UIC John Marshall Journal of Information Technology & Privacy Law

Volume 18
Issue 4 *Journal of Computer & Information Law - Summer 2000*

Article 7

Summer 2000

Privacy on Federal Civilian Computer Networks: A Fourth Amendment Analysis of the Federal Intrusion Detection Network, 18 J. Marshall J. Computer & Info. L. 1049 (2000)

David Hueneman

PRIVACY ON FEDERAL CIVILIAN COMPUTER NETWORKS: A FOURTH AMENDMENT ANALYSIS OF THE FEDERAL INTRUSION DETECTION NETWORK

I. INTRODUCTION

Cyber-terrorism[1] has become an issue of greater concern for both the Clinton Administration and private industry.[2] The massive wave of cyber-attacks[3] on large Internet corporations during the second week of

1. *See* Clifford A. Wilke, *Infrastructure Threats from Cyber-Terrorists* (visited Feb. 12, 2000) <http://www.occ.treas.gov/ftp/bulletin/99-9.txt>. The definition of cyberterrorism is very broad including "the use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." *Id.* "These can be operations to disrupt, deny, corrupt, or destroy information resident in computers or available via computer networks." *Id.*

2. *See* Neil King Jr., Glenn R. Simpson, and Ann Grimes, *ZDNet: Clinton Calls forInternet-Security Summit* (visited Feb. 13, 2000) <http://www.zdnet.com/filters/printerfriendly /0,6061,2436551-2,00.html>. At a meeting between the National Security Council and top Internet executives, Jeffrey Hunker, White House director for critical infrastructure protection, stated, "We're not calling this a national-security issue per se, but on the other hand, we're not saying, 'Oh, well, it's just the private sector,' this is something that has affected the economy. . .and that alone makes it very important." *Id.*

3. *See* Wilke, *supra* note 1. Cyber-terrorist attacks can take many forms. *Id.* They include disruption of telecommunications services or computer, satellite, or cable services, including intrusive methods of monitoring such services. *Id.* Cyber-terrorists can release information that had been stored "within or communicated through computer, cable, and satellite or telecommunications systems." *Id.* Cyber-terrorists can also modify "computer programming codes, computer network databases, stored information, or computer capabilities." *Id.* Furthermore, they can manipulate "computer, cable, satellite, or telecommunications services resulting in fraud, financial loss or other federal criminal violation." *Id.* Finally, they can use their computer knowledge to extort government agencies or companies to destroy data or program files. *Id. See also* Bob Sullivan, *Misconfigured Routers Blamed for Sate of Internet Attacks* (visited Feb. 13, 2000) <http://www.msnbc.com/news/368039.asp>. Internet attacks were denial-of- service attacks, which are "attacks in which a hacker floods a network server with data with the goal of causing the system to crash." *Id.*. *See also* Mel Duvall, *ZDNet: Web Attacks Spur Hack Insurance* (visited Feb. 13, 2000) <http://www.zdnet.com /zdnn/stories/news/0,4586,2436984,00.html>. In the wake of the February 2000 attacks by hacker, Insurers against Internet hackers have had an increase in demand for their service. *Id.*

February 2000[4] called into question the need for government regulation[5] or monitoring[6] of its own networks. The inherent problem with monitoring the networks is that it may be interpreted as an erosion of privacy rights. There is no doubt that privacy is an important concern for users because every day, more and more people are spending more time on the Internet for a wide variety of functions.[7] However, a network user's right to privacy must be weighed against the government's interests and those of private corporations.[8] The fight against cyber-terrorists is similar to fighting a guerrilla war. Rather, this problem will require eternal vigilance,[9] meaning the government may have to utilize Fourth Amendment exceptions to protect cyberspace from the certain attacks made against government computer networks.

Imagine if one morning you woke up and heard a newscast announcing[10] that the non-public computer network systems for the Department of the Labor,[11] the Department of Justice, and the Department of Energy were all attacked. Experts believe that it may be weeks before they can regain control. The Department of Labor has lost 25% of its data, leav-

---

4. *See* Laurent Belsie, *Wake-up Week for Web Security Hacker Attacks on Several Major Sites Reveal Difficulty of Safeguarding the Internet from Increasing Threats,* Christian Science Monitor, Friday, Feb. 11, 2000, at CHSM 1. The attacks were based against Yahoo!, eBay, Amazon.com, Buy.com, ZDNet, eTrade. *Id.*; *See also* Connie Guglielmo, *Web Attacks by the ABCs* (visited Feb. 13, 2000) <http://www.zdnet.com/zdnn/stories/comment / 0,5859,2435990,00.html>. The author here suggests that there may have been a serial cyber-terrorist, who made it nearly through the alphabet when he was implementing his denial of service attacks on the Internet top sites. *Id.*

5. *See* Chris Cobbs, *Does Uncle Sam Want to be Your Big Brother? Computers, User Privacy and the Law Technology is Far Outpacing Efforts to Protect Users' Rights,* ORLANDO SENTINEL, Nov. 21, 1999, at G1.

6. *See* discussion *infra* note 19, of the President's plan to monitor federal civilian networks under FIDNet.

7. *See* Annette Hamilton, *ZDNet: News: Rush Home to Surf? Join the Crowd* (visited Feb. 13, 2000) <http://www.zdnet.com/zdnn/stories/news/0,4586,2435087,00.html>. Research has suggested that nearly 25% of the 110 "online" Americans come home from work and spend all all evening online. *Id.*

8. *See* discussion *infra* note 19, of private industry's right as a member of the critical infrastructure to pay the burden of securing their respective portion of the nation's economy.

9. *See* Jim Rapoza, *ZDNet: News: Web Attacks Give New Meaning to 'Eternal Vigilance'* (visited Feb. 13, 2000) <http://www.zdnet.com/pcweek/stories/columns / 0,4351,2435465,00.html> (*quoting* Thomas Jefferson).

10. Although the following is purely hypothetical, in light of the February 2000 attacks certainly this scenario could be possible.

11. *See* Brock Meeks, Alan Boyle and Bob Sullivan, *ZDNet: News: Hack Attack Knocks out FBI site* (visited Feb. 13, 2000) <http://www.zdnet.com/zdnn/stories/news/ 0,4586,2266648,00.html>. The FBI Internet site was taken down in retaliation for serving search warrants on Global Hell (gH) a well-known hacker group. *Id.*

ing the costs well into the millions.[12] The government has attempted to find out who crashed the systems but as yet has had no success. One Internet rumor claims that the attack was brought about by Arab fundamentalists from Afghanistan.[13] However, there have also been reports that this attack was brought about by small groups and their simultaneous occurrence is merely coincidence. If the government had been able to monitor traffic to the federal agency's non-public networks to respond cross department reaction more quickly, the outcome might have been different.

The President's National Plan for Information System Protection[14] is designed to protect America's infrastructure from just this type of cyber-attack.[15] The plan calls for the creation of the Federal Intrusion Detection Network (FIDNet),[16] which will be responsible for monitoring the federal departments and agencies.[17] While FIDNet is being designed to monitor the entry of Federal non-public computers for intrusion, it is not yet being considered for private computer networks or Internet sites.[18] The privacy problem with FIDNet arises when private users access federal civilian non-public networks and are subject to monitoring.

The President's Plan calls for cooperation between the federal government and private industry.[19] As of August 2000, the Plan was in the early stages with respect to the private industries the government has

12. *See* Jennifer Mack, *ZDNet: Attack Victims Count their Losses* (visited Feb. 13, 2000) <http://www.zdnet.com/zdnn/stories/news/0,4586,2436501,00.html>. The companies attacked on the second week of February 2000 have stated that the losses are relatively insignificant. *Id.*

13. *See* John Arquilla, David Ronfeldt, and Michele Zanini, *Networks, Netwar, and Information-Age Terrorism* (visited Feb. 13, 2000) <http://www.rand.org/publications/MR/MR989/MR989.pdf/MR989.chap3.pdf>.

14. *See* Version 1.0 [hereinafter President's Plan].

15. *See* Defending America's Cyberspace: National Plan for Information Systems Protection, i (Pub. Papers Jan. 7, 2000) [hereinafter Defending America's Cyberspace].

16. *See id.* at xix. "These intrusion detection systems are already in use in the Executive Branch and Congress." *Id.*

17. *See id.* at xix.

18. *See* Christopher J. Dorobek, *FIDnet Will Monitor Federal, not Private, Nets, Administration says,* Government Computer News, October 25, 1999, at 9. Originally the FIDNet plan was to include private computers in the monitoring system. *Id.* This included corporate computers that were part of the critical infrastructure. *Id.*

19. *See* Defending America's Cyberspace, *supra* note 15, at iii. The President would like the government to form a close relationship with the representatives of private industry as well as those of public services that are involved in the critical infrastructure of the country. *Id.* The President's Plan does not want to have to achieve the goals through regulation. *Id.* Rather, the President sees possible regulation as an impediment to the achievement of protecting American's Cyberspace. *Id.* The President's Plan also does not want to micromanage the critical infrastructure. *Id.* Rather, the individual sectors of the critical infrastructure will determine for itself "what practices, procedures, and standards are necessary for it to protect its key systems." *Id.*

identified as part of the economy's critical infrastructure.[20] The President's Plan initially arose out of President Clinton's Presidential Decision Directive 63 (PDD 63).[21] Directive 63 was signed in 1998 and required the assessment of America's cyber-defenses.[22] The President's Plan is a by-product of PDD 63.[23] Although the Plan is currently voluntary for private industry, what would happen if cyber-attacks became an everyday occurrence? The federal government might take a heavy hand to watch over its commercial Internet "little brother." In fact, the President's Plan has already been criticized for giving the FBI too much responsibility and for failing to give control over to the agencies with the most experience in this area.[24]

This comment will explore the relationship between the privacy of the users of the federal non-public civilian computer networks and the government's power to monitor such networks. The background will explain what a network is, how cyber-terrorists can greatly damage a system, what the government is planning to do about the problem, and the constitutional protections involved. The analysis will examine the Fourth Amendment and the Electronic Communications Privacy Act and consider their respective effects on the implementation of FIDNet, while determining if any exceptions would allow the FIDNet plan to go forward in the face of Fourth Amendment rights.

---

20. *See Computer Security: Clinton Announces Plan, Seeks Funds to Combat Threats to Computer Security*, BNA Washington Insider, Jan. 10, 2000.

21. *See* Computer Technology Security: Hearing before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism & Government Information, 106th Cong. (2000) (statement of Robert F. Bennett).

