation may not be forthcoming, however, from a private company likely to resent the intrusion, inconvenience, and cost of such surveillance. The extent to which a private company may be forced to assist government agents in mail surveillance is thus critical to this form of electronic mail cover.

This issue will be resolved in the government's favor: court ordered compliance is a common technique used to counter a private company's reluctance to cooperate with a governmental surveillance.[140] The status of the third party as a private, rather than public, entity does not affect judicial authority to compel compliance with law enforcement agents in the fair administration of justice.[141] A variety of private companies—pharmacies,[142] banks,[143] and libraries[144]—have been judicially ordered to aid law enforcement surveillance. These cases provide abundant precedent for compelling an electronic mail service to assist government agents by supplying the pertinent information for covering indirectly transmitted electronic mail.

---

140. " '[T]he citizenry may be called upon to enforce the justice of the state . . . with whatever implements and facilities are convenient and at hand.' " *New York Telephone*, 434 U.S. at 175-76 n.24 (quoting Babington v. Yellow Taxi Corp., 250 N.Y. 14, 17, 164 N.E. 726, 727 (1928)).

141. "The conviction that private citizens have a duty to provide assistance to law enforcement officials when it is required is by no means foreign to our traditions." *Id.*

142. Whalen v. Roe, 429 U.S. 589 (1977).

143. California Bankers Ass'n v. Shultz, 416 U.S. 21 (1974).

144. Brown v. Johnston, 328 N.W.2d 510 (Iowa), *cert. denied*, 463 U.S. 1208 (1983). The surveillance of library patrons' reading habits poses concerns similar to those of governmental surveillance of electronic mail. Most major metropolitan libraries have converted their circulation records from cumbersome manual card check-out procedures to on-line recordation of circulation. Computerized circulation records facilitate the investigation of library records and invite the gaze of researchers, who may want to derive statistics on reading habits, as well as law enforcement agents, who may want to examine a suspect's reading choices. Prior to the computerization of library circulation records, such investigations were impractical; now computerized records provide potentially fertile databases for administering these investigations. Whether such investigations are searches requiring a warrant is an issue which remains largely unaddressed.

The Iowa Supreme Court in *Brown v. Johnston* found that fourth amendment protections do not extend to library circulation records, and held that the protection of circulation records from governmental surveillance is outweighed by the state interest in the fair administration of criminal justice. *Id.* at 512-13. The court acknowledged the potential chilling effect of unhampered or indiscriminate government searches of circulation records, writing that "[t]he effect of forced disclosure of library records would be to chill citizens' reading of . . . books because others might learn of it . . . and any such inquiry would invade their fourth amendment zone of privacy." *Id.* at 512. *See* Comment, Brown v. Johnston: *The Unexamined Issue of Privacy in Public Library Circulation Records in Iowa*, 69 IOWA L. REV. 535, 539 (1984).

VI. Future Electronic Mail Cover: A Cause for Reevaluating the Search vs. Surveillance Paradigm

Courts have consistently exempted mail cover and pen register surveillance from the search warrant requirement because the techniques reveal no content of communication.[145] The holdings indicate that surveillance of electronic mail which reveals only the means of its communication would not evoke judicial imposition of the warrant requirement. Appropriately restrictive regulation of electronic mail cover, therefore, will place electronic mail cover in the array of other methods used to monitor the means of communication—manual mail cover, pen register, and similar procedures—which dwell safely outside the perimeter of the Fourth Amendment. But an increasing reliance on electronic communications will entail a reconsideration of the principles which currently delimit fourth amendment protection.

A. The Problem with *Katz*'s Subjective Requirement

The *Katz* formula—that an individual must subjectively and reasonably expect privacy as to information about her before the Fourth Amendment will require police to obtain a search warrant prior to collecting that information[146]—remains fundamental to courts in determining whether a governmental procedure is sufficiently intrusive to comprise a search.[147] But requiring an individual *consciously* to desire privacy with regard to an interest before that interest begets constitutional protection fails to serve fourth amendment purposes in an era of electronic surveillance.

