

Testimony of Deirdre Mulligan

by [Deirdre Mulligan](#) [1]

March 26, 1998

Speaker: Deirdre Mulligan

**Testimony of Deirdre Mulligan,
Staff Counsel, Center for Democracy and Technology
to the
House Committee on the Judiciary
Subcommittee on Courts and Intellectual Property
March 26, 1998**

I. Introduction And Summary

The Center for Democracy and Technology (CDT) is pleased to have this opportunity to testify on the issue of privacy protection in the online environment.

CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet. One of our core goals is to enhance privacy protections for individuals in the development and use of new communications technologies.

To focus my testimony this morning, I will begin by outlining five trends in technology with ramifications for the existing framework of privacy protections in electronic communications. The current mix of legal and self-regulatory protections for privacy has not kept pace with technology and its growing role in society. The core of my testimony is a series of policy recommendations:

- identifying areas in which Congress should enhance existing privacy protections;
- recommending the creation of an institutional structure for addressing privacy concerns in a proactive and ongoing manner; and,
- urging the US government (and others) to engage in several non-traditional methods of developing and implementing privacy policy that are of particular relevance to the global, decentralized networks that comprise our communications infrastructure.

It is critically important to ensure that privacy protections keep pace with changes in technology. This requires a periodic assessment of whether changes in technology pose new threats to privacy that must be addressed through changes in law. Many of our existing laws were constructed to meet dual purposes, such as protecting privacy and meeting legitimate law enforcement needs, or protecting privacy and promoting the cost-effective operation of the health care system. We must examine whether they continue to set the bounds of permissible government and private sector action in a fashion consistent with privacy protection. In addition, we should evaluate whether technology itself can be used to advance privacy in this new environment. Finally, the globalization of the communications system requires us to consider alternative methods for achieving policy goals, be they self-regulation or international agreements.

II. Technology Trends with Ramifications for Individual Privacy in Electronic Communications

B. The transactional data generated through the use of new technologies is a rich source of information about individuals' habits of association, speech, and commercial activities. This vast new data is essential to the operation of the packet-switching medium and provides the raw material for many of the unique functions the Internet offers, yet it poses significant privacy concerns. Interactive media generate, capture and store a tremendous amount of information. At the same time the flexibility of new media is blurring the distinction between the content of a communication and the transactional data used to route the message to its destination. Transactional data in this new media is more detailed, descriptive, and identifying than ever before. Aggregated, it is capable of revealing as much about the individual as the content of a message.

C. The globalization of communications technology is eroding national borders. Governments are finding it increasingly difficult to enforce laws -- be they laws to protect or repress their citizens. The fluidity of borders on the Internet promises to promote pluralism, the free flow of information and ideas, diverse associations, and, we hope, democracy. On the other hand, enforceable, workable privacy protections for the global information infrastructure have yet to emerge leaving individuals' communications and personal data vulnerable.

D. The lack of centralized control mechanisms. The distributed nature of the Internet's infrastructure distinguishes it, at least in degree, from existing communications systems. Its decentralized nature allows it to cope with problems and failures in any given computer network by simply routing information along alternate paths. This makes the Internet quite robust. However, the lack of centralized control mechanisms may frustrate those seeking to regulate activities on the network. Decentralized systems are inherently less secure. They pose new challenges to protecting data during storage and transmission.

E. Decrease in computing costs and the focus on client-side controls over network interactions present new opportunities to empower individuals. The Internet continues to shift control over interactions away from the government and large private sector companies. The ability to build privacy protections into the users interface with the network offers the opportunity to craft privacy protections that shield individuals regardless of the jurisdictional law and policy. Providing individuals with technical means to control and secure their communications and personal information may pave the way for privacy protections that are as decentralized and ubiquitous as the networks themselves.

A. The explosive growth of the Internet is transforming our methods of communicating and methods of gathering, processing and sharing information and knowledge. In 1986, when Congress updated the communications privacy laws, the Internet was comprised of approximately 50,000 computers. Today the Internet is comprised of upwards of 20 million Internet host computers globally and estimates on individual users hover around 100 million people worldwide. Unlike traditional media, the Internet supports interactions ranging from banking to dating, from one to one communications, town hall meetings, political events, to commercial transactions.

III. Policies from the Pre-network World

Current policies protecting individual privacy in electronic communications are built upon Fourth Amendment principles designed to protect citizens from government intrusion. While premised on Fourth Amendment concepts, the contours of existing statutory protections are also a product of the technical and social "givens" of specific moments in history. Some of these historical givens have

changed dramatically, with implications for the effectiveness and relevance of existing statutory protections for privacy.