22. *See id.* "PDD 63 required the Executive Branch to assess the vulnerabilities of computer-based systems and to remedy deficiencies in order to become a model of information security. PDD 63 called for the development of a detailed federal plan to protect U.S. critical infrastructures and to defend America against information warfare." *Id.*

23. *See id.* "As the Plan notes, it is in fact an invitation to a dialogue – an important first step." *Id.*

24. *See id.* Bennett states that there are two main things wrong with the plan: First, the architecture is flawed in its structure:The FBI is given the coordination function, which immediately raises DoD and industry suspicions as well as turf battles. The plan focuses on the hacker threat, not the broader threat of information warfare. The plan fails to articulate a strategy for reconstitution and recovery if an attack occurs. DOD and NSA have the most experience, but their roles are uncertain.Second, the Administration's organization makes it difficult to follow the money. Approximately nine committees have some CIP oversight responsibility over $2.04 billion spread across 15 agencies. Of the $2.04 billion in the 2001 budget that is tagged for CIP, $276 million would be new funding. *Id.*

II. BACKGROUND

A. COMPUTER NETWORKS

Computer networks[25] are designed to enable computers and users to communicate with each other and share information.[26] While there are many benefits in using a network as opposed to stand-alone computers,[27] the greatest advantage is that it allows resources, data, and applications to be shared.[28] Networks allow computers to reach their full capability.[29]

There are two types of networks: a peer-to-peer network and a client-server network.[30] In a peer-to-peer network, there is no hierarchy.[31] As the name implies, every workstation has the same "authority" to access data as any other workstation, so every workstation has access to the same resources as any other.[32] The advantages of this type of network are that it provides efficient information sharing among users on the network.[33] However, this type of configuration also has serious security drawbacks.[34] One workstation operator may be able to access information on another workstation that the other operator wants to keep private or secure.[35]

---

25. *See* Lee James McMunn, *This page contains an overview of computer networks* (visited Feb. 13, 2000) <http://www.awstevenson.demon.co.uk/SYSNOTES/comnet.htm>. "Computer data network may be defined as a number of computers and related devices interconnected by one or more transmission paths." *Id.*

26. *See Computer Network* (visited Feb. 13, 2000) <http://chaminade.org/mis/NETWORKS.HTM>. Computer networks have two or more computers that are connected to form a communication system. *Id.* This system can include printers, scanners, or and other peripheral device. *Id.* The communication system "allows users to share information and resources." *Id.* "In contrast, a stand-alone computer stores all data on its own disk drives and is physically connected to each of its peripheral devices." *Id.*

27. *See id.* Consider the following example: "In a school computer lab with thirty stand-alone computers you would need to purchase thirty printers if you wanted each student to print from his/her computer." *Id.* In contrast, if you had thirty *networked* computers (called workstations) each of them could print over the network to a single printer." *Id.*

28. *See id.*

29. *See id.*

30. *See id.*

31. *See id.*

32. *See Computer Network* (visited Feb. 13, 2000) <http://chaminade.org/mis/NETWORKS.HTM>. A good example might be a particular workstations' hard disk or CD-ROM drive. *Id.* Each of these would be a "resource that all the other workstations could access. No single computer manages or controls the peer to peer network; all workstations are equal. Examples of peer to peer network operating systems are *Windows for Workgroups*, *Windows95*, and Artisoft *Lantastic*." *Id.*

33. *See id.*

34. *See id.*

35. *See id.*

Client-server networks are much more secure.[36] Under this type of network, the server is the ultimate authority.[37] Client workstations make requests to the server for data, and the server will only deliver the data if the client is properly authorized to receive that data.[38]

When a person attempts to access[39] a protected network—generally one that contains valuable information that must be safeguarded—a user identification and user password are often required.[40] There are three steps that a user must complete to gain access to the network. The first step is to let the network servers know that the user wants to begin the login process.[41] Once the network is aware that a user is attempting to access it, the network server tries to determine who the user is and whether the user has authority to log in to the network.[42] Finally, once the network server has determined that the user identification is proper, the password is examined to make sure it is valid—that it exactly matches the password assigned to the user by a network manager.[43]

---

36. *See id.*

37. *See id.*

38. *Computer Network* (visited Feb. 13, 2000) <http://chaminade.org/mis/NETWORKS.HTM>. "The client (customer) is the workstation that connects to a server (owner), which in turn provides services." *Id.*

39. *See id.*

40. *See id.* "It is the Network Manager's responsibility to handle these tasks." *Id.* For example, a Network Manager would add a new user to the system and determine to which resources, applications, and data the user can access (called assigning rights)." *Id.*

41. *See id.*

> The first step is to find the location of login, or find the doorway. The server needs to be aware that there is someone wishing to access it. To tell it that you wish to access the network you must use the command LOGIN. When you type the word LOGIN and press ENTER you are telling the computer to begin the process of giving you access to its resources. In some operating systems such as *Windows95* a dialog box appears to help you through this log in process.

Id.

42. *See id.*

> In this second step you must tell the network who is attempting to gain access so a to verify the authenticity of the proposed user. In essence the network will ask you 'Who are you?' Since it cannot orally ask you this, it displays the phrase *Enter your login name* on the bottom of the monitor. Every network user has a unique user name that is also called the login name. The login name is assigned by the Network Manager.

Id.

43. *See Computer Network*, *supra* note 38. The final step is to "verify that you are who you say you are." *Id.* Just think if you knocked on your friend's door might she recognize you simply from the sound of the knock, or would you have to call out that it was you. *Id.* A network cannot recognize who the person attempting access simply by accessing a login page much in the same way your friend could not know who was at the door simply by a knock. *Id.* This is why a network "uses a secret password to confirm who you are" in the same way that your friend may rely on your voice or, perhaps, might look through a peephole just to make sure that you are who you say you are. *Id.* Unique passwords "assigned by the Network Manager and it should be changed frequently." *Id.* When you type in this

This concept works whether the user is physically connected to the server, such as through a computer lab workstation wired into the school's main server, or outside the physical building using a dial-in or remote connection.[44]

Once inside the network, users have access to the information in the server subject to certain conditions. For example, users may have different rights[45] from one another.[46] In a university setting, for example, a student may view certain files, such as her class syllabus but may not change or destroy files in the syllabus folder on the server.[47] These rights are associated with the user's identification and password.[48] Most often, rights are set for specific "areas" on the server, such as a certain set of directory folders.[49]

With the dawn of the Internet, however, unauthorized access problems have become critical. The Internet is simply a gigantic client-server system on a wide-area network (WAN)[50] that gives anyone with a

---

password you will notice that as you type nothing appears on the monitor. This is the way the file server keeps your password secret-it does not display anything on the monitor as you type." *Id.*

44. *See id.*

45. *See id.* By rights it is meant the ability to access certain information that may have been designated restricted according to some classification system. *Id.*

46. *See id.* Many times this depends on your classification within an organization such as a company or school. *Id.*

47. *See id.* "Students might have the right to create files in certain folders, but they may be restricted from deleting files or modifying certain ones. A user might not be able to print on certain networked printers, access a certain network drive, or start a particular application program." *Id.*

48. *See id.*

49. *See Computer Network*, *supra* note 38. They indicate whether the user can access the folders at all, which is sometimes referred to as whether or not the user can "see" the folders. *Id.* If the user can see a certain set of folders, the PC user is given one of two types of access to those folders: "read" or "write" permissions. *Id.* Read access (sometimes called "read-only access") means that the user can view files or documents within the folder, but they cannot edit or delete those files. *Id.* Write access (sometimes called "read-write" access) allows the user not only to view files but to edit and delete the files as well. *See also Webopedia Definition and Links* (visited Mar. 26, 2000) <http://webopedia.internet.com/Data/read_only.html>; *Webopedia Definition and Links* (visited Mar. 26, 2000) <http://webopedia.internet.com/Data/read_write.html>. The significance of these various level of access is that often network administrators believe that they have protected parts of the network from unauthorized access. *See Computer Network*, *supra* note 43. The login process and the various access levels provide protections to the entire network or to specific parts of the network. *Id.*

50. *See What is a WAN?* (visited Mar. 26, 2000) <http://www.dcninc.com/whatawan.htm>. A WAN, on the other hand, includes computers that are outside this type of "hardwired" network. *Id.* For example, if the law office above opened a new branch in another town, they may want to connect the two offices. *Id.* The individual machines on the network are too far apart for the law firm to "hardwire" them, so the local phone company provides some of the connectivity. *Id.* For example, they may set up dial-up connec-

computer and a modem access to certain data residing on Internet servers. However, the problem arises when network administrators[51] mistakenly believe that the "private" portions of their networks are secure. Network administration is extremely complex, and Internet technology is so new that many administrators do not yet appreciate the many ways their networks can be breached. A "firewall" is the layer of protection on a server that keeps unauthorized users out of protected portions of a network.[52]

The Internet was created in the 1960's as a means to connect all of the various networks at research institutions to ease the access of information between research scientists.[53] Similar to single computers, these

---

tions, so a user in one office must use a modem and dial the other office to connect. *Id.* This is the way most home users access the Internet – through dial-up modem connections. *Id.* The office may also choose to use "dedicated' lines, meaning that they lease a permanent connection from the phone company. This is the way most large businesses access other parts of the company and access the Internet through permanent, dedicated connections. A local-area network ("LAN"), on the other hand, is entirely contained within a relatively small physical area, such as a single building. *LAN* (visited Apr. 3, 2000) <http://www.whatis.com/lan.htm>. It may be as small as two or three computers linked together, or as large as an entire corporate office building. *Id.* The workstations making up the network are physically linked with cable that runs from one machine to another and generally includes printers, routers, and other network hardware. *Id.* For example, a small law firm purchases ten PCs, five printers, and a server (which is generally a very powerful PC running special server software). *Id.* They would also purchase the physical cable to connect these machines, and a network operation team of people would physically unroll the cable and connect each of the machines together. *Id.* The cable allowing communication between the PCs and the server are completely controlled by the company and they are physically contained within the office space. *Id.* The only way for someone with another PC to access this type of network is to log onto one of the existing PCs or to physically bring a new PC into the office, run another length of cable, and physically connect the new PC to the network. *Id.*

51. *See* Microsoft Encarta Online Encyclopedia 2000, *System Administrator* (visited Mar. 29, 2000) <http://encarta.msn.com/find/Concise.asp?z=1&pg=2&ti=01C33000>. System Administrator, in computer science, the person responsible for administering use of a multiuser computer system, communications system, or both. *Id.* A system administrator performs such duties as assigning user accounts and passwords, establishing security access levels, and allocating storage space, as well as being responsible for other tasks such as watching for unauthorized access and preventing virus or Trojan horse programs from entering the system. *Id.* A related term, sysop (system operator), generally applies to a person in charge of a bulletin board system, although the distinction is only that a system administrator is associated with large systems owned by businesses and corporations, whereas a sysop usually administers a smaller, often home-based, system. *Id.*

52. *See What is a Firewall?* (visited Mar. 13, 2000) <http://www.digi4fun.com/ConSeal3.html>. A firewall is used to prevent unauthorized persons from gaining entry onto a computer network. *Id.* They also prevent persons from going to particular sites that have been forbidden by a systems operator. *Id.* Persons with computer port scanner, not to be confused with the graphical interface used to make computer files of hard copy images, can gain entry to vulnerable computers. *Id.*

53. *See* CHARLES PLATT, ANARCHY ONLINE NET CRIME 38-39 (1996).

networks were isolated, and had to be connected to each other.[54] All of the networks were connected to the Advanced Research Projects Agency Network ("ARPANet").[55] ARPANet was designed so that there would be no centralized switching center.[56] The design allowed ARPANet to continue operating even after a severe attack from a foreign government.[57] The system worked even if several of the computers in the ARPANet failed to work.[58] The Internet is very similar in design to ARPANet,[59] which provides the Internet the enormous added benefit of an inherent defense due simply to its design.

