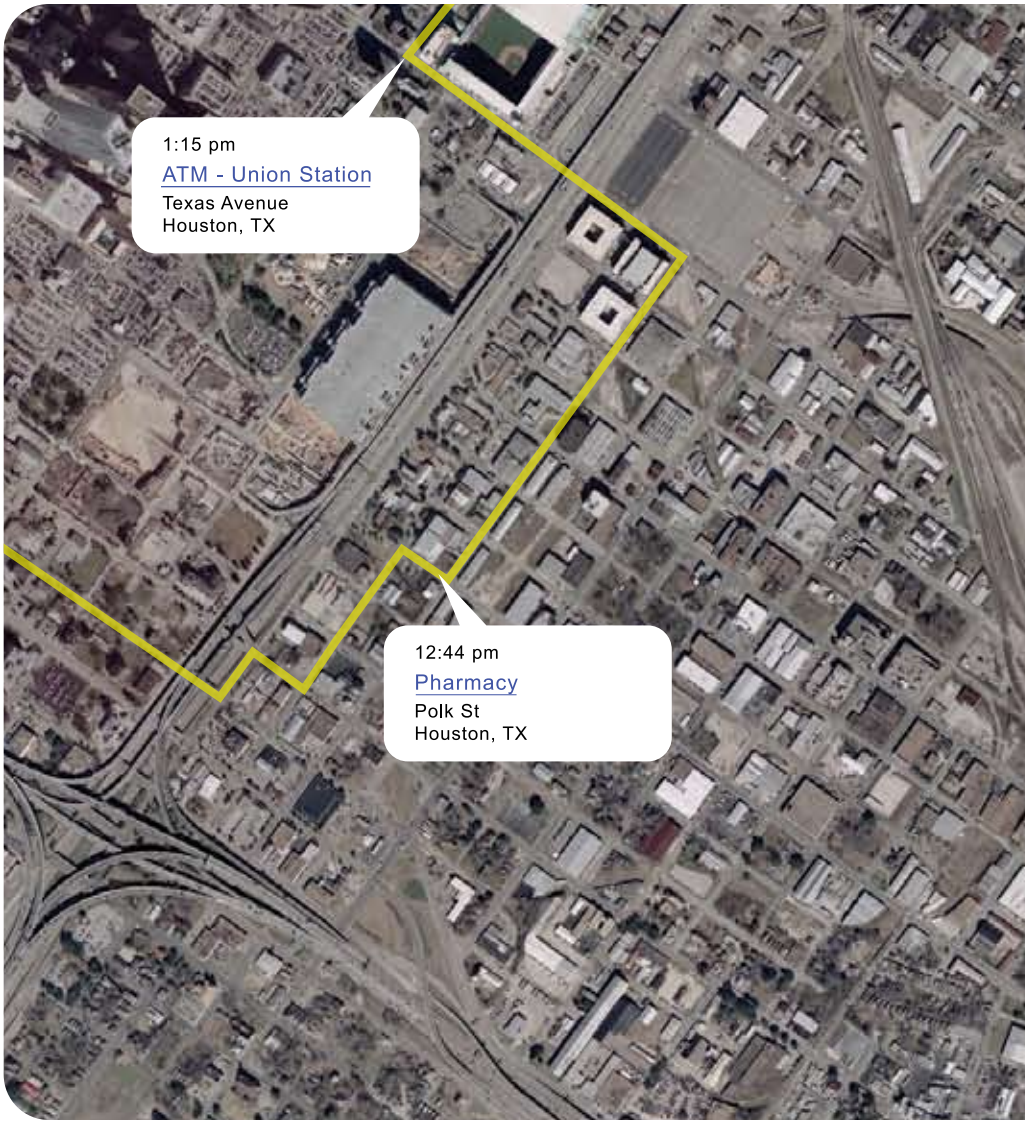
Digital Search & Seizure:

Updating Privacy Protections to Keep Pace with Technology



CENTER FOR
DEMOCRACY
&
TECHNOLOGY

The Center for Democracy and Technology is a non-profit, non-partisan public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet.

This report was researched, written and produced with the generous support of the John D. and Catherine T. MacArthur Foundation, the Open Society Institute, and other CDT supporters.

Ari Schwartz, Lara Flint, Prof. Deirdre Mulligan (Boalt Hall, University of California, Berkeley), Gemma Suh, Indrani Mondal and James X. Dempsey researched and wrote this report. Ben Karpf provided additional research assistance.

1634 I Street, NW

Washington, DC 20006

(202) 637-9800

(202) 637-0968 (fax)

www.cdt.org

Digital Search & Seizure:

Updating Privacy Protections to Keep Pace with Technology

February 2006

Information and communications technologies are changing so rapidly that they are outpacing the law's privacy protections. Services like online storage of email and location capabilities built into cell phones offer tremendous convenience but also generate large amounts of data revealing our thoughts, associations and whereabouts. Personal information held by service providers is accessible to the government under weak standards based on outdated Supreme Court decisions. The major federal law on surveillance was written in 1986, before the World Wide Web even existed. Courts and Congress should respond. The Internet and communications industry, public interest organizations and the government need to enter into a dialogue aimed at ensuring that the fundamental right of privacy is protected in the face of technological change.

Table of Contents

Introduction

Every day, Americans use the Internet and wireless services to access, transfer and store vast amounts of private data. Financial statements, medical records, travel itineraries, and photos of our families – once kept on paper and secure in a home or office – are now stored on networks. Electronic mail, online reading and shopping habits, business transactions, Web surfing and geo-location data constitute detailed personal profiles. More and more of our lives are conducted online and more and more personal information is transmitted and stored electronically.

Consider the following ways in which information and communications technologies have changed in the past 20 years:

- Both cellular phones and the Internet have become ubiquitous in our daily lives, fundamentally altering the way we work and interact and yielding many benefits, but also generating in the hands of service providers comprehensive