Crafting proper privacy protections in the electronic realm has always been a complex endeavor. It requires a keen awareness of not only changes in technology, but also changes in how the technology is used by citizens, and how those changes are pushing at the edges of existing laws. From time to time these changes require us to reexamine our fabric of privacy protections. The issues raised below indicate that it is time for such a review.

In response to Supreme Court decisions finding that electronic surveillance was a search and seizure covered by the 4th Amendment and law enforcement's arguments that it was a needed weapon against organized crime, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The wiretap provisions of Title III authorized law enforcement wiretapping of telephones within a framework designed to protect privacy and compensate for the uniquely intrusive aspects of electronic surveillance.

In brief, the legislation Congress enacted in 1968 had the following components: the content of wire communications could be seized by the government in criminal cases pursuant to a court order issued upon a finding of probable cause; wiretapping would be otherwise outlawed; wiretapping would be permitted only for specified crimes; it would be authorized only as a last resort, when other investigative techniques would not work; surveillance would be carried out in such a way as to "minimize" the interception of innocent conversations; notice would be provided after the investigation had been concluded; and there would be an opportunity prior to introduction of the evidence at any trial for an adversarial challenge to both the adequacy of the probable cause and the conduct of the wiretap. "Minimization" was deemed essential to satisfy the Fourth Amendment's particularity requirement, compensating for the fact that law enforcement was receiving all of the target's communications, including those that were not evidence of a crime. The showing of a special need, in the form of a lack of other reasonable means to obtain the information, was viewed as justification for the failure to provide advance or contemporaneous notice of the search.

Due to privacy considerations arising from changes in technology, primarily the advent of wireless services and the growing use of email, in 1986 Congress adopted the Electronic Communications Privacy Act (ECPA). Congress' action was in part spurred by the recognition that individuals would be reluctant to use new technologies unless privacy protections were in place.

ECPA did recognize the importance of transactional data. ECPA set forth rules for the use of pen registers and trap and trace devices, which capture out-going and incoming phone numbers respectively. It also established rules for law enforcement access to information identifying subscribers of electronic communication services. For transactional information relating to e-mail ECPA requires a warrant, for other transactional data it requires a court order, a mere subpoena, or consent.

To a large degree ECPA extended the Title III protections to the interception of wireless voice communications and to non-voice electronic communications such as fax and email while in transit. However, ECPA did not extend all of Title III's protections to electronic communications. Unlike Title III, which limits the use of wiretaps to a limited list of crimes, court orders authorizing interceptions of electronic communications can be based upon the violation of any federal felony. While constitutional challenges to the introduction of information obtained in violation of ECPA may succeed, ECPA contains no statutory exclusionary rule as Title III does.

Moreover, Congress set very different rules for access to electronic communications while they are in storage incident to transmission. When the government goes to AOL or another service provider and asks it to provide a copy of a person's email messages from the AOL server where they sit waiting to be read, an ordinary search warrant is enough without the special protections of minimization, judicial supervision and notice to the individual found in Title III.

B. Assumptions of the existing framework

In drafting ECPA Congress began the process of dealing with fundamental changes in technology. They recognized that transactional data needed privacy protections. However, the framework of Title III and the advances of ECPA did not envision the World Wide Web and the pervasive role technology would come to play in our daily lives. Underlying Title III and ECPA were a number of assumptions about both the nature and the use of electronic communications:

A. From phones to email: The existing framework

- 0. The transmission of private communications and records stored with third parties, including records of such communications, raise different privacy considerations.
- 0. The majority of electronic communications are by nature ephemeral.
- 0. The private sphere of personal communications and interactions would be located at the end-points, not in the medium itself.
- 0. The government's collection and use of information about individuals' activities and communications is the greatest threat to individual privacy.
- 0. Transactional data is not rich in intimate, personal detail.

Congress has only begun to wrestle with the fact that some of these assumptions, while perhaps accurate at one point in history, have changed dramatically since the initial framework for protecting electronic communications was articulated in 1986. Congress took a first small step towards recognizing the changing nature of transactional data in the networked environment with amendments to ECPA enacted as part of the Communications Assistance for Law Enforcement Act of 1994 (CALEA). The 1994 Amendments recognized that transactional data was emerging as a hybrid form of data, somewhere between addressing information and content, and was becoming increasingly revealing of personal patterns of association. For example, addressing information was no longer just a number and name, but contained the subject under discussion and information about the individual's location. Therefore, Congress raised the legal bar for government access to transactional data by eliminating subpoena access and requiring a court order, albeit one issued on a lower relevance standard. Some issues were left unanswered, and new ones continue to arise as communications technology advance.

IV. Four Examples Reveal the Current Weaknesses of Existing Statutory Protections for Privacy in light of the Shifts in Electronic Communications Technology and its Use in Society.

Individuals traditionally kept their diaries under their mattress, in the bottom drawer of their dresser or at their writing table. Situated within the four walls of the home these private papers are protected by the Fourth Amendment. With the advent of home computers individual diaries moved to the desktop and the hard-drive. Writers, poets, and average citizens quickly took advantage of computers to manage and transcribe their important records and thoughts. Similarly, pictures moved from the photo album to the CD-ROM.

Today, network computing allows individuals to rent space outside their home to store personal files and personal World Wide Web pages. The information has remained the same. A diary is a diary is a diary. But storing those personal thoughts and reflections on a remote server eliminates many of the privacy protections they were afforded when they were under the bed or on the hard-drive. Rather than the Fourth Amendment protections -- including a warrant based on probable cause, judicial oversight, and notice -- the individual's recorded thoughts may be obtained from the service provider through a mere court order with no notice to the individual at all.

B. Medical records in cyberspace

To bring home what this means in a business setting lets look at medical records. Hospitals, their affiliated clinics and physicians are using intranets to enable the sharing of patient, clinical, financial, and administrative data. Built on Internet technologies and protocols, the private networks link the hospital's information system, to pharmacy and laboratory systems, transcription systems, doctors and clinic offices and others. The U.S. government is contemplating the development of a federal governmentwide computer-based patient record system. According to news reports, the Internet and World Wide Web-based interfaces are under consideration. The private sector is moving to integrate network computing into the a sensitive area of our lives -- the doctors office.

As computing comes to medicine, the detailed records of individuals' health continue to move not just out of our homes, but out of our doctors offices. While the use of network technology promises to bring information to the fingertips of medical providers when they need it most, and greatly ease billing, prescription refills, and insurance pre-authorizations, it raises privacy concerns.

In the absence of comprehensive federal legislation to protect patient privacy, the protections afforded by ECPA and other statutes are of utmost importance. Unfortunately, the protections afforded to patient data may vary greatly depending upon how the network is structured, where data is stored, and how long it is kept. If records are housed on the computer of an individual doctor then access to that data will be governed by the Fourth Amendment. Law enforcement would be required to serve the doctor with a warrant or subpoena and the doctor would receive notice and have the chance to halt an inappropriate search. Under federal law, the patient however, would receive no notice and have no opportunity to contest the production of the records. When information is in transit between a doctor and a hospital through a network, law enforcement's access is governed by the warrant requirements of ECPA, and neither doctor nor patient receive prior or contemporaneous notice. If the records are stored on a server leased from a service provider the protections are unclear. They may be accessible by mere subpoena. If they are covered by the "remote computing" provisions of ECPA this would severely undermine privacy in the digital age.

In addition to concerns about government access to personal health information, recent news stories have focused the public on the misuse of personal health information by the private sector -- particularly when its digitized, stored and manipulated. Recently the Washington Post reported that CVS drug stores and Giant Food were disclosing patient prescription records to a direct mail and pharmaceutical company. The company was using the information to track customers who failed to refill prescriptions -- sending them notices encouraging them to refill and to consider other treatments. Due to public outrage -- and perhaps the concern expressed by Senators crafting legislation on the issue of health privacy -- CVS and Giant agreed to halt the marketing disclosures. But the sale and disclosure of personal health information is big business. In a recent advertisement Patient Direct Metromail advertised that it had 7.6 million names of people suffering from allergies, 945,000 suffering from bladder-control problems, and 558,000 suffering from yeast infections.

The sale and disclosure of what many perceive as less sensitive information is also raising privacy concerns. This past summer AOL announced plans to disclose its subscribers telephone numbers to business partners for telemarketing. AOL heard loud objections from subscribers and advocates opposed to this unilateral change in the "terms of service agreement" covering the use and disclosure of personal information. In response, AOL decided not to follow through with its proposal.

As we move forward we must ask, will personal records be afforded differing levels of privacy protection merely because of where and how they are stored? Will individuals be the arbiters of their own privacy, able to make decisions about who knows what about them? How will individual privacy be protected in interactions in the private sector.

C. The case of Timothy R. McVeigh

In January news stories broke about a highly decorated seventeen-year veteran of the U.S. Navy who was to be discharged based on information obtained by the Navy from America Online. The facts surrounding the incident raise many concerns with privacy in the online world. Using an AOL

screenname "boysrch," Timothy McVeigh sent an email to a civilian Navy volunteer. The curious volunteer looked up the screenname in AOL's member profile directory and discovered that the subscriber identified himself as "Tim, from Honolulu, Hawaii, employed by the military, and gay." The volunteer passed the screen name and profile information on to her husband, a Navy officer. It eventually landed in the hands of the Judge Advocate General who undertook an investigation. A Navy paralegal called AOL's customer service and asked for information about the subscriber belonging to the screenname "boysrch." AOL identified Timothy R. McVeigh as the subscriber.

According to the administrative separation proceedings, the Navy paralegal had not obtained a warrant, a court order, a subpoena, or Timothy McVeigh's consent prior to contacting AOL, and was therefore in violation of ECPA. In its statement arguing against Timothy McVeigh's request for an injunction, the Navy stated that ECPA puts the obligation on AOL to withhold information, not on the government to follow appropriate procedures. Equally troubling is the fact that because the statute penalizes only "knowing or intentional" violations, it is unclear whether a cause of action will succeed for this violation of privacy and ECPA.

This case illustrates a number of weaknesses of ECPA. ECPA limits the disclosure of information to the government but allows online service providers and others to disclose information, other than the contents of communications, about subscribers to other parties. Is the disclosure of information to the Navy, or more generally the government, an individual's only privacy concern? We can certainly imagine scenarios in which information tying a screenname, and possibly online activities, to an individual's real world identity would substantially invade an individual's privacy and potentially enable further harm to befall him. Of specific concern would be the disclosure of information about children in such a setting. While the government's access to this information, and subsequent actions based upon it, are the source of harm in the McVeigh incident, it is quite possible to imagine a situation equally troubling involving the disclosure of such information to a private party.

A second troubling aspect of ECPA revealed by the McVeigh case is that the lack of a statutory exclusionary rule coupled with penalties that only focus on intentional violations do not create incentives for parties to effectively implement its requirements. In the McVeigh case ECPA itself may not limit the use of the illegally obtained information. While the Constitution may, the lack of a statutory exclusionary rule undermines the goal of assuring that the government follow appropriate procedures designed to protect privacy at the front-end. Similarly, the existing penalty structure set out in ECPA does not encourage proactive behavior to protect privacy. In the incident involving McVeigh, AOL claimed that they did not know they were providing information to a government agent, and therefore under the existing statutory penalties they may not be liable.

D. We know where you are and what you're doing.

An example of the power of transactional data comes from the "location" information available through many cellular networks. In the course of processing calls, many wireless communications systems collect information about the cell site (location) of the person making or receiving a call. Location information can be useful, as Ted Rappaport, the inventor of the hand-held cell phone locator, stated, "If you could know accurately where things are, not only would you feel safer because emergency services could find you, but law enforcement could use it more easily to track the bad guys." But as one reporter put it, "Cellular telephones, long associated with untethered freedom, are becoming silent leashes..." The technology is proceeding in the direction of providing more precise location information, a trend that has been boosted by the rulings of the Federal Communications Commission in its "E911" (enhanced 911) proceeding, which requires service providers to develop a locator capability for medical emergency and rescue purposes. Location information may be captured when the phone is merely on, even if it is not handling a call. Private sector uses of this information are also under consideration. A company in Japan is experimenting with a World Wide Web site that allows anyone to locate a phone and the person carrying it by merely typing in the phone number.

In the online environment, transactional data can do more than just track the individual's location. It can provide insight into their thoughts, their affiliations, and their politics. It can reveal whether they are at home or at work. In a world where transactional data captures the full contours of a person's life it is time to provide it with stronger privacy protections.

A. Personal papers in cyberspace

V. Recommendations

As we consider privacy in the changing communications environment we must ask whether the assumptions of a previous time and technology, and legal distinctions based upon them, continue to make logical sense. Or more importantly, whether they provide protections reflective of our commitment to individual privacy autonomy, dignity, and freedom. Policies designed to implement the Fourth Amendment developed in a 20th century world of paper records -- even as extended to protect transient voice communications -- may not be applicable to 21st century technologies where many of our most important records are not "papers" in our "houses" but "bytes" stored electronically and our communications rather than disappearing into thin air are captured and stored at distant "virtual" locations for indefinite periods of time.

To address privacy in the electronic communications environment the Congress should:

Reexamine the need for limits on the disclosure and use of personal information by private entities. Both the Federal Trade Commission and the Department of Commerce are engaged in initiatives designed to promote "fair information practice principles" in the online environment. We are encouraged that Congress is exploring protections for individual privacy during private sector activities. In considering this issue we recommend that discussions focus on the Code of Fair Information Practices developed by the Department of Health, Education and Welfare (HEW) in 1973 and the Guidelines for the Protection of Privacy and Transborder flows of Personal Data, adopted by the Council of the Organization for Economic Cooperation and Development in 1980.

Reconsider how the lines have been drawn between records entitled to full Fourth Amendment protection and business records that fall outside the protection of the Fourth Amendment. There are now essentially four legal regimes for access to electronic data: (i) the traditional Fourth Amendment standard, for records stored on an individual's hard drive or floppy disks; (ii) the Title III-ECPA standard, for records in transmission; (iii) the business records held by third-parties, available on a mere subpoena with no notice to the individual subject of the record; and, (iv) a third, the scope of which is probably unclear, for records stored on a remote server, such as the research paper (or the diary) of a student stored on a university server or the records (including the personal correspondence) of an employee stored on the server of the employer. As the third and fourth categories of records expand because people find it more convenient to store records remotely, the legal ambiguity and lack of strong protection grows more significant and poses grave threats to privacy in the digital environment.

Heighten the standard for access to transactional data. Transactional data are in many ways a person's digital fingerprints, although far more easily captured. Transactional records provide unprecedented information about the places, people, and activities that comprise the individual's daily life.

Create a privacy entity to provide expertise and institutional memory, a forum for research and exploration, and a source for guidance and policy recommendations on privacy issues. The existing crisis-driven approach to responding to privacy concerns has hindered the development of sound rational policy and failed to keep pace with changes in technology. The US needs an independent voice empowered with the scope, expertise, and authority to guide public policy. Such an entity has important roles to play on both the domestic and international fronts. Without an independent voice, privacy rights in the United States will not be afforded adequate consideration and protection in emerging media.

Encourage the development and implementation of technologies that support privacy on global information networks. Technological mechanisms for protecting privacy are critically important on

the Internet and other global medium. Developing meaningful privacy protections in the online environment requires us to realize that our laws and Constitutional protections may not follow our citizens, their communications, or their data as it travels through distant lands. Technology can provide protections regardless of the legal environment.

Strong encryption is the backbone of technological protections for privacy. Today technical tools are available to send anonymous email, browse the World Wide Web anonymously, and purchase goods with the anonymity of cash. The World Wide Web Consortium's Platform for Privacy Preferences, currently under development, will provide an underlying framework for privacy -- allowing Web sites to make their information practices available to visitors and individuals to set privacy rules that control the flow of data during interactions with Web sites. This effort has involved non-profit, for-profit and government representatives.

The U.S. should encourage the development of privacy-enhancing technologies that address the need either to eliminate data collection, or where data collection occurs: to limit the data collected; to communicate data practices; and, to facilitate individualized decision-making where consistent with policy.

Collaborate with other governments, the public interest community and the business community to develop global solutions for the decentralized network communications environment. Traditional top down methods of implementing policy and controlling behavior, be they international agreements, national legislation, or sectoral codes of conduct enforced by the private sector, offer incomplete responses to the privacy issues arising on the global information infrastructure. Implementing privacy policy in the decentralized, global and borderless environs of international networks raises difficult questions of effectiveness and enforcement. The U.S. should work with all parties -- other governments, international bodies, the public interest and for-profit communities to build consensus on appropriate policy. Providing a seamless web of privacy protection to individuals' data and communications as it flows along this international network may require new tools -- legal, policy, technical and self-regulatory -- for implementing policy. The U.S. should actively participate in their crafting.

Thank you for the opportunity to participate in this important discussion about protecting privacy in the online environment.

~~The copyright © 2003 by the Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).~~

Source URL: <https://cdt.org/testimony/testimony-deirdre-mulligan-7>

Links:

[1] <https://cdt.org/personnel/deirdre-mulligan>