B. CYBER-ATTACKS

Cyber-terrorists can use a variety of means to attack a network.[60] Unlike traditional forms of terrorism, where capital expenditures went into coordinated physical attacks, information warfare requires very little money and even less exposure. However, like more traditional forms of terrorism, the numbers of persons involved is low, thereby keeping all casualties to a minimum.[61] In fact, all that is really needed to effect a heavy attack are a telephone, computer, hacker software, and a modem.[62] Furthermore, attacks do not have to take the form of actual destruction. Rather, one type of cyber-attack, for example, could be the simple monitoring of telecommunication, cable, computer, or satellite

---

54. *See id.*

55. *See id.; What is ARPANet (a Definition)* (visited Feb. 27, 2000)<http://www.whatis.com/arpanet.htm>.

56. *See* Platt, *supra* note 53, at 38-39. "[E]ach node in the network was smart enough to operate independently, routing messages to other nodes on its own initiative." *Id.* "Electronic mail followed an unpredictable zigzag path, skipping from one site to the next, using any connection that happened to be lightly loaded at that particular moment." *Id.* This type of organization is similar to that of modern terrorist groups. *Id.* In fact, it is they who have begun to realize that the highly centralized hierarchies provide for easy destruction in times of conflict. *See also* Arquilla, Rondfeldt, and Zanini, *supra* note 13.

57. *See* Platt, *supra* note 53, at 38-39.

58. *See id.* "The original system, ARPANet was fault-tolerant." *Id.* This means that virtually nothing could prevent it from sending the information to the next node. *Id.* This type of system would allow it to function even in the most dangerous of situations. *Id.* For example, "[w]hen a node in Chicago went down, messages could just as easily pass through Detroit [because] the system was supposed to be usable in a national emergency." *Id.*

59. *See id.* The Internet is based on the National Science Foundation ("NSFNet"), which in 1987 began to connect private computers together. *Id.*

60. *See* Bob Sullivan, *Misconfigured Routers Blamed for Spate of Internet Attacks,* (visited Feb. 13, 2000) <http://www.msnbc.com/news/368039.asp>. The second week of February cyber-attacks used denial-of-service attacks. *Id.*

61. Here casualties does not refer to the loss of human life in the process of fulfilling a mission. Rather it refers to simply being arrested by some authority for the breaking into of the targeted computers.

62. *See* Wilke, *supra* note 1.

systems.[63] Besides denial-of-service attacks, there are worm attacks, domain-name-service hijackings, logic bombs or Trojan horses, and mail bombings.[64] Worm attacks are used to overload the system by having the program reproduce itself on the server.[65] Domain-name-service hijackings are used to prevent Internet users from gaining access to a particular Internet site by rerouting all inquiries from that site to a completely different location, thereby making the original Internet site unavailable to the requester.[66] Logic bombs are programs that when triggered may disrupt the entire computer system by making the entire disk unreadable.[67] Finally, there are e-mail attacks, or mail bombings. These include bombarding a specific e-mail account with thousands of messages to shut down the recipient's e-mail server or e-mail access. E-mail attacks may also involve Trojan horse programs that are attached to e-mails. When the curious user runs the program, it operates like a logic bomb or Trojan horse and can disrupt the user's PC or the entire network. There are even e-mail Trojan horse programs designed to self-replicate themselves by automatically e-mailing a copy of the attacking message to everyone in the user's e-mail address book.[68]

Law enforcement can stop cyber-terrorists in a variety of ways. One way, not currently supported by the Clinton administration, is to allow for higher levels of encryption.[69] Since the level of encryption determines the level of data security, it is natural to want a higher level of encryption when dealing with increasingly sensitive data. Of course, this also means that cyber-terrorists can communicate more effectively, because government officials would be required to break codes hackers employed to encrypt their information.[70]

---

63. *See id.*

64. *See* Sullivan, *supra* note 60.

65. *See id.*

66. *See id.*

67. *See id.* "These programs could be used to launch broad-based attacks that would be difficult to defend against and impossible to trace back to the hacker." *Id. See also Introduction to Viruses* (visited Sept. 25, 2000) <http://www.stiller.com/vintro.htm>.

68. *See id.*

69. *See* Peter Coffee, *Analysis: Clinton Passed up a Golden IT Opportunity* (visited Feb. 13, 2000) <http://www.zdnet.com/pcweek/stories/news/0,4153,2429104,00.html>. The President stressed the concern for the integrity of critical institutions and our personal safety as he commented on the natural effects of Internet technology. *Id.* Calling for the "protection of medical and financial records, conveniently omitting to mention his own administration's continual attempts to weaken our privacy by imposing impracticable technologies (such as key escrow) and by the unconstitutional broadening of police powers (such as covert hard-disk searches and pre-encryption monitoring of data-entry operations)." *Id.*

70. *See id.* The Clinton Administration has been willing to grant greater access to higher security but only at the price of privacy in the form of key escrows. *Id.*

C. The Electronic Communications Privacy Act and The President's Plan

The Electronic Communications Privacy Act ("ECPA") was enacted in 1986 to update Title III of the Omnibus Crime Control and Safe Streets Act of 1968—the federal wiretap law.[71] The purpose of the act was to modify privacy protections so that such protections might be modernized relative to technological advancements.[72] The Framers of the Constitution did not realize the advances in technology that would occur in the years to come.[73] The telephone is an example of such a technological advancement of which the Framers might never have dreamed. However, as is obvious today, the tapping of a telephone line is one of the easiest ways for the government to acquire information.[74] The ECPA was enacted to address these sorts of new applications that the Framers could not have provided for with the Fourth Amendment

The President's Plan was created as a result of PDD 63, and the government will challenge the private sector to secure America's computer systems by taking the lead and acting as the role model for suc-

71. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126 (1988)). S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555. There are three sections to the ECPA. *Id.* Title I of the ECPA concerns the interception of wire, oral and electronic communications that affects interstate commerce or foreign commerce. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555. Title I implicitly excludes oral communication as being protected by defining the communication that is protected as: "transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or a photooptical system that affects foreign or interstate commerce." *Id.* Title II addresses the access of stored information or transactional records and communications and is "modeled after the Right to Financial Privacy Act, 12 U.S.C. 3401 et seq. to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." *Id.* Title III addresses trap and trace devices as well as pen registers. *Id.* Together they combine to form Congress' answer to the technological advancements that have occurred over the years. *Id.*

72. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555. The purpose of the Act is to "protect against the unauthorized interception of electronic communications." *Id.* The Bill was designed to update the 1968 law and "clarify Federal privacy standards in light of dramatic changes in new computer and telecommunications technologies." *Id.*

73. *See id.* The vision of the Framers of the Constitution was somewhat limited by what the methods of governmental intrusion at the time. *Id.* When they discussed the methods of governmental intrusion, they thought in terms of physical intrusion, intrusions such as those in to the "house, papers, and effects." *Id.* Those things that have traditionally been held as intrusive have been limited by the Fourth Amendment. *Id.* Foresight is limited, and as such accommodations need be made to accompany unforeseen change. *Id.* This is what the ECPA intends to accomplish. *Id.*

74. *See* Katz v. United States, 389 U.S. 347 (1967).

cess.[75] The President's Plan will protect several key infrastructure sectors within the economy.[76] However, the entire plan to protect the critical infrastructure will be voluntary for both private industry and the states and will be mandatory only for federal agency systems.[77] It is uncertain what information the private sector will be requested to submit to the government to participate in this protective partnership. However, as the Plan progresses, expectations of the private sector should be clarified.[78] After the February cyber-attacks, there may be a heightened level of cooperation between the federal government and private industry.

The President's Plan calls for the creation of FIDNet,[79] a system

---

75. *See* Computer Technology Security: Hearing before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism & Government Information, 106th Cong. (Feb. 1, 2000) (statement of John S. Tritak, Director Critical Infrastructure Assurance Office). President Clinton challenged the Federal Government in a way not challenged for some time. *Id.* He specifically wants the Federal Government to be the "model for critical infrastructure protection-to put our own house in order first." *Id.*

76. *See* Defending America's Cyberspace, *supra* note 15, at ii. "This directive requires that the Executive Branch assess the cyber vulnerabilities of the Nation's critical infrastructures–information and communications, energy, banking and finance, transportation, water supply, emergency services, and public health, as well as those authorities responsible for the continuity of federal, state, and local governments." *Id.* This plan is all-inclusive. *Id.* Depending on how one defines each of these sectors, more than half of the economy could fall under this new plan. *Id.* What type of privacy would be left to the legitimate user of the Internet once this plan were to be followed by corporations on the Internet? *Id.* Another related issue will be the ability of the federal government to force the States to comply with this plan. *Id.*

77. *See id.* The President's Plan requires that the government and private sector work together. *Id.* The type of cooperation required for such a plan unparalleled. *Id.* The President sees that the only way to protect all of America's critical infrastructure cyberspace is for our "Nation as a whole [to] rise to [the] challenge." *Id.* at iii. The President, believing that the private sector would not cooperate if the government were to mandate such a solution, decided that the government must lead by example. *Id.* To do so, the President pledged that the government would be ready to help so as to ensure that the partnership of providing for the defense of America's critical infrastructure cyberspace would become a reality in the near future. *Id.*

78. *See id.* at iii.

79. *See id.* FIDNet will monitor Federal civilian Agencies and Department computers by detecting intrusion at critical system nodes. *Id.* at 13, 39. Significantly, FIDNet is structured carefully to identify a small class of intrusions. FIDNet focuses on attacks upon Federally owned, non-public networks or domains. FIDNet allows each of the participating Government Agencies to continue monitoring its own systems, in accordance with existing law. A preliminary legal review by the Justice Department has concluded that, subject to certain limitations, the FIDNet concept complies with the ECPA. However, an interagency legal review team continues to look at FIDNet issues and implications of the ECPA and many other statutes such as the Privacy Act of 1974 as the FIDNet concept continues to develop. *Id.* at 3-4. FIDNet will create an "automated system for incident reporting and handling." *Id.* at 13. The General Services Administration ("GSA") will operate a "centrally managed operational structure for processing, disseminating, warning, and coordi-

that uses thousands of software programs[80] to monitor the federal government's computers for suspicious activity, such as indications of computer network intrusions.[81] The project has been described as a burglar alarm.[82] First, information regarding unauthorized attempts to access a system will be collected by the respective government agency.[83] Second, anomalies would be reported to the General Services Administration ("GSA") for further analysis.[84] Thus, FIDNet would not allow the GSA to monitor at all. Traditionally, the monitoring of computer system security has been left to the system administrator of the respective agency or department.[85]

FIDNet will enhance the intrusion detection systems that many agencies already have in place,[86] and it will link federal agencies to-

---

nating status of the affected infrastructure systems." *Id.* at 13. *See also* Computer Technology Security: Hearing before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism & Government Information, 106th Cong. (Feb. 1, 2000) (statement of Marc Rotenberg) [hereinafter Rotenberg testimony]. "The Plan views the Internet as a domestic communications structure that must be secured from above from foreign threats. But the original architects of the network knew better. A communications network that can be secured from above can also be taken out from above." *Id.*

80. *See* Rotenberg testimony, *supra* note 79. "Networks of thousands of software monitoring programs would constantly track computer activities, looking for indications of computer network intrusions and other illegal acts." *Id.*

81. *See id.* This capability will function in concert with GSA's Federal Computer Incident Response Capability, and assist Federal Agencies to detect and analyze computer attacks and unauthorized intrusions; share attack warnings and related information across Agencies; and respond to attacks in accordance with existing procedures and mechanisms.

82. *See* Computer Technology Security: Hearing before the Senate Committee on the Judiciary Subcommittee on Computer Security, 106th Cong. (Feb. 1, 2000) (statement of John Tritak). "The program - much like a centralized burglar alarm system - would operate within long-standing, well-established legal requirements and Government policies covering privacy and civil liberties." *Id. But see* Rotenberg testimony, *supra* note 79. "An open-ended monitoring authority that essentially gives a single federal agency the authority to track the communications across all federal computer networks." *Id.* Such an authority is not founded on current statutory provisions. *Id.*

83. *See* Computer Security: Congressional Testimony, 106th Cong. (Mar. 9, 2000) (statement of John Tritak). Intrusion information would be collected by the "Agency experts" or their systems operators. *Id.*

84. *See id.* Only when the agency sees anomalous activity will it further that information on to the GSA. *Id.* FIDNet will "not become a pass-through for information to the Federal Bureau of Investigation or other law enforcement entities." *Id.* Law enforcement would receive information about computer attacks and intrusions only under long-standing legal rules—no new authorities are implied or envisioned by the FIDNet program." *Id.*

85. *See* Memorandum from Ronald Lee, Associate Deputy Attorney General, on Comments on the National Information Systems Protection Plan to Jeffrey Hunker, Director Critical Infrastructure Assurance Office (March 8, 1999) (on file with the Electronic Privacy Information Center at <http://www.epic.org/security/cip/lee_memo.html>. [hereinafter *Lee memo*].

86. *See* Protecting Information Infrastructure: Hearing before the Senate judiciary Committee Subcommittee on Technology and Terrorism, 106th Cong. (October 6, 1999)

gether to allow more solid security across the federal government.[87] In addition to alerting the GSA, the system will report anomalous activity to the National Infrastructure Protection Center ("NIPC")[88] to alert the other Federal network protection systems, providing for a kind of early warning system. Another extremely important aspect of FIDNet is the voluntary sharing of information from the private sector to the federal government, which occurred during the early February 2000 cyber-attacks.

D. FOURTH AMENDMENT

The Fourth Amendment[89] prevents the government from infringing on a citizen's natural and inalienable right[90] to be left alone by the government in order to pursue his or her own beliefs and thoughts.[91] Furthermore, the Framers intended that the Fourth Amendment protect all citizens from the encroachment of the state upon their natural liberties.[92] This right is not limited to persons in their homes. It attaches to an individual and will protect the individual wherever the individual travels.[93] The Supreme Court has held that the Fourth Amendment has

---

(statement of Michael A. Vatis, Director of the National Infrastructure Protection Center, Federal Bureau of Investigation).

87. *See id.* "FIDNet will enhance agencies' cyber security by linking their intrusion detection systems together so that suspicious patterns of activity can be detected and alerts issued across agencies." *Id.*

88. *See id.* The purpose of the NIPC is to provide early warning of attacks and to attempt to gather information about the attacker. *Id.*

89. *See* U.S. CONST. amend. IV. The Fourth Amendment 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.

Id.

90. *See* Meachum v. Fano, 427 U.S. 215, 230 (1976) (Stevens, J., dissenting). "The relevant constitutional provisions are limitations on the power of the sovereign to infringe on the liberty of the citizen." *Id.* "I had thought it self-evident that all men were endowed by their Creator with liberty as one of the cardinal unalienable rights. *Id.* "It is that basic freedom which the Due Process Clause protects, rather than the particular rights or privileges conferred by specific laws or regulations." *Id.*

91. *See* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967). "The [framers]. . .recognized the significance of man's spiritual nature. . .his feelings and . . . intellect [knowing] that only a part of the pain, pleasure and satisfactions of life are to be found in material things." *Id.*

92. *See* Meachum, 427 U.S. at 230.

93. *See* Terry v. Ohio, 392 U.S. 1, 8-9 (1968). The *Terry* Court recognized that right to privacy from unreasonable searches by the government is very broad:

> This inestimable right of personal security belongs as much to the citizen on the streets of our cities as to the homeowner closeted in his study to dispose of his secret affairs. For, as this Court has always recognized, 'No right is held more

three requirements: 1) unbiased warrants 2) issued in ongoing investigations for 3) specific objects or information. The first requirement is that disinterested magistrates should issue all warrants.[94] Lord Mansfield held over two centuries ago that limitations on the information sought should be left to a judge, not the officer seeking the information.[95] The second requirement is that the government should state the probable cause for requiring the individual's liberty to give way to the interest of the government.[96] This generally involves showing—that the subject of the warrant will further an ongoing criminal investigation.[97] This preserves a person's liberty to be free from governmental interference by preventing investigations into a person's history before a crime has even been committed.[98] Finally, the third requirement forces the government to describe with particularity what it is attempting to seize for its ongoing investigation.[99] The government is not afforded the opportunity to voluntarily comply the Fourth Amendment, nor can the government offer to use the least intrusive means to gather evidence for the purposes of

---

sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law.'

Id.

94. *See* Dalia v. United States, 441 U.S. 238, 255 (1979).

95. *See* United States v. United States Dist. Court, 407 U.S. 297, 316 (1972) (*citing* Leach v. Three of the King's Messengers, 19 How.St.Tr. 1001, 1027 (1765)). *See also* Connally v. Georgia, 429 U.S. 245, 250 (1977). The Court was presented with a case where the justice of the peace, who was paid for his services, issued a warrant. *Id.* "It is, in other words, another situation where the defendant is subjected to what surely is judicial action by an officer of a court who has 'a direct, personal, substantial, pecuniary interest' in his conclusion to issue or to deny the warrant." *Id. See also* United States v. United States Dist. Court, 407 U.S. 297, 316-17 (1972). "The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute." *Id.* The Court goes on to say that to allow the Executive branch to issue its own search warrants not subject to the neutrality of the judiciary is to give the Executive carte blanche. *Id.* Such "unreviewed executive discretion [that]may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." *Id.*

96. *See* Warden v. Hayden, 387 U.S. 294, 307 (1967). "There must, of course, be a nexus—automatically provided in the case of fruits, instrumentalities or contraband—between the item to be seized and criminal behavior." *Id. See also United States*, 407 U.S. at 318. "Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights." *Id.*

97. *See Dalia*, 441 U.S. at 255.

98. *See* United States v. United States Dist. Court, 407 U.S. 297, 316 (1972). "The further requirement of 'probable cause' instructs the magistrate that baseless searches shall notproceed." *Id.* They must further demonstrate that "'the evidence sought will aid in a particular apprehension or conviction' for a particular offense." *Id.*

99. *See id.* at 316 (citing Leach v. Three of the King's Messengers, 19 How.St.Tr. 1001, 1027 (1765)) (stating that "common-law principles prohibited warrants that ordered the arrest of unnamed individuals who the officer might conclude were guilty of seditious libel."). *Id.*

an ongoing criminal investigation.[100] The requirement of particularity prevents the government from showing probable cause and then making broad and general searches of the accused person or her home.[101] It also prevents the government from seizing items that have not been described in the warrant.[102] The less that is left up to law enforcement agencies, the less likely that an individual's Fourth Amendment rights will be infringed.[103] These three requirements are intended to prevent the government from conducting unreasonable searches and seizures.[104]

III. ANALYSIS

A. FOURTH AMENDMENT AND EXPECTATION OF PRIVACY

Increased Internet use has raised questions regarding the issue of privacy against government intrusion.[105] The FIDNet plan is being attacked because it lacks a legal foundation.[106] Whenever someone uses a network, they send packets of information from their computer to another computer.[107] These packets are subject to interception by a systems operator when she monitors the network to which she is assigned.[108] While the FIDNet plan specifically addresses the problems with intrusion on non-public federal computer networks, FIDNet, however, may serve as a model for corporate Internet monitoring plans or federal plans to monitor intrusion on public networks.[109] Therefore, it

100. *See* Katz v. United States 389 U.S. 347, 356-57 (1967). "[T]his Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end." *Id.*

101. *See* Stanford v. Texas, 379 U.S. 476, 485 (1965). Requiring search warrants to describe with particularity the objects to be seized proscribes all-purpose searches. *Id.* This also has the effect of preventing the police from coming into the home of a person with a search warrant, but to make some general search of the house in hopes to find evidence of other crimes. *Id.*

102. *See id.*

103. *See id.*

104. *See* U.S. CONST. amend. IV; *see also* Terry v. Ohio, 392 U.S. 1, 8-9 (1968).

105. At the same time that FIDNet is presented as a vital security protection, it has far-reaching privacy implications that some users may not find acceptable as a trade-off for inhanced protection against governmental or commercial interruptions.

106. *See* Rotenberg testimony, *supra* note 79. "There is no 'cyber threat' exception to the Fourth Amendment." *Id.* "The fact that the government announces that a warrantless search may occur is hardly a sufficient legal basis to permit such searches to take place." *Id.* However, as will be shown, there is ample authority upon which the FIDNet plan to rest.

107. *See How Does the Net Work?* (visited Mar. 26, 2000) <http://coverage.cnet.com/Content/Features/Techno/Networks/ss02.html>.

108. *See id.*

109. This could be a problem, because the expectation of privacy would be different on the Internet. While many sites do have privacy policies that are located on the bottom of a

becomes important to analyze network monitoring in relation to the potential privacy problems. In order to address these privacy concerns, the Fourth Amendment and the ECPA will govern both the President's Plan and FIDNet.

The FIDNet plan would not be effective if the government were encumbered by the requirements of the Fourth Amendment because of the sheer number of persons accessing federal civilian networks and the inability of the government to obtain search warrants on every person. There is good reason to scrutinize the government when it acts without the requirement of a warrant. The strict requirements for establishing a connection between the information sought and some criminal behavior,[110] and for obtaining permission to search, are crucial because authorities may otherwise be tempted to overlook privacy rights in their zeal to solve an ongoing investigation.[111] This conflict between individual privacy and law enforcement efforts illustrates the need for an independent magistrate who can make an objective determination of the sufficiency of the evidence of a crime before allowing the government to override the individual's privacy interest.[112] The particularity requirement also helps guard against an officer simply going out to a house and searching for anything at all that happens to be incriminating, whatever the item, and whatever the alleged crime.[113] In other words, it ensures that information must be subject to an ongoing investigation before it can be collected.[114] To tolerate anything less would directly encroach on the individual rights that the constitutional authors sought to explicitly

---

web page, many people do not read them, and may therefore be unaware of being monitored.

110. *See* Warden v. Hayden, 387 U.S. 294, 307 (1967) (explaining that there must exist a nexus between the item sought and ongoing criminal investigation).

111. *See id.* at 307-08. The Court discussing that even where very general warrant authority has been given for national security purposes, there have been limits. *Id.* "Even in the Espionage Act of 1917, where Congress for the first time granted general authority for the issuance of search warants, the authority was limited to fruits of crime, instrumentalities, and certain contraband." *Id.* "[T]he physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed." *See also* Riddick v. New York, 100 S. Ct. 1371, 1379-80 (1980) (citing United States v. United States District Court, 407 U.S. 297, 313 (1980). "It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." *Id.*

112. *See* United States v. United States Dist. Court, 407 U.S. 297, 316 (1972). "Where practical, a governmental search and seizure should represent both the efforts of the officer to gather evidence of wrongful acts and the judgment of the magistrate that the collected evidence is sufficient to justify invasion of a citizen's private premises or conversation."

113. *See id.* at 316-17 (citing Leach v. Three of the King's Messengers, 19 How.St.Tr. 1001, 1027 (1765)). "'It is not fit,' said Mansfield, 'that the receiving or judging of the information should be left to the discretion of the officer. The magistrate ought to judge; and should give certain directions to the officer.'" *Id.*

114. *See id.*

protect. Any search conducted outside the scope of judicial authority granted to the government under a warrant is unreasonable.[115]

There are, however, exceptions to this general rule that the government must obtain a search warrant. The Fourth Amendment allows the government to search without a warrant when a warrant exception exists because the person communicating information has no reasonable expectation of privacy.[116] The ECPA does not create a reasonable expectation of privacy in electronic communications.[117] Rather an individual must find such protection within the Fourth Amendment.[118] Further-

115. *See* Coolidge v. New Hampshire, 403 U.S. 443, 455 (1971). "Thus the most basic constitutional rule in this area is that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well delineated exceptions.'" *Id.*

116. *See* Katz v. United States 389 U.S. 347, 351 (1967). In *Katz*, the Court recognized that a particular place does not give rise to an expectation of privacy even though traditionally a reasonable person might not think that it would. *Id.* Although the Court has described Fourth Amendment problems in terms of areas, if has never suggested that this concept can serve as a solution to every Fourth Amendment problem. *Id.* Katz was convicted of communicating wagering information by telephone in violation of federal statute. *Id.* at 348. Federal agents recorded Katz's telephone conversations while Katz was inside a phone booth making calls. *Id.* The government had used a listening and recording device attached to the outside of the telephone booth, and at trial was initially allowed to admit these conversations into evidence. *Id.* However, Katz challenged the admission of such evidence on the grounds that a telephone booth was a constitutionally protected area. *Id.* While the Court technically rejected the petitioner's issue stating that the Fourth Amendment protects persons, not places, they instead chose to address the matter of whether the particular individual held an expectation of privacy in a particular place, as opposed to whether a particular place is protected. *Id.* at 350. The "correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase constitutionally protected area," but rather that the Amendment protects "individual privacy against certain kinds of governmental intrusion.". *Id.* The Court held that it is the private communication between two individuals that is at issue, regardless of whether the government, or public, may be able to observe that communication is taking place. *Id.* at 352. What a person seeks to preserve as private, even though they might be in a public area, may be constitutionally protected. *Id.* The Court found that in a variety of settings an individual may have an expectation of privacy that is reasonable:

> No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.

Id. at 352.

The government's effort to read the Constitution more narrowly ignores "the vital role that the public telephone has come to play in communication." *Id.* Merely because agents could see that Katz was communicating over the telephone, does not defeat the individual's expectation of privacy. *Id.* Therefore, what the individual is doing is more important with respect to Fourth Amendment analysis than where he is when he's doing it.

117. *See* United States v. Hambrick, 55 F. Supp. 2d 504, 507 (1999).

118. *See id.*

more, even if there was such a reasonable expectation of privacy, it can be destroyed by some of the exceptions to the ECPA.[119]

When an individual is arrested while committing a crime, he cannot object to a search of his person or home for items connected with that crime. By analogy, if a cyber-terrorist were arrested while hacking into a computer, the cyber-terrorist could not object to the search of the computer used to commit the crime.[120] The immediate area where the crime was committed may be searched without a search warrant, but the government is geographically limited as to what is subject to a warrantless search beyond that limited scope.[121] An individual has a right against unreasonable search and seizure only insofar as he has a reasonable expectation of privacy[122] balanced against the purpose behind the invasion into the individual's privacy.[123] However, an expectation of privacy cannot be an absolute bar against searches.[124] Rather, an expectation of privacy must be both subjectively reasonable and one that society is prepared to objectively consider reasonable.[125] It thus follows that a reasonable expectation of privacy will change over time as society changes in response to emerging technologies.[126] Therefore, whether the FIDNet

119. *See* 18 U.S.C. § 2511 (2)(a)(1).

120. *See* Agnello v. United States, 269 U.S. 20, 30 (1925). "The right [to search] without a search warrant contemporaneously to search persons lawfully arrested while committing crime and to search the place where the arrest is made in order to find and seize things connected with the crime as its fruits or as the means by which it was committed, as well as weapons and other things to effect an escape from custody is not to be doubted." *Id.*

121. *See id.* (holding that while the government may search the vicinity, such a right does not extend to places not specifically included in the warrant). "[The arrestee's] house was several blocks distant from. . .where the arrest was made" and therefore outside of the limited scope of a warrantless search. *Id.*

122. *See* O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (citing United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

123. *See* United States v. Place, 462 U.S. 696, 703 (1983). A necessary balance must be struck between the "nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." *Id.*

124. *See O'Connor*, 480 U.S. at 715.

125. *See id.* (citing United States v. Jacobsen, 466 U.S. 109, 113 (1984)) (stating that an expectation of privacy must be one "that society is prepared to consider reasonable"). This would rule out persons harboring expectations that others clearly find unreasonable in the hope of preventing the government from using certain information obtained through a warrantless seizure. *Id.* For instance, one could not have an reasonable expectation of privacy walking down the street shouting to a friend that you killed someone last night; nor could one have a reasonable expectation of privacy while standing in the window of a McDonald's with a shotgun aimed at several patrons.

126. *See id.* While the Supreme Court may not always follow this logic, it does seem apparent that society will accept as reasonable more expectations of privacy as population increases, thereby limiting the area of seclusion to which one may have become accustomed and the increase in technology that infringe on basic notions of privacy. An example of such are radio scanners that are capable of intercepting cellular phone calls.

plan is constitutional rests on whether a person using a federal civilian non-public computer network has a subjective expectation of privacy that society is willing to recognize as reasonable. The problem comes when a government agency begins to monitor information flowing into and out of its network.

B. Monitoring of Federal Civilian Non-public Networks

The FIDNet plan would allow network administrators to monitor hackers who might try to cause damage to the network by erasing stored data or planting malicious code.[127] For example, if a user were accessing information that they were not authorized to access or destroying computer files, a network administrator could monitor this activity either personally or through sophisticated software.[128] This is distinguishable from cases in which an employer sets up a video camera to monitor the work area to protect the employer's property from theft or damaged.[129] An analogy to the FIDNet plan would be a telephone company that monitors telephone calls when it believes that an individual is not paying for calls placed.[130] Under the FIDNet plan, administrators would monitor networks to ensure that users would not disrupt the integrity of an agency's network.[131]

Although there is no set formula to determine a reasonable expectation of privacy in a particular case,[132] the Court has looked at a variety of factors (none of which are present with respect to a person using a federal civilian computer network) to determine whether an expectation of privacy is reasonable in a particular case.[133] For example, the uses[134]

---

127. *See* Wilke, *supra* note 63.

128. *See* Defending America's Cyberspace, *supra* note 15, at xx.

129. *See* Vega-Rodriguez v. Puerto Rico Telephone Co., 110 F. 3d 174, 176 (1st Cir. 1997) (describing a telephone company's installation of video cameras for security purposes).

130. *See* United States v. Clegg, 509 F. 2d 605, 608 (1975).

131. *See* Defending America's Cyberspace, *supra* note 15, at xx.

132. *See* O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (citing Oliver v. United States, 466 U.S. 170, 178 (1984). "We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable." *Id.*

133. *See id.* (citing United States v. Chadwick, 433 U.S. 1, 7-8 (1977); Jones v. United States, 362 U.S. 257, 265 (1960); Payton v. New York, 445 U.S. 573 (1980)). "[T]he Court has given weight to such factors as the intention of the Framers of the Fourth Amendment: the uses to which the individual has put a location; and our societal understanding that certain areas deserve the most scrupulous protection from government invasion." *Id.* The Court went on to say that where the expectation of privacy is "based upon societal expectations that have deep roots in the history of the Amendment" the more likely protection will be given to the person. *Id.*

134. *See* O'Connor, 480 U.S. at 716. The Court has recognized persons with totally private offices, where in the usual course of business no other person has access to the contents of the office, as having an acceptable expectation of privacy in accordance with

to which an individual puts a location may determine whether society will recognize that the individual has a reasonable expectation of privacy.[135] Furthermore, a person who voluntarily exposes information to the public in a mass e-mail cannot claim a reasonable expectation of privacy over the information and consequently cannot claim Fourth Amendment protection.[136]

Under the FIDNet plan, a system set up to monitor whether intrusions have taken place would not disrupt any reasonable expectations of privacy. When users are logged onto a network, they communicate with a government server,[137] and therefore with a government agency. Furthermore, because this communication is flowing to a server, a network administrator is capable of monitoring what the user is doing on the server.[138] This is analogous to a worker being videotaped while working in an office. Therefore, to the extent that such a disclosure of information was voluntary, a hacker or user of a federal civilian network cannot claim a reasonable expectation of privacy.[139]

Second, an individual cannot claim a reasonable expectation of privacy while knowingly revealing information to a government agency.[140] Individual users disclose what they are doing to the federal agency by

---

societal beliefs. "Within the workplace context, [the] Court has recognized that employees may have a reasonable expectation of privacy against intrusions by police."

135. *See* Katz v. United States 389 U.S. 347, 351 (1967). (Harlan, J. concurring). Justice Harlan questions the Court's overt pronouncement that a particular place could be protected. *Id.* Rather, he says it is the subjective expectations of the individual as well as the public's willingness to accept such an expectation of privacy. *Id.* Whereas as here, where an individual made a telephone call at a pay phone "that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable." *Id.*

136. *See id.* "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Id.*

137. *See supra* note 42 and accompanying text.

138. *See* Amalgamated Transit Union v. Suscy, 538 F. 2d 1264, 1267 (7th Cir. 1976), *cert. denied,* 429 U.S. 1029 (1976) (stating that a governmental agency is subject to the Fourth Amendment protections against unreasonable searches and seizures). *See also How does the net work, supra* note 107.

139. *See* Vega-Rodriguez, 110 F. 3d at 181 (stating that it is constitutionally permissible to videotape employees when they are working especially when they are told in advance that such taping will take place, and video cameras have "no greater range, then objects or articles that an individual seeks to preserve as private may be constitutionally protected from such videotaping only if they are not located in plain view."). If each agency provides some sort of banner on the login page, then this will further help destroy any expectation of privacy. *Id.*

140. *See* Lewis v. United States, 385 U.S. 206, 212 (1966) (holding that where statements were willingly made to the agent there is no expectation of privacy); U.S. v. Amon, 669 F. 2d 1351, 1358 (10th Cir. 1981) (*citing* Couch v. United States, 409 U.S. 322, 335-36 (1973); Katz v. United States, 389 U.S. at 347) (holding that Fourth Amendment rights are not violated because one could claim a reasonable expectation of privacy when they voluntarily submit documents to the IRS).

communicating through its network. This is clearly distinguishable from *Katz*, because in *Katz* the individual had a subjective expectation of privacy in his communication by going in to a phone booth and shutting the door behind him so as to exclude any government official from hearing what he was saying.[141] In the network environment, even if such a person did harbor a subjective expectation of privacy, the expectation would be unreasonable because what the person is doing is directly communicated to the government agency.[142] This is analogous to situations where there is a statutory duty to report certain information to a federal agency.[143] The courts have held that such voluntary disclosure of such information leaves no reasonable expectation of privacy.[144] Furthermore, the communication is meant for no one other than the government agency that is being contacted. Therefore, a court would likely hold that the monitoring of a federal civilian non-public networks does not violate the Fourth Amendment because there is no reasonable expectation of privacy with respect to this type of communication.[145] However, in the event a court were to find a reasonable expectation of privacy, an analysis of the ECPA is appropriate.

To be a protectable communication under the ECPA, a communication has to fall within the statutory provisions.[146] An electronic communication within the ECPA is defined as the transfer of data by wire.[147] When an individual uses a federal agency's network, they will use a computer that is attached either by a wire directly to a federal civilian network or by a modem that is used to dial the access number.[148] Thus, the

---

141. *See* Katz, 389 U.S. at 352.

142. *See* Lewis, 385 U.S. at 212.

143. *See* Amon, 669 F. 2d at 1358 (citing Couch v. United States, 409 U.S. 322, 335-36; Katz v. United States, 389 U.S. 347).

144. *See id.*

145. *See* Lewis, 385 U.S. at 212.

146. *See* United States v. Rose, 669 F.2d 23, 27 (1st Cir. 1982) *cert. denied*, 429 U.S. 828 (stating that a communication must fall within the statutory provisions before it will be protected. Even if it did fall within statutory provisions, the defendant had no reasonable expectation of privacy when he broadcast information over his HAM radio.).

147. *See* 18 U.S.C. § 2510 (12). The ECPA provides the following definition for electronic communication:

> (12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
> (A) any wire or oral communication;
> (B) any communication made through a tone-only paging device;
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

Id.

148. *See* Platt, *supra* note 54.

communication of actions taking place on a federal network is within the definition of an electronic communication because data are communicated to the federal agency over its network.

The ECPA generally prohibits the interception of electronic communications by either a governmental agency or by an Internet Service Provider ("ISP").[149] The communication of actions on a federal agency's network is sent over an electronic communication service as defined within the ECPA.[150] Interception, as defined in the ECPA, is the acquisition of the content of an electronic communication.[151] The content of an electronic communication is what is relevant for the ECPA governing interception, not its context.[152] Because federal agencies may not legally record the contents of an electronic communication, it becomes important to distinguish between content and the context under which the information was sent. Content means the substance of a communication.[153] Therefore, although a federal agency could record such things as when a transaction occurred, they could not record its substance.

The ECPA recognizes the difficulty of determining whether a person could have an expectation of privacy that society was ready to accept as reasonable.[154] However, the ECPA does not confer any additional expectation of privacy.[155] The courts instead use the traditional test to deter-

149. *See* § 2511(1). The section provides in part: "(1) Except as otherwise specifically provided in this chapter any person who (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; shall be punished." *Id.*

150. *See* § 2510 (15). Electronic communication service is any "service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.*

151. *See* § 2510 (4). Intercept includes "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id. See also* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555. The legislative history makes it clear that the ECPA applies to the interception of data: "This Amendment clarifies that it is illegal to intercept the non-voice portion of a wire communication." *Id.* "For example, it is illegal to intercept the data or digitized portion of a voice communication." *Id.*

152. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555.

153. *See* 18 U.S.C. § 2510 (4). The definition of contents is that "when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." *Id.* For example, with respect to a love letter, the content would be the "I love you" attached, while the context would be the color of the envelope the letter came in. *Id.* It would not be illegal, for example, to intercept the time and date that an e-mail was sent, information that, if discovered, could be very valuable in itself even absent the content therein, while it would be an illegal seizure.

154. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555. "In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as [whether there does or does not exist a reasonable expectation of privacy] are not always clear or obvious." *Id.*

155. *See* United States v. Hambrick, 55 F. Supp. 2d 504, 507 (1999). Congress did not legislatively determine that a person has an expectation of privacy. *Id.* In *Hambrick*,

mine any expectation of privacy that an individual may have while communicating electronically.[156] Thus, the FIDNet plan must rely on one of the statutory exceptions if a court were to find a reasonable expectation of privacy within the communication.

The FIDNet plan would likely rely on the electronic communication service provider exception to the ECPA.[157] This exception provides that a network administrator may monitor communications in the normal course of business to ensure the quality of the service and to protect the property rights of the service provider.[158] An agency should be cautious

---

Hambrick had communicated with a 14-year old boy in a internet chat-room, and attempted to get the boy to move in with him. *Id.* at 505. The government obtained the online user name of Hambrick in order to determine his identity. *Id.* The court held that Hambrick did not "[have] a reasonable expectation of privacy in his name, address, social security number, credit card number, and proof of Internet connection." *Id.* The ECPA does not prevent a Internet Service Provider from turning over information that a subscriber has child pornography on his computer. *Id.* "The fact that the ECPA does not proscribe turning over such information to private entities buttresses the conclusion that the ECPA does not create a reasonable expectation of privacy in that information." *Id.*

156. *See id.* A person cannot voluntarily expose his data to another. *Id.* For a person to have a reasonable expectation of privacy "two conditions must be met: (1) the data must not be knowingly exposed to others, and (2) the Internet service provider's ability to access the data must not constitute a disclosure." *Id.*

157. *See Lee memo, supra* note 85. "Although each agency is a service provider and can therefore monitor its own network to protect against network intrusions, this does not mean, by extension, that GSA is a service provider within the meaning of the statute for the entire federal government." *Id. See also* Rotenberg testimony, *supra* note 79. An individual federal agency can monitor its own network, because it is a service provider as provided for in the ECPA. *Id.; see also* Hambrick, 55 F. Supp. 2d at 507. The GSA is not a service provider as defined in 18 U.S.C. § 2510 (15). *See* Rotenberg testimony, *supra* note 79. This misses the point, because under the FIDNet plan the individual federal agencies will continue to monitor their respective networks. *See supra* note 83. Furthermore, the ECPA provides an exception for electronic communication service providers. *See infra* note 163.

158. *See* 18 U.S.C. § 2511 (2)(a)(i). The statute provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or on officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

Id.

See also Clegg, 509 F.2d at 612 (5th Cir. 1975). "However, we feel that it is quite clear and we do hold that § 2511(2) (a), at a minimum, authorizes a telephone company which has reasonable grounds to suspect that its billing procedures are being bypassed to monitor any phone from which it believes that illegal calls are being placed." *See also* United States v. Harvey, 540 F. 2d 1345, 1353 (8th Cir. 1976). "The clear purpose of 18 U.S.C. § 2511(2) (a) (i), which was designed to allow the disclosure of justified wire monitoring by communica-

about monitoring all action on a network because the exception is limited to monitoring only when there is a reasonable basis for believing that its network integrity is being violated. To the extent that there is a reasonable basis for an intrusion, any information gathered during the course of ordinary business would be exempted from the ECPA.[159] In order for the FIDNet program to come under this exception, however, a government agency must be maintaining an electronic communication system within the statutory definition.[160]

An electronic communication service is a service that provides users the ability to "send or receive electronic communication."[161] An electronic communications system is a facility for electronic communications.[162] Such a system includes telephone companies as well as ISPs.[163] In *United States v. Monroe*, the court found that the Air Force was the electronic communication service provider within the ECPA because they supplied the means of electronic communication.[164] Likewise under FIDNet, a federal agency with a network that is capable of communicating would probably be covered under the service provider exception. This conclusion is further strengthened by *United States v. Mullin*.[165] As long as the information collected relates to the protection

---

tion carriers for the purpose of criminal prosecution of those who fraudulently use their services." *Id.* This is analogous to the FIDNet problem. A government agency that wishes to ensure that only those people that are permitted to gain access are those gaining access, so they set up a monitoring facility. Such a monitoring facility is not so concerned with prosecutions that it will turn over every single incident of person attempting to gain access. *See* Defending America's Cyberspace, *supra* note 15, at xx. Furthermore, the monitoring is done so as to ensure the quality control of their respective electronic communication systems.

159. *See* 18 U.S.C. § 2511 (2)(a)(i).

160. *See id.*

161. *See* § 2510 (15). The relevant portion states that "electronic communication service means any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.*

162. *See* § 2510 (14). "Electronic communications system means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *Id.*

163. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555. "Existing telephone companies and electronic mail companies are providers of electronic communication services." *Id.* Other services like remote computing services may also provide electronic communication services." *Id.*

164. *See* United States v. Monroe, No. 99-0536, 2000 WL 276509, *1 (C.A.A.F. Mar. 13, 2000). *See also* Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (stating that a city police department is an electronic communication service provider when it provides computers to police with which to communicate).

165. *See* United States v. Mullins, 992 F. 2d 1472 (9th Cir. 1993), *cert. denied*, 509 U.S. 905 (1993). The court in *Mullins* held that as long as the network administrator was acting within the scope of employment to protect the rights and property of her employer by moni-

of federal agency's network from unlawful, fraudulent, or abusive use based on a reasonable belief, the FIDNet plan will meet the service provider exception. While monitoring electronic communication may be lawful under the ECPA, there is still the issue of whether a federal agency is permitted under the statute to disclose such information to anyone besides a law enforcement agency.[166] Under the President's Plan, federal agencies will be disclosing information collected to the GSA for further analysis. The statute prohibits the disclosure of information acquired that is in contravention of the statute.[167] However, as has been demonstrated, a federal agency is not in violation of the ECPA when it monitors its networks.[168] Therefore, a federal agency can relate any information to the GSA obtained under §2511(2)(a)(i).

C. Accessing E-mail and Files on Personal Network Files

The question of whether stored communications are afforded a reasonable expectation of privacy remains. A federal agency may wish to monitor files loaded by hackers that have gained access to the network or a federal employee who has loaded a virus onto the network to cause damage to the network. A computer network can store e-mail or other files,[169] and often a user will have her own e-mail folder where her received messages are stored on the network.[170] The user can access the messages by accessing the network's e-mail system.[171] E-mail folders are similar to a mailbox, where other persons, specifically the deliverer, can look into the box and see the types of letters in the folder.[172] The crucial difference between e-mail and traditional mail is that network

---

toring employee's apparent misuse of American Airlines' electronic communication service, there was no violation of the ECPA.

166. *See* 18 U.S.C. § 2511 (1) (c) provides:

> Except as otherwise specifically provided in this chapter any person who— intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; shall be punished.

Id.

167. *See id.*

168. *See id; see also* Simmons v. Southwestern Bell Telephone Co., 452 F. Supp. 392 (W.D. Okla. 1978), *aff'd* 611 F.2d 392, 397 (1979) (holding that where an interception is lawful under §2511(2)(a)(i), Defendant is not liable for public disclosure of information intercepted).

169. *See* Encyclopedia Britannica, *Electronic Mail* (visited Mar. 29, 2000) <http://www.britannica.com/bcom/eb/article/7/0,5716,1567+1,00.html>. "Network users typically have an electronic mailbox that receives, stores, and manages their correspondence." *Id.*

170. *See id.*

171. *See id.*

172. *See* United States v. Monroe, No. 99-0536, 2000 WL 276509, *1 (C.A.A.F. Mar. 13, 2000).

administrators can see the contents of the messages.[173] In addition, sometimes messages are not sent directly to the personal e-mail folder because the folder may be full and incapable of storing more messages.[174] Messages are then stored in a temporary folder.[175] A network administrator, when determining how to redistribute the contents of the temporary folder, may come across the contents of the message by looking at the subject.[176] Likewise, documents may be stored in a user's network folder, where the network administrator can gain access to them in order to maintain the network.[177] The network administrator, therefore, acts like the first line of defense against files that may contain malicious data that could wreak havoc on a network. It becomes necessary to determine the expectation of privacy of a federal civilian network user when she accesses an agency's network in light of the administrator's active role in ensuring network integrity.

Searches in some areas deserve more Fourth Amendment scrutiny than others.[178] A search of a person's home, for example, deserves a high level of scrutiny.[179] Even the area immediately surrounding a person's home is subject to a higher level of scrutiny than are public places.[180] While the Fourth Amendment demands exacting scrutiny of warrantless searches and seizures in the physical space of an individual's home,[181] the FIDNet plan arguably does not involve searches of a person's home, office, or personal effects. Rather, the plan authorizes only system administrators to monitor unauthorized entry and anomalous activity of authorized users on the government network.[182]

---

173. *See id.*

174. *See id.*

175. *See id.*

176. *See id.*

177. *See id.* Network folders are somewhat analogous to a filing cabinet without a lock, where many files can be stored, but eyes can peer in and see what is in there. Like the e-mail folders, network administrators have access to personal folders to ensure that the network as a whole functions well.

178. *See* Agnello v. United States, 269 U.S. 20, 30 (1925).

179. *See* Payton v. New York, 100 S. Ct. 1371, 1380 (1980). The "Fourth Amendment law that some searches and seizures inside a man's house without warrant are per se unreasonable in the absence of some one of a number of well defined 'exigent circumstances." *Id.*

180. *See* Oliver v. United States, 466 U.S. 170, 178 (1984). "In this light, the rule of Hester v. United States, supra, that we reaffirm today, may be understood as providing that an individual may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home." *Id.*

181. *See* Terry v. Ohio, 392 U.S. 1, 9 (1968). (citing Union Pac. R. Co. v. Botsford, 141U.S. 250, 251 (1891)). "'No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law.'" *Id.*

182. *See generally* Defending America's Cyberspace, *supra* note 15.

In *O'Connor*, the Supreme Court held that a person in an office might have a reasonable expectation of privacy in parts of the office that are isolated.[183] Although a user accessing a personal folder on a federal civilian computer network may have a subjective expectation of privacy that items in a personal folder will not be searched, the search in *O'Connor* is distinguishable from the FIDNet plan. First, the fact that contents of a network folder are protected by a password known only to the user does not transform the folder's contents into the user's personal files, giving that user an reasonable expectation of privacy.[184] Furthermore, because the users' e-mail folders or personal folders are generally issued for official duties, they are similar to other types of government property, for which no reasonable expectation of privacy is recognized.[185] Because the information is exposed to a network administrator there can be no expectation of privacy.[186] It therefore becomes apparent that users of a federal civilian computer network have no reasonable expectation of privacy.

Even if users had a reasonable expectation of privacy, the Court would weigh the purpose behind the imposition of the search when it

183. *See* O'Connor v. Ortega, 480 U.S. 709, 715 (1987). "Having determined that Dr. Ortega had a reasonable expectation of privacy in his office, the Court of Appeals simply concluded without discussion that the 'search . . . was not a reasonable search under the fourth amendment.'" *Id.*

184. *See* United States v. Monroe, 50 M.J. 550, 558-59 (A.F.C.C.A. 1999) *aff'd* 2000 WL 276509. While a user may be able to change his initial password so as to prevent other user's from accessing his e-mail or other files, network administrators are not denied the knowledge of the users' password because it is the network administrator's job to ensure that the network is running at maximum efficiency. *Id.* "What this means is that the existence of a personal password is only of passing significance, because appellant was not allowed a password in order to exclude the EMH administrator, but potential interlopers only." *Id. See also* McLaren v. Microsoft Corp., NO. 05-97-00824-CV, 1999 WL 339015 (Tex. Ct. App. May 28, 1999). McLaren equated a personal password with a locker supplied by a company that had a lock purchased by an employee. *Id.* at *4. The court distinguished this analogy by stating that a locker is provided to store personal items, not work items. *Id.* The court stated that the computer that McLaren used was given to him to person work-related jobs including the "ability to send and receive e-mail messages," and as a consequence the e-mail messages were an "inherent part of the office environment." *Id.*

185. *See* Monroe, 50 M.J. at 558-59 (*citing* United States v. Muniz, 23 M.J. 201, 204-6 (C.M.A.1987), *aff'd* 2000 WL 276509 (stating that there is no expectation of privacy in government property "even if the government property in question is capable of being secured."). Furthermore, the court found that because his e-mail folder was issued for "official duties, his electronic mailbox was akin to other types of government property routinely designated for or assigned to military personnel for performance of their official duties." *Id.*

One does not acquire a reasonable expectation of privacy in government property designated or assigned under these circumstances." *Id.* at 558.

186. *See id.*

evaluated the constitutionality of the governmental action.[187] The Court looks first at the interest advanced by the government.[188] The interest need not be to protect law enforcement personnel.[189] Rather, the government must simply state that its purpose is to enhance crime protection and detection, as opposed to protecting the welfare of the law enforcement personnel per se.[190] Second, the Court weighs the public's interest against the nature and extent of the search to determine whether the interest sought outweighs the individual's rights.[191]

In *U.S. v. Place*, the Supreme Court held that the detention of a traveler's luggage to identify its contents is constitutional.[192] Drug enforcement agents received information that Place was carrying narcotics in his luggage.[193] The defendant argued that the police should not be able to simply assert a general law enforcement interest to overcome the reasonable expectation of privacy that a person may have, because then all warrantless searches would be valid where the government has established that the individual may be involved in a crime.[194] The Supreme Court held that the public has an interest in stopping the illegal transportation of drugs.[195] This allows a balance to be struck between the

187. *See* United States v. Place, 462 U.S. 696, 703 (1983).

188. *See id.* (holding that the government has an interest in preventing the noxious spread of narcotics that has caused so much damage to society, and that therefore the seizing of a suspected drug trafficker's luggage is within the constitutional limits of the Fourth Amendment). *Id.*

189. *See id.* at 703-04.

190. *See id.* In *Place*, the Court reaffirmed the requirement of a public interest to be asserted by the government before they could overcome an expectation of privacy that a person might have. *Id.* The Court went on to reject respondent Place's argument that the government must be able to show that the police were protecting their personal welfare before a warrantless search, absent exigent circumstances, would be valid. *Id.* The Court stated that *Terry* stood for the proposition that all that the government must demonstrate is that the initial seizure of the person was used as a means of an "effective crime prevention and detection." *See id.* In other words, the government need not demonstrate that the officers are fearing some imminent threat or danger to their person before they may initiate search without a warrant. *See id.*

191. *See id.* at 705.

192. *See id.*

193. *See* United States v. Place, 462 U.S. 696, 699 (1983).

194. *See id.* at 703-04. Place argued that "absent some special law enforcement interest such as officer safety, a generalized interest in law enforcement cannot justify an intrusion on an individual's Fourth Amendment interests in the absence of probable cause." *Id.*

195. *See id.* The test that the Court has applied is whether the interests of the government are substantial. *Id.* In other words, the interest sought to be advanced need not be "independent of the interest in investigating crimes effectively and apprehending suspects." *Id.* The Supreme Court agreed with the government's argument that seizures are permitted "on the basis of reasonable, articulable suspicion, premised on objective facts" that a crime is taking place. *Id.* The Supreme Court stated that the "[t]he public has a compelling interest in detecting those who would traffic in deadly drugs for personal profit." *Id.* (quoting United States v. Mendenhall, 446 U.S. 544, 561 (1980) (Powell, J. con-

Fourth Amendment and law enforcement.[196]

The government's interest in preventing users who illegally access or misuse their access to civilian computers from disrupting the integrity of federal civilian computer systems, and ultimately the administration of the federal government, is as compelling as the interest that was upheld in *Place*. Any expectation of privacy that a user could possibly have must be weighed against the government's interest.[197] Given the result in *Place*, a user's expectation of privacy in e-mail folders or personal network folders would probably not overcome the government's interest in protecting its networks, if the court recognized a reasonable expectation at all.[198]

If a court found that the user had a reasonable expectation of privacy, an analysis of the ECPA as it applies to stored communications would follow. Electronic communications under the ECPA includes e-mail.[199] Electronic communications, however, do not include cordless telephone transmissions between a base unit and the cordless telephone.[200] Wire or oral communications are also excluded.[201] Communications from a tracking device are also excluded from the meaning of

---

curring). *See also* Michigan v. Summers, 452 U.S. 692, 700 (1981). The Court in *Summers* held that the police could search an individual coming out of a drug house that the police had a search warrant to search. *Id.* at 693. Summers challenged the search as unconstitutional. *Id.* The Court stated that there are those "seizures admittedly covered by the Fourth Amendment constitute such limited intrusions on the personal security of those detained and are justified by such substantial law enforcement interests that they may be made on less than probable cause, so long as police have an articulable basis for suspecting criminal activity." *Id.*

196. *See Place*, 462 U.S. at 705.

197. *See id.* at 703.

198. *See id.*

199. *See id.* Electronic mail is communication between person over public or private telephone lines. *Id.* Usually, messages are communicated through a computer keyboard, and then sent over the "telephone lines to a recipient computer operated by an electronic mail company." *Id. See also* McVeigh v. Cohen, 983 F. Supp. 215 (1998).

200. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555.

201. *See id.* Communications that are made through a paging device that is tone-only are also excluded from protection under the ECPA, because the Supreme Court has held that information revealed voluntarily is not protected under the Fourth Amendment. *See* Lewis v. United States, 385 U.S. 206, 212 (1966). A tone-only pager informs the user that a message is sent by emitting a beep. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555. The user, then, has to calling a predetermined number to retrieve the sent message. *See id.* Whereas, a display pager, the kind most persons are accustomed to today, may display the message visually. *Id.* Afterwards, the person call telephone the individual sending the message without the use of a third person. *Id. See also* United States v. Miller, 425 U.S. 435, 443 (1976). The Constitution does not proscribe the attainment of "information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.*

electronic communication.[202] Under the ECPA it is illegal to access stored electronic communications.[203] The definition of electronic storage includes the temporary storage of electronic communication that is intermediate or incidental to the communication.[204] Electronic storage also includes the periodic backup of electronic communication such as e-mail.[205] The government can access the contents of electronic storage of an electronic communication only with a validly issued warrant.[206] This mandate, however, is not absolute, because where the contents of an in-

---

202. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555. A tracking device can be electronic or mechanical, and is usually authorized by a court order, to permit an individual to monitor the movement of a person or object. *Id.* An example would be a device used to monitor the movement of a car.

203. *See* 18 U.S.C. § 2701 (a). The statute reads as follow:

> (a) Offense.—Except as provided in subsection (c) of this section whoever—
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceeds an authorization to access that facility;
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

Id.

204. *See* 18 U.S.C. § 2510 (17). The Statute provides

> (17) "electronic storage" means—
> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

Id.

205. *See* 18 U.S.C. § 2510 (17)(B).

206. *See* 18 U.S.C. § 2703 (a). The government can obtain the "contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant." *Id.* It becomes easier for a law enforcement agency would like to obtain the contents of an electronic message that has been in storage for more than 180 days with the use of a warrant or by giving notice to the user of the electronic communication system. *Id.* The statute provides that

> A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

Id. 18 U.S.C. 2703 (b) provides that

> Contents of electronic communications in a remote computing service.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity

Id.

dividual's home computer are discovered by an ISP and then turned over the police, the police may use the information despite the lack of a valid warrant.[207]

E-mail and other electronic communications that might be stored in a personal network folder would be protected under the ECPA.[208] However, one exception to the ECPA is particularly relevant to the FIDNet plan. This exception allows the provider of an electronic communication service to access any electronic communication that it stores even if another person stores that information.[209] In *United States v. Monroe*, the court found that the government was an electronic communication service provider within the ECPA definition.[210] The government could access any of Monroe's e-mail that was stored on the network.[211] However, the government cannot disclose the contents of a communication on its networks that appeared to relate to the commission of a crime unless the contents were discovered inadvertently.[212] Under the FIDNet plan,

---

207. *See* United States v. Kennedy, No. 99-10105-01, 2000 WL 49055, at *5 (D. Kan. Jan. 3, 2000). An ISP that turns over information about a subscriber's account information. *Id.*

208. *See supra* note 197.

209. *See* 18 U.S.C. § 2701 (c). This statute provides:

> (c) Exceptions.—Subsection (a) of this section does not apply with respect to conduct authorized—
>
> (1) by the person or entity providing a wire or electronic communications service;
>
> (2) by a user of that service with respect to a communication of or intended for that user; or
>
> (3) in section 2703, 2704 or 2518 of this title.

Id.

210. *See* United States v. Monroe, No. 99-0536, 2000 WL 276509, *1 (C.A.A.F. Mar. 13, 2000). *See also* Bohach, 932 F. Supp. at 1236. (Stating that a city police department is an electronic communication service provider when it provides computers to police with which to communicate). *See also United States v. Simons*, 29 F. Supp. 2d 324, 325 (E.D. Va. 1998) *aff'd and rem'd* No. 99-4238, 2000 WL 223332 (4th Cir. Feb. 28, 2000). In *United States v. Simons*, Simons was employed by the Foreign Bureau of Information Services (FBIS). *Id.* The systems operator, while conducting routine service of the network's fire wall noted that there were a large number of "hits" under the word "sex." *Id.* at 326. The systems operator noted that a large number of the hits were located on Internet sites. *Id.* He, then proceeded to tell the Network Branch Chief of his findings. *Id.* After looking at the Internet sites, the systems operator was able to determine that the content of the Internet sites was related to the business being conducted by Simons. *Id.* The court found that such a search of the firewall and the computer was in the course of business of the systems operator of maintaining the computer network. *Id.* at 328. When the systems operator examined the firewall, he was not looking at a particular user's activity. *Id.* Rather, only after he found hits that alerted him as to the misuse of the system did he further investigate the activity. *Id.* "This search was justified at the inception because it was Mauck's duty as Manager to monitor Internet use. The search was also reasonably related in scope because it was reasonable that a keyword "sex" search would show whether any users were engaging in inappropriate workplace computer activity." *Id.*

211. *See* Monroe, 2000 WL 276509 at *5.

212. *See* 18 U.S.C. § 2702 (b) (6). This provision provides:

therefore, information that is stored would have to be discovered inadvertently.[213] FIDNet intentionally looks for anomalous information that might show signs of intrusion.[214] Futhermore, the GSA, and other agencies that are being told the information, are not law enforcement agencies.[215] The GSA is a service organization;[216] there is no hint of law enforcement. Therefore, an agency must not disclose any information to the GSA or any other agency that is not a law enforcement agency.[217]

The government should seek to improve the existing technology to prevent people from gaining initial access instead of thinking in terms of how much monitoring is necessary once a user connects to the network. In addition, although users of a nonpublic federal civilian computer network have little or no reasonable expectation of privacy, users may still subjectively believe they will not be monitored. The government should disclose such information through a method that prevents user access until the networks alerts users that they are subject to monitoring.

IV. CONCLUSION

The President's Plan to protect federal agency from cyberterrorism certainly has laudable goals and can operate within the constitutional limitations on search and seizure. However, it may not be necessary to implement a monitoring program like FIDNet. Rather, the government has several alternatives to increased monitoring within governmental organizations. Such alternatives, individually, will not completely dispense of privacy issues on government networks, but each offers certain

---

(6) to a law enforcement agency—
(A) if the contents—
(i) were inadvertently obtained by the service provider; and
(ii) appear to pertain to the commission of a crime; or
(B) if required by section 227 of the Crime Control Act of 1990 [42 U.S.C.A. § 13032].

Id.

213. *See id.*

214. *See* Defending America's Cyberspace, *supra* note 15, at xx.

215. *See* 18 U.S.C. § 2702 (b) (6).

216. *About the U.S. General Services Administration* (visited Mar. 29, 2000) <http://www.gsa.gov/aboutgsa.htm>. The mission statement provides the following description concerning the duties of the GSA:

> We provide expertly managed space, supplies, services, and solutions, at the best value, to enable Federal employees to accomplish their missions. GSA is about great work environments—wherever government works, whether in an office building, a warehouse, a national forest, or a government car. In support of this mission, GSA provides workspace, security, furniture, equipment, supplies, tools, computers, and telephones. GSA also provides travel and transportation services, manages the Federal motor vehicle fleet, oversees telecommuting centers and Federal child care centers, preserves historic buildings, manages a fine arts program, and develops, advocates, and evaluates governmentwide policy.

Id.

217. *See* 18 U.S.C. § 2702(b)(6).

advantages that might enable the government to lead private industry in transforming the Internet privacy debate.

The government can achieve its goal of securing networks and giving effect to network users' subjective expectations of privacy in three ways: legislation recognizing a greater expectation of privacy in electronic communications; legislation or federal agency regulation requiring a posting of notice to any person entering the network; and increasing security on federal networks to prevent access.

The first alternative of legislating a greater expectation of privacy would be the least desirable because it could give criminals a safe harbor within which to hide when they are caught. The second alternative, posting a notice on the entry of a network that users may be subject to monitoring, is the least expensive method of giving notice to users. Such a notice should include a link that would have to be actively clicked by the user, indicating that they understand everything included in the notice. It provides users with knowledge of potential monitoring. Further, it seriously weakens claims of an objective expectation of privacy because any user would have submitted to the federal agency that they read and understood the terms of use of the network.

Finally, the most obvious, but most expensive, means of achieving secure networks would be to secure the networks at the entrance. In other words, the focus should be on the door of the network and preventing unauthorized access, rather than on network monitoring when the individual is already on the network. Such a plan is analogous to leaving the keys in your car with the doors unlocked and watching as the thief starts your car and drives away. Agencies should know who is at the door before the door opens, which is why network security must begin with who is accessing federal networks.

Similar plans will be applied to networks of private critical infrastructure corporation as well as Internet sites. The same issues will apply. The same alternatives will exist. If the President desires that the government take the lead in protecting critical infrastructure data, he should lead by adopting a plan that focuses less on monitoring and more on preventing access. The more monitoring becomes an acceptable, entrenched alternative, the less likely users will be able to support a objective expectation of privacy.

David Hueneman