Towards Coherent Regulation of Law Enforcement Surveillance in the Network Society

Serena Chan
Laboratory for Information and Decision Systems
Massachusetts Institute of Technology
Cambridge, MA 02139
chans@mit.edu

L. Jean Camp*
Kennedy School of Government
Harvard University
Cambridge, MA 02139
Jean_Camp@harvard.edu

Abstract

In this paper, we study the evolution of telecommunications technology and its impact on law enforcement surveillance. Privacy and the need for law enforcement to conduct investigations have not been at the center of the recent public policy debate. Yet, policy environments have approved law enforcement surveillance that can be and is intrusive. Law enforcement surveillance therefore deserves particular attention when discussing the basic human right to privacy. We illustrate that despite the gradual acceptance of the basic human right to privacy, in the digital age the United States (US) government continues its historical pattern of using technology to enhance its power of search . The most recent example is the installation of the Digital Collection System 1000 (DCS1000), formerly known as Carnivore, a classified packet sniffer, on American networks by the American federal law enforcement agency.

We discuss pre-convergence surveillance in the areas of US postal mail, telegraph and telephone communications, as well as physical surveillance. We also analyze post-convergence surveillance in the area of physical surveillance, encrypted telephony and the Internet (e.g., electronic mail). From examination of these cases, we see that not only is there a technology convergence but also a convergence of jurisdiction. We note that ensuring protection of privacy rights of the individual is not an adequate method of keeping government surveillance in check.

* The contributions of Jean Camp to this work were funded in part by NSF grant 9985433, and an equipment grant from HP. This work represents solely the opinions of the authors, and in no way reflects the beliefs of Harvard, the United States Government, or the Notes/Windows environments in which we are employed.

We conclude with a discussion of surveillance principles on which to build a coherent technology-neutral policy for law enforcement surveillance of electronic information. A good policy takes into account many factors, including technology, cryptography and electronic surveillance, the aims and practices of intelligence and law enforcement agencies, and the history of society's attempts to deal with the problems of technological change over the previous centuries.

1 Introduction

The growth of interception is a result of technological improvements that have drawn more and more valuable traffic onto telecommunications channels. The means by which we communicate (e.g., telegraph, telephone, electronic mail and video conferencing) have expanded due to technological changes. In the twentieth century the frequency of communications and interactions has increased as communications technology has advanced, with ever more trivial messages being transmitted and thus potentially intercepted. [Schement and Terry 1995] The ability intercept those increasingly frequent communications (e.g., wiretaps) means that spying on communication channels becomes increasingly rewarding for governments, businesses and criminals. Laws cannot change the fact that communications are inherently subject to interception and digital technology is making interception ever easier. [Diffie, 1998]

In this paper, we study the evolution of telecommunications technology and the challenges to surveillance faced by law enforcement agencies. We focus on the history of the United States (US). US government surveillance will have an increasing impact on the global civil society because of the globalization of packet-based communications networks- as a great deal of international traffic travels across American network wires. The bandwidth exchanges operating on the coasts of the US illustrate that surveillance policies in the US will effect citizens in the Pacific Rim and the European communities. This was evident by the fact that China lost its Internet connection to foreign web sites due to a broken fiber optic cable connecting China to the US. The Boston Globe reported that the undersea link carries approximately one-quarter of US-Asian Internet traffic. We illustrate that the United States government has historically tried to increase its power of search, despite the gradual acceptance of the basic human right to privacy.

In Sections 2 and 3, we discuss surveillance practices preceding the widespread adoption of digital communication in the areas of US postal mail, telegraph and telephone communications.

As new technologies arise, law enforcement agencies will continually face challenges in maintaining their traditional practices of electronic surveillance capabilities. In Section 4, we analyze surveillance in the area of physical surveillance, encrypted telephony and the Internet (e.g., electronic mail) in the US. From the examination of these cases, we will see that not only is there the much-heralded convergence of telecommunications channels, but also a resulting convergence of jurisdictions. Rather than curtailing law enforcement surveillance activities per se, policy in the US has emphasized privacy protection of individuals in particular sectors (e.g., video tapes rentals, credit records). [Camp, 2000] The traditional assumption that ensuring the privacy of the individual will keep government surveillance in check is not adequate when sectorial protection for privacy is the norm.

In Section 5, we discuss privacy principles on which to build upon in order to create a coherent technology-neutral policy for law enforcement surveillance of electronic information. We discuss how a US-based digital surveillance standard might comply and conflict with European data protection principles. We conclude that the American legal approach of sectorial protection of privacy offers less promise than the European data-protection paradigm for creating and maintaining consistent surveillance policies in an time with rapidly changing information technology. In Section 6, we conclude that ultimately, to create the foundation for good policy we must be aware of many factors, including technology, cryptography and electronic surveillance, the aims and practices of intelligence and law enforcement agencies, and the history of society's attempts to deal with similar problems over the previous centuries. We offer a set of principles, comparable to but distinct from those offered by the Council of Europe, for post-convergence surveillance.

2 Postal Mail Surveillance

Postal mail privacy depends on the care of the carrier because communications can be compromised only through physical interception of letters and packages. In colonial America, before a formal postal system existed, letters and packages were transported in an ad hoc manner by ship captains, friends or hired delivery men. Mail delivered to a central location in town might sit unattended, opened for inspection by anyone passing by, until the intended recipients collected their mail. The privacy-protecting technologies of the time included sealing letters with wax or encoding those messages where secrecy was critical. [Kahn, 1996] These technological fixes to the problem of communications privacy were found inadequate, and legal action was taken by the English. Thus the 1710 English Post Office Act prohibited the opening of mail except by warrant. In 1753, the Postmaster General for the English Colonies, Benjamin Franklin, prompted all postmasters to take an oath not to open mail. Yet British officials, not

Franklin's postmasters, regularly opened mail searching for information regarding plots and conspiracies among the colonists preceding the American Revolution. Military authorities on both sides throughout the American Revolution continued the practice of invading privacy by opening letters assumed to be full of intelligence information. [Diffie, 1998; Regan, 1995]

Incentives to open letters existed even in the early days of the US. Mail was easy to intercept and motives came from many sources, such as partisan rivalries. George Washington and Thomas Jefferson have both given accounts suggesting that their letters were opened. Privacy protection of mail communications increased to some extent by the nineteenth century, through a rise in mail volume and the use of envelopes and locks on mailbags. On the legal front, a major postal statute of 1825 prohibited everyone, not only postal workers, from opening a letter before it was delivered to the intended recipient. [Regan, 1995] The law made no exemption for opening letters for official purposes.

Yet despite the fundamental respect that the mails held, the various crises of the nation resulted in significant changes in privacy of the mails. In *Searight v. Stokes, 44 US (3 How.) 151, 169 (1845)*, a case on state taxation of Federal mail, it was determined that mail is not only under the protection of the Government, but that the mail is the property of the Government.

Social tensions have repeatedly given rise to the call to limit the distribution of controversial ideas using the mails. During his State of the Union speech, President Andrew Jackson proposed making abolitionist mailings illegal in the Southern states. This was objected to as an extension of Federal power and failed to pass. However, after a bloody extended civil conflict, the mood of the nation was considerably altered. In 1878, the Supreme Court elevated this protection against examination of letters by clarifying Fourth Amendment coverage to first class postal letters in *Ex parte Jackson (96 US 727)*. [Diffie, 1998] However, in this ruling the Court allowed a privilege for Federal Government in the mail of lower classes by stating, "the right to designate what shall be carried necessarily involves the right to determine what shall be excluded." The extension of governmental power to examine mail does not seem extreme, when placed against the recognition that a considerable amount of the nation was under or recently had been under martial law.

The next threat to second- and third-class mail was the concern of morality resulting from new technologies and the associated economic dislocations. Anthony Comstock was a leader of the turn-of-the-century crusades to protect the corruptible morality of America's youth from the overwhelming intensity of new media (including broadcasting, color lithography and automated presses). As Postmaster General, Comstock prohibited the use of mail to send any "obscene, lewd, or lascivious book, pamphlet, picture, paper, print, or other publication of an indecent

character." Implementing such controls required regular searches of second- and third-class mail and seizures of documents intended for distribution. Such controls still hold today in some states, for example, prohibiting unsolicited mailing regarding contraceptives and women's health. [Beisel, 1997]

Similar importance was given to mail as the Cold War emerged in the early 1950s. In the twentieth century, the US Postal Office was allowed to detain "communist political propaganda." [Alderman & Kennedy, 1995] Until 1965, in *Lamont v. Postmaster General (381 US 301),* the government ownership of the mails could outstrip the right of the people to private mail. That the right to speak and the closely related freedom to read actually require the freedom to read without fear of surveillance was not fully recognized with respect to the mails until Griswold V. Connecticutt overthrew the remnants of Comstockery. [Cohen, 1996]

Controls on mail remained until the seventh decade of the twentieth century. Throughout this period, private mail carriers could be hired for the purpose of message delivery. Private mail carriers had at all times (excluding war) the unquestioned support of the Fourth Amendment. Similar rights exist today; however, the private carriers can now choose to cede these rights for the packages in their possession, and thus the users. Again "the right to designate what shall be carried" includes designating the rights allowed to the recipient and senders of parcels. For example, United Parcel Services (UPS) allows bulk searches of its packages (e.g., law enforcement agents who bring in drug-sniffing dogs) while Federal Express (FedEx) requires a warrant for specific packages.

In the age of Benjamin Franklin, the Postmaster General held a high standard. Later, as violent political disagreement tore the nation, the primacy of government ownership came to rule. This peaked with the appointment of Anthony Comstock, who leaves his name as a synonym for censorship. With respect to the mails, the sorting and distribution technologies have changed but the security of an individual envelope has varied little during the centuries. Public mood overwhelmed Constitutional controls, reaching a peak at the end of the nineteenth century. There are traditions in the law to argue for broad-based prohibition of materials, as well as arguments for a high degree of user privacy. Like the concept of individual equality and autonomy before the law, the development of privacy in the mails was stated gracefully during the nation's founding. Yet the attaining the ideals required two centuries of halting progress.

3 Telegraph and Telephone Surveillance

The advent of the telegraph and telephone brought forth new methods of communications. Because the communications are conducted in a physically private space and sent by wire, people assume their communications have a level of privacy that often does not exist. [Regan, 1995] Telegraph information can be obtained by reading the messages from copies kept by the telegraph companies or by tapping the wire. The US government preferred the first search method because wide government surveillance of the telegraph required technical skill and training. [Diffie, 1998] Telegraph communications were constantly tapped during the American Civil War by both the Union and Confederate armies to determine battle plans and troop movements. Like the Internet, the telegraph systems were based on early military investment. Also like the Internet, the private use of the technology easily outstripped the government-related uses as the technology became widely adopted.

As the government tried to control the wired communications medium by obtaining copies of telegrams and censoring messages, many of the company operators refused to cooperate with the government. It seemed that the government sough to establish broad search privileges for itself while trying to protect communications privacy from the owners and operators of the networks. Nevertheless, public officials and private parties discovered how to tap communications almost immediately after the invention of the telegraph and telephone. [Diffie, 1998] Wiretapping would occur for many decades due to the ease of tapping and the value of information obtained. Press organizations would tap the wire communications of rival organizations to facilitate being first to report major news events. Wiretapping was also used for personal financial gain in the mid-1800s when several Western Union operators and a Wall Street broker intercepted messages regarding financial matters and substituted false information. [Regan, 1995]

As is the case today, privacy-enhancing technologies and regulations were sought to address the lack of privacy. Five years after the patent of the telephone, a patent for a telephone scrambler was issued. During the war emergency of World War I, Congress effectively took ownership of the telephone company, paying 'rents' instead of dividends to holders of stock in AT&T. After the war there was considerable debate with respect to the wisdom of private ownership, which was increasingly a global anomaly. While under governmental control, Congress prohibited the tapping of or interference with telegraphs and telephone messages "without authority." After the war emergency, over the objections of the Department of War, the telephone system was placed again in private hands and the controls on wiretapping passed out of effect. The sole purpose of the legislation was to protect the property of the telegraph and telephone companies and the government while under government control; not for protecting the privacy of users or content of communications. [Regan, 1995]

It was not until the late 1920s when privacy of communications would become a public issue. Across the nation different local police departments followed vastly different standards, some using wiretapping regularly and some seeing it as a clear violation. By 1927, more than twenty-five states made wiretapping a crime but wiretapping was prevalent at both the state and federal levels. The constitutionality of wiretapping was first tested in the *Olmstead v. United States, 277 US 438 (1928)*. Based on telephone wiretaps presented by federal agents, Roy Olmstead, a bootlegger in the state of Washington, was convicted of violating federal Prohibition laws. The federal trial judge admitted the wiretap evidence even though Washington state law prohibited wiretapping. Olmstead appealed his conviction arguing that the wiretap evidence should not have been admitted, however the appeals court upheld the conviction. The appeals court ruled that because there was no trespassing or seizing of physical property, wiretapping did not violate either the Fourth or Fifth Amendment. The Supreme Court reviewed the appeals court decision and supported it. [Regan, 1995] In the majority opinion, the Supreme Court found it to be the job of Congress to protect telephone privacy by stating, "the policy of protecting the secrecy of telephone messages by making them, when intercepted, inadmissible as evidence in federal criminal trials may be adopted by Congress through legislation, but it is not for the courts to adopt it by attributing an enlarged and unusual meaning to the Fourth Amendment." Yet the ringing dissent argued presciently "subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."

The notion of wiretaps as searches that were not protected under the Constitution led the way for widespread wiretapping. There was no uniform wiretap policy among the federal agencies or between the states. Wiretapping was used as means of political and social control, beyond the limits of proper law enforcement and occurred unchecked due to public ignorance. [Diffie, 1998] Some agency heads believed that law enforcement interests justified privacy invasions imposed by wiretapping while others did not. Although bills were introduced in Congress to ban and regulate wiretapping, wiretapping practices continued without any change until the development of the current wiretapping policy in 1967 through the courts when the *Olmstead* case was overturned in *Katz v. United States, 389 US 347 (1967).*

In *Katz,* the Federal Bureau of Investigation (FBI) placed a bugging device in a telephone booth with the intention of monitoring Katz's conversations, allegedly regarding gambling operations. The Supreme Court overturned *Olmstead* and ruled that the telephone bug violated privacy and constituted a search and seizure under the Fourth Amendment. [Regan, 1995] The Fourth Amendment of the Constitution was now interpreted as providing protection against illegal searches of an individual and not just an individual's property.

Title III of the Telecommunications Act specified crimes for which a court order could be requested and established procedural requirements for law enforcement, including obtaining a court order approved by a high-ranking prosecutor; proving that probable cause existed for believing that a crime had been committed, that the target of the surveillance was involved, and that evidence would be obtained through the surveillance; certifying that other investigative procedures would be ineffective; and describing how the surveillance effort would be minimized. If an application met these requirements, a judge could approve the court order for thirty days with a possible extension. At the close of the surveillance, notice was to be given to the people affected, unless the judge decided to postpone the notice. Illegally obtained evidence could not be used in any official proceedings. [Regan, 1995] Yet these requirements were widely ignored in the practice of wiretapping by the FBI, with documented cases of misuse of wiretaps for forty more years.

Technological advances during the 1980s, e.g., communications transmitted over radio, microwave, satellite and fiber optics, threatened the privacy protections offered under Title III. Title III covered the "aural acquisition" of "wire and oral" communications that were carried over common carrier communications facilities. The practice of wiretapping seemed threatened, as callers could use Caller ID, Call Forwarding and other database services to escape surveillance. In response, Congress enacted the Communications Privacy Act of 1986 (ECPA), extending Title III protections and requirements to all new types of voice, data and video communications, including cellular phones, electronic mail, computer transmissions and voice pagers. [Regan, 1995]

In the case of emerging technologies law enforcement has sought to ensure the continued compliance of communications companies, sough to require the adoption of some technologies (e.g., key escrow), and taken advantage and creating their own surveillance technologies (e.g., Carnivore). In summary, the normal protections for privacy for postal communications do not hold in for electronic communications.

4 Post-Convergence Surveillance in Practice

4.1 Physical Surveillance

Today, a variety of technologies invade the privacy of millions of individuals everyday. For example, frequent shopper programs gather the buying habits of millions of consumers into a

computerized database, which may then be sold to marketing firms. Physical surveillance, e.g., electronic video and metal detectors, for security purposes is employed in many federal and state government buildings, banks, department stores and airports. Cordless phone conversations can be accidentally intercepted in a home or on a car radio. While these examples are contemporary and generally accepted by the American public, the concerns about privacy and technology are not new. [Regan, 1995; Alderman and Kennedy, 1995] Most physical surveillance techniques are accepted as public safety measures. Moreover, citizens are generally informed that the area is under surveillance and of the camera's whereabouts.

The policy debate continues when it involves the actions of the government to collect information. According to the American Civil Liberties Union (ACLU) of Florida, attendants at the Super Bowl in January 2001 were secretly photographed as they entered the stadium in Florida. The photographs were then digitized for computer comparison to criminal records in police databases. Fans were unaware that their faces were digitally captured for computer comparison to criminal records or that they could be questioned or held by law enforcement officers. The ACLU has requested public hearings regarding the surveillance and complete information of how the images were and hopefully disposed of. It is not certain what databases were used for comparison nor if the surveillance activity was authorized by sports officials. Because there was no notification of the surveillance, the ACLU is concerned that Fourth Amendment rights of those in attendance were violated.

Other high-tech surveillance devices make it possible to monitor activities inside a person's home without any physical intrusion. In the recent Supreme Court case *Kyllo v. United States*, No. 99-8508, the lawyer for an Oregon man convicted of growing marijuana in his home argued that the police engaged in an illegal search by using a thermal imager to detect the distinctive heat pattern made by the high-intensity lights that are often used for growing marijuana. The police used the information as the basis for obtaining a search warrant for the house. The issue is whether law enforcement agents violated the Fourth Amendment by failing to obtain a warrant before using the thermal imager. The attorney for the government argued that people did not have a reasonable expectation to privacy "in the heat that's on the exterior surfaces of their walls." Under court precedents, people forfeit any expectation of privacy if they conduct business in front of an open window. It would be an astonishing jump to conclude that people who fail to stop the emission of "waste" heat give up their right to privacy in their homes. [Greenspan, 2001]

Institutions and locations have long been singled out in American law for particular protection from or submission to surveillance: private homes, libraries, medical establishments, public assemblies and universities. The work factor and expense of physical surveillance has long been

the greatest constraint upon it. Constant physical surveillance will tax the resources of even the most determined regime, as the files of the East German police illustrate. These constraints are being lessened in particular by a combination of video and face recognition technologies. Video surveillance brings the previously exempt case of physical surveillance into the realm of the wiretap with the creation of ubiquitous automated surveillance. Thus, the use of such devices should also be included in any consideration of electronic surveillance.

4.2 Electronic Data Surveillance

The US government is still attempting to establish broad search privileges expand despite the gradual acceptance of a basic human right to privacy. The advancement of computer technology, specifically encryption, is proving to be a challenge to law enforcement surveillance. The response of the FBI and other law enforcement agencies since the late 1980s has been a series of programs designed to maintain its wiretapping abilities. The programs are designed to address the difficulties in maintaining electronic surveillance and to enhance their ability to monitor communications. First, in 1992 the FBI introduced the Digital Telephony Proposal, which required telephone switching equipment to include provisions that provided for authorized wiretapping. Because the FBI found it difficult to install court-authorized wiretaps due to the new switching technology, the bill mandated all telecommunications providers, both public carriers and private branch exchanges, to design systems that would assist government interceptions and to bear all the costs for redesign. [Diffie, 1998] Next, the US government tried to adopt a new federal standard for communications called Clipper. Clipper is a key-escrow system that provide user with strong cryptographic equipment to protect their privacy against most individuals but guarantees that the government has the ability to read the communications if it wished. The National Security Agency (NSA), an intelligence agency for intercepting foreign government communications and breaking their encryption codes, developed the cryptographic algorithm, known as Skipjack. [Schneier, 1997]

Both the Digital Telephony Proposal and Clipper failed to gain acceptance from industry and Congress. The underlying idea behind these two plans was to provide a "back door" for the US government to decrypt messages for the purposes of law enforcement and national security. The two proposals allowed the government to maintain its ability to wiretap to ensure a secure society. Privacy advocates, on the other hand, feared the abuse of information collection by the government. In addition, there was no independent review of the Skipjack algorithm because the NSA classified it. Businesses objected because of the difficulty of integrating the necessary hardware. Clipper also lacked marketability because it would not interest foreign customers, as the back door was only available to the US government. [Diffie, 1998; Schneier, 1997]

By 1994, the FBI modified the Digital Telephony Proposal to limit wiretapping to common carriers and apportion $500 million to cover costs. Carries would have 3 years to meet the terms and after that, a failure to perform a wiretap order could result in a heavy fine. Congress tried to accommodate the FBI's desire to maintain surveillance capabilities by passing the bill under the name Communications Assistance for Law Enforcement Act (CALEA). The telecommunications industry is not responsible for decrypting or for ensuring the government's ability to decrypt. However, they are required to assist law enforcement agencies with interception needs. Law enforcement agencies are still required to obtain court approval for wiretaps. [Diffie, 1998]

The current debate involving law enforcement electronic surveillance involves the Digital Collection System 1000 (DCS1000), formerly known as Carnivore. DCS1000 is a software system developed and introduced by the FBI in 1997 for Internet surveillance. [Kerr, 2000] The FBI's traditional investigative process of wiretapping is ill-suited for investigating electronic crimes because of the way the Internet connects thousands of systems with millions of users and crosses national boundaries. The Internet makes it very difficult to be policed by traditional means and be subjected to exact targeting. Unlike telephony systems, which generally provide only voice and low bandwidth communications services, the Internet provides a host of other forms of communications. Internet users frequently use electronic mail and electronic messaging services to communicate with one another using text instead of voice. These messages are often the targets of court-ordered interception. Some services on the World Wide Web resemble print more than they resemble a phone call. Other services, such as streaming video, resemble broadcast media, such as television. These types of communications are less-commonly the targets of court-ordered interception, but are now easily under surveillance.

A balance must be struck between employing new technologies to lawfully obtain information while providing enhanced privacy protection. This not only applies to the law enforcement community but to the private sector and the American people. The Internet is allowing everyone to gain the ability to keep close track of individual's interests. Web pages can record IP addresses and other available information. [Diffie, 1998] Users can send electronic mail on the Web that informs them when the recipient has picked up the message. Historically, the US has taken an ad hoc approach in considering surveillance. In the following section, we establish post-convergence surveillance principles, determined by examining pre-convergence surveillance and propose a coherent technology-neutral policy for law enforcement surveillance of electronic information.

5 Post-Convergence Surveillance Principles

As illustrated in the previous sections, communications are inherently subject to interception and digital technology has made ubiquitous interception ever more simple. Laws cannot change these facts but may regulate the surveillance and collection of information. [Diffie, 1998] Historically, US emphasis has been on protecting the privacy rights of individuals rather than restraining the surveillance activities of organizations. Yet, protecting individual rights does not adequately check the surveillance activities of the government and organizations.

We recognize that the needs of law enforcement agencies to intercept and collect information about the communications of criminals and about criminal activities must be balanced against expectations of communication privacy for those who are not under investigation. Any surveillance system for the Internet and other packet communications should meet the requirement for openness. This will ensure that each individual's right to privacy is protected but still allow law enforcement agencies access to information that they need. The DCS1000 system has failed the openness principle. Because it is a classified system, DCS1000 cannot be proven secure regardless of the assertions of those allowed access to the details. One possible reason for the classification of DCS100 is the fear that the system would be compromised. Public exposure, however, does not necessarily weaken a secure system. For a system to be proven secure, it must be subject to public scrutiny and peer review. Potential areas for exploitation can be reduced if the programming community can be given the opportunity to conduct tests and to search for software bugs.

Ultimately, to make good policy we must consider the sort of world in which we want to live and what effects our actions will, indeed can, have in bringing about such a world. Such considerations depends on awareness of many factors, including the technology or cryptography and electronic surveillance, the aims and practices of intelligence and law enforcement, and the history of society's attempts to deal with similar problems over more than a century. [Diffie, 1998] Concurrent with our work, the Council of Europe has been developing a policy with regards to data protection privacy and surveillance. Some of our ideas comply with the European principles, while others do not. In the development of a coherent technology-neutral policy for law enforcement surveillance of electronic information, we consider the following principles:

1. Each law enforcement agency must be accountable and subject to audit for all information in its possession.

2. The purposes for which the information is processed should be identified at the time of authorization, before the time of collection. Authorization should include a

particular type of interception regarding a particular criminal suspect, user e-mail address or account number. A finite and reasonable time period for authorization must be stated at the time of authorization and the surveillance should end or be re-authorized at the end of the stated time.

3.It should be possible to confirm, without the cooperation of law enforcement, that the collection of information in a particular case is limited to what is necessary for pursuing the identified purposes. This principle can be achieved by requesting the telecommunications carrier (or non-law enforcement body) to collect information and deliver to law enforcement only the information request by the court order. For example, the Internet Service Provider (ISP) could collect and provide the information to law enforcement.

4.Collected information should not be used or revealed for purposes other than those identified in the request for authorization. For example, if surveillance of a murder suspect indicates that the suspect may be using illegal drugs, a new investigation or charge of illegal drug use should not be allowed based on the surveillance without complete judicial review.

5.Collected information should be retained only as long as necessary. However, we do not agree with the European principle that deletion of collected data unbeknown to the individual is adequate.

6.Collected information should be accurate and up-to-date.

7.Data subjects should be informed that information has been collected even if the data is no longer necessary to the law enforcement agency. Data subjects should be allowed to access their personal information. This will help ensure that collected information is kept accurate and up-to-date. (This is currently the case with American citizens and records of the FBI.)

8.Collected information should be protected with appropriate security safeguards.

9.No secret information system or unauthorized data compilations should exist.

10.If the suspect and law enforcement are in different jurisdictions then law enforcement must meet the standards set by both jurisdictions to justify surveillance, rather than seeking the lowest common denominator

We do not agree with the European Council's belief that new technology for data surveillance and processing may be released after all measures have been taken to ensure that their planned use complies with legislation. Technology will inherently be modified in the field, if for no other reason than to ensure the functionality of the technology in a rapidly changing and heterogeneous environment. For example, new operating systems require new versions of software to maintain previous abilities. The requirement that software be upgraded, tested and patched to be continually useful precludes one-time evaluation of technologies as proposed by the European Council. Under the European Council's proposal, a complete examination of technology happens only at one moment in a quickly changing environment. Instead, we propose the guidelines listed below.

Technologies developed for surveillance purposes need to meet the following specifications:

- A clear definition of what information will be collected and what filtering or selection criteria will be used to store and/or access information that has been collected.

- A test plan should be part of the specification. Before any interception tool can be used, the results of the test plan and an analysis by an independent research organization of both the tool and its compliance with the specification must be made publicly available. This is necessary but not sufficient.

- The specification must identify and justify whether the filtering of intercepted communications may be done before or after intercepted communications are received by the law enforcement agency.

- The standard must specify where (in the network) the tool will be deployed, the type of information intercepted, and the type of information then transmitted to the law enforcement agency.

- The owner of the communications service must manage the technology whenever and wherever possible. Complete audit records from the communication carrier to law enforcement, detailing the information for future audits, should be a requirement, and not an option, for any proposed technology.

- In order to enable examination and transparency, all law enforcement surveillance software should be available for examination in source code form. This will also result in more secure and reliable code.

6 Conclusions

Ensuring the privacy of the individual in the market is not adequate for ensuring the privacy of the individual with respect to law enforcement; however, such marketplace privacy is a pre-requisite for citizen privacy. The European principles for data protection and surveillance offer the beginning of a foundation on which to build technology-neutral standards for surveillance; although given the uniquely and necessarily intrusive nature of law enforcement surveillance, the principles are not entirely suitable.

It is understood that surveillance is a high priority in the law enforcement community. Policymakers need to take a broader view in examining this issue and creating legislation that serves the interests of the nation. Policy initiatives involving telecommunications surveillance need to have a solid understanding of the technologies involved. The targeting of specific individuals should not infringe upon the privacy rights of other users on the telecommunications network. Privacy must be afforded especially to those who are not themselves the subject of investigation, but whose communications might happen to have been intercepted incidentally. If technologies are to be developed for the purpose of surveillance, then open source development should be aggressively encouraged.

Policies need to be technology-neutral in order to withstand the further evolution of telecommunications technologies and services. In particular, we argue that the telecommunications industry assist law enforcement agencies in their interception needs instead of the government implementing their own surveillance techniques. For example, the ISPs would provide filtered - not raw - information to law enforcement, as telephone companies do in response to court orders for telephone taps. Such a practice will create a window of transparency whereby law enforcement requests for communications are documented and the transfer of data can be observed. The increasingly private nature of networks offers promise that an increasing transparency of dataflow to law enforcement is possible. However, the European Council proposal would lead to ineffective one-time analysis of dynamic surveillance technologies and a loss of privacy rights as the lowest common denominator is adopted across jurisdictions. As seen in the United States, while powerful individual leadership may create high privacy levels during times of transition, clear and comprehensive policies are needed to prevent later crises and concerns from overriding initial privacy protection.

References

ACLU calls for public hearings on Tampa's "snooper bowl" video surveillance. (February 1, 2001), online at http://www.aclu.org/news/2001/n0d0101a.html accessed 04.03.2001.

Alderman, E. and Kennedy, C. (1995), The right to privacy, Alfred A Knopf, New York, NY.

Agre, Philip E. and Marc Rotenberg. (1997), Technology and privacy: the new landscape, The MIT Press.

Beisel, N., (1997), Imperiled innocents: Anthony Comstock and family reproduction in Victorian America, Princeton University Press.

Bennett, Colin J. and Rebecca Grant. (eds.) (1999), Visions of privacy: policy choices for the digital age, University of Toronto Press, Inc.

Bray, Hiawatha. (February 10, 2001), Chinese lose link to net as cable fails undersea outage cuts off foreign web sites; cause still unclear, The Boston Globe, C1.

L. Jean Camp (2000) Trust & Risk in Internet Commerce, MIT Press, Winter (Cambridge, MA).

Cohen, J., (1996), A right to right to read anonymously: a closer look at copyright management in Cyberspace, 28, *Conn. L. Rev*. 981

Diffie, Whitfield. and Susan Landau. (1998), Privacy on the line: the politics of wiretapping and encryption, The MIT Press.

Greenhouse, Linda. (February 21, 2001), Heat-seeker's ability to pierce the home comes under Supreme Court's scrutiny, The New York Times, A17.

Kahn, David (1996) *The Codebreakers*, Scribner; NY, NY.

Kerr, Donald M. (September 6, 2000), Carnivore diagnostic tool, Congressional Statement Federal Bureau of Investigation.

Regan, Priscilla M. (1995), Legislating privacy: technology, social values, and public policy, The University of North Carolina Press.

Schneier, Bruce. and David Banisar (1997), The electronic privacy papers: documents on the battle for privacy in the age of surveillance, John Wiley & Sons, Inc.

Schement, Jorge Reina and Terry (1995) Tendencies and Tensions of the Information Age, New Brunswick: Transaction Publishers.