The heart of electronic surveillance is covertness. Justice Brennan has noted that "the usefulness of electronic surveillance depends on lack of notice to the suspect."[148] Electronic acquisition of data is particularly insidious when its subject has *voluntarily* disclosed desired information. But disclosure would likely be less voluntary if the discloser were apprised of the usefulness of volunteered information as a surveillance device for law enforcement agents. The impropriety of relying on individual subjective expectations to ascertain fourth amendment protection is exemplified by electronic mail surveillance. Many electronic mail users may remain unaware of the vulnerability of the records of their communications to investigative agents. Posting a letter conventionally, a correspondent is likely to understand the logistics of transportation, and to

145. Smith v. Maryland, 442 U.S. 735 (1979) (pen register); United States v. New York Telephone Co., 434 U.S. 159 (1977) (pen register); Vreeken v. Davis, 718 F.2d 343 (10th Cir. 1983) (mail cover); United States v. Choate, 576 F.2d 165 (9th Cir.), *cert. denied*, 439 U.S. 953 (1978) (mail cover).

146. 389 U.S. at 361 (Harlan, J., concurring).

147. *See supra* note 91 and accompanying text.

148. Lopez v. United States, 373 U.S. 427, 463 (1963) (Brennan, J., dissenting).

realize that postal workers will handle the mail between mailboxes. In contrast, electronic delivery and its technological machinations are much less comprehensible to the average electronic mail user.[149] Additionally, agencies may store copies of electronic messages to protect against liability for loss or damage to messages, and the electronic correspondent may not know when electronic duplicates of letters are retained by the company. Company policies and practices which are unknown to subscribers, coupled with the technical complexity of electronic transmissions, suggest that it is inappropriate to require an electronic mail user consciously to construct an explicit expectation of privacy with regard to electronic correspondence.

B. Electronic Surveillance: Logistical Information Takes on Substantive Proportions

Electronic enhancement of techniques which monitor the means of communication portends a disturbing expansion in the power of ostensibly "nonsubstantive" surveillances. Courts have emphasized that electronic recording is entirely different from manual recording. In *Lopez v. United States*,[150] Justice Brennan indicated the problems inimical to electronic surveillance:

> [T]here is a qualitative difference between electronic surveillance . . . and conventional police stratagems such as eavesdropping and disguise. The latter do not so seriously intrude upon the right of privacy. . . . But as soon as electronic surveillance comes into play, the risk changes crucially. There is no security from that kind of eavesdropping, no way of mitigating the risk, and so not even a residuum of true privacy.[151]

The opposing view contends that technological improvement alone cannot affect the fourth amendment analysis of a surveillance technique. Technology has upgraded various manual surveillance techniques without changing the type of data acquired. For example, the use of an electronic tracking device, known as a beeper, facilitates the tracking of a suspect's movements. In theory, the same record could be compiled by physically following the suspect. An electronic surveillance which only improves the ability to accumulate data that could be compiled manually does not affect fourth amendment analyses. This reasoning appealed to the Supreme Court in *United States v. Knotts*,[152] in which the use of a beeper by police without a warrant was upheld. The Court held that "scientific enhancement of this sort raises no constitutional issues which

149. For a discussion of the general lack of knowledge of how the systems work, see I. MAYER, *supra* note 3, at 11.

150. 373 U.S. 427 (1963).

151. *Id.* at 465-66 (Brennan, J., dissenting).

152. 460 U.S. 276 (1983).

visual surveillance would not also raise."[153] The Ninth Circuit Court of Appeals followed this rationale in *United States v. Brock*,[154] holding that since a beeper was a "mere sense enhancement technique," its use did not transform the physical tracking of a suspect into a search.[155] Technological upgrading renders surveillance techniques more efficient,[156] but no constitutional violation necessarily occurs from an increase in the *efficiency* of otherwise constitutional surveillance procedures.

These analyses are persuasive, but fail to recognize that the onus of electronic surveillance lies in an increased *capacity* for governmental acquisition of information, not simply a greater efficiency in doing so.[157] As technological sophistication grows, Justice Brennan's concern in *Lopez*—that electronic enhancement may sufficiently transform a manual technique so as to require new constitutional analysis[158]—becomes increasingly persuasive. The Ninth Circuit's *Brock* opinion qualifies its own holding, conceding that "[a]t some point, the amount and specificity of the information revealed and the duration of the monitoring would require the use of the particular sense enhancement device to be characterized as a search."[159] Moreover, Justice Stevens, concurring with the majority in *Knotts*, emphasized that although it may be possible to use sense enhancing techniques without invoking the Fourth Amendment, "it by no means follows that the use of electronic detection techniques does not implicate especially sensitive concerns."[160]

Blanket constitutional endorsement of "mere sense enhancement" of surveillance techniques disregards the ramifications of an enormous increase in the amount of information made possible by such sense enhancement. The ramifications are depicted vividly by Justice Douglas in *California Bankers Association v. Shultz*.[161] Justice Douglas criticized the analysis which allows electronic devices to escalate the government's surveillance capacity without simultaneously increasing the restraints placed on those techniques.[162] Focusing solely on information contained on one's checks, he portrayed the potential for misusing conglomerations of data:

> In a sense a person is defined by the checks he writes. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational

153. *Id.* at 285.

154. 667 F.2d 1311 (9th Cir. 1982).

155. *Id.* at 1322.

156. Landever, *supra* note 40, at 602-03.

157. The increased capacity is reflected by the explosion in the amount of information obtainable by means of skillful access to computer networks. *Id.* at 598-99.

158. 373 U.S. at 449-50 (Brennan, J., dissenting).

159. 667 F.2d at 1322.

160. 460 U.S. at 288 (Stevens, J., concurring).

161. 416 U.S. 21 (1974).

162. *Id.* at 85 (Douglas, J., dissenting).

> interests, the papers and magazines he reads, and so on *ad infinitum*. . . . Now that we have the data banks, these other items will enrich that storehouse and make it possible for a bureaucrat—by pushing one button—to get in an instant the names of the 190 million Americans who are subversives or potential and likely candidates.[163]

C. Electronic Mail Cover: Where Does the Search Begin?

The courts have acknowledged that at some point an enormous amount of seemingly trivial, voluntarily relinquished information, accumulated by means of electronic recording, sufficiently resembles a search so as to be restricted by the warrant requirement.[164] The controversy generated by electronic mail cover is not that it is faster or easier than manual mail cover, but that it is more powerful: the breadth of information available increases significantly as more communications are transmitted electronically.[165] Technology renders surveillance more efficient by improving the mechanics of the techniques. Operating in tandem with increased efficiency, however, is an increase in power brought to such techniques by electronics. The technological trend toward centralization of commercial and private transactions[166] completed from a home or business computer portends an electronic mail cover which potentially will reveal political affiliations,[167] mail order purchases,[168] tax and bill payments,[169] memoranda, travel plans, job application re-

163. *Id.*

164. Justice Douglas has opined that all forms of wiretapping, bugging, and electronic surveillance sufficiently resemble searches so as to offend the Fourth Amendment. Gelbard v. United States, 408 U.S. 41, 62 (1972) (Douglas, J., concurring).

165. For effectively dour depictions of the use and abuse of electronically stored data, see J. WICKLEIN, ELECTRONIC NIGHTMARE 11-12, 195-98 (1981). One potential misuse of an increase in power is the governmental cross referencing of electronically stored data. Also called computer matching, this process accesses various discrete information banks to accomplish such tasks as profiling specific persons, ferreting out tax fraud, and discerning the misuse of government funds. For a discussion of the pending threat posed by this commingling of information, see Kirchener, *Privacy: A History of Computer Matching in the Federal Government,* COMPUTER WORLD, June 23, 1981, at 1, col. 1.

166. The "intelligent telephone" symbolizes the impending centralization of banking, shopping, and information services. The Greater New York Savings Bank offers one such service: a subscriber may complete credit card and banking transactions, and obtain stock quotations and voice libraries of recorded information, by pushing the appropriate buttons on her telephone. Baer, *Telecommunications Technology in the 1980's,* in COMMUNICATIONS FOR TOMORROW, *supra* note 23, at 84-85. For further discussion of centralized information services, see Landever, *supra* note 40, at 605-07.

167. The potential to transmit electronically requests for political information, to communicate electronically with political representatives, and to receive political literature via electronic mail is depicted in J. DEKEN, *supra* note 27, at 324-25.

168. Deken also discusses electronic purchasing. *See id.* at 322-23.

169. Transmitting tax information electronically is discussed in Gerofsky, *supra* note 3, at 309-10 n.31.

quests,[170] and membership records.[171] The ability to cross-tabulate and analyze electronically stored information could reveal an alarmingly accurate profile of an individual.[172]

Emphasizing that interpretation of fourth amendment protections must be a dynamic process, the *Brock* court wrote that "[a]daptation of Fourth Amendment values and jurisprudence to the electronic age into which we are rapidly moving presents a challenge with which this nation will be concerned for some time to come."[173] This challenge is posed by electronic mail cover: when electronic surveillance techniques, which are unrestricted by the warrant requirement, begin to acquire dispositive, revealing bodies of facts, recategorizing the techniques as searches will be essential. Although proper restrictive codification may enable electronic mail cover to exist unfettered by fourth amendment restrictions, a judicial awareness for the abuse of an electronic mail cover must check its development. The emphatic distinction between substance and logistics of communication becomes less meaningful as methods for gathering and analyzing nonsubstantive information grow in sophistication. As electronic mail becomes increasingly integrated into American society,[174] judicial willingness to reevaluate the paradigm which may currently exempt electronic mail cover from the Fourth Amendment would curb the emergence of an ever-present governmental gaze.

Conclusion

A proposal for developing electronic mail cover which surveys electronic communication requires resolution of several constitutional issues. Procedurally, care must be taken to ensure the electronic mail cover reveals only nonsubstantive, envelope-like data. This may be accomplished by modeling electronic mail cover after existing and comparable surveillance procedures. As electronic mail becomes an increasingly prevalent means of communication, the ability of electronic mail cover to collect and convey large, cohesive amounts of "nonsubstantive" data

170. *Id.*

171. These and other data are obtainable pursuant to the manual mail cover. *See Choate*, 576 F.2d at 201 (Hufstedler, J., dissenting). The emergence of electronic mail suggests that these data will be obtainable through electronic mail cover.

172. See, e.g., *What Your Wallet Reveals About You*, San Francisco Chron., Oct. 7, 1984, at A16, col. 1, for an exposition of the mounds of personal data retrievable by applying cursory information—*i.e.*, voter registration and driver's license number—to access more privileged information stored in computer databases.

173. 667 F.2d at 1318.

174. Electronic mail grew successfully from 1980 through 1985, with the number of messages transmitted doubling every year. It is predicted that by the end of the decade, the number of electronic messages transmitted annually will have reached 10 billion. That number will exceed 40 billion by 1995, according to forecasts compiled by the Office of Technology Assessment. *See* LAWYERS ON LINE, *supra* note 6, at 138; *see also* Gerofsky, *supra* note 3, at 305.

will inevitably emerge. Reevaluation of the constitutional categorization of electronic mail cover will then be crucial. The reams of electronic communications networks which span the country leave information-laden trails and bestow a tempting tool to be used by investigative and law enforcement agencies. The power of this device is enormous, and if improperly plied, ominous.

In a society whose interstices are increasingly transparent, it is essential to protect electronically stored data more stringently than tangible records. One evocative comparison emphasizes this: "Orwell's thesis was surveillance, which was used to impose Big Brother's will on people. At the time, Orwell could only see the use of microphones and television; the surveillance in *1984* was done clumsily. But now surveillance is done simply by monitoring the flow of information."[175] The "microphones and television" of *1984* have matured into the adroit and surreptitious techniques of 1987. Interpretation of the Fourth Amendment must parallel this metamorphosis to ensure that such techniques are not cloaked in legitimacy by an absence of Orwellian "clumsiness."

*By C. Leigh Haynes**

175. *Fear of Filing: A Computer-Age Dilemma,* Chicago Reader, July 22, 1983, at 4, col. 2 (interview with George Trubow).

* B.A., Northwestern University, 1982; Member, third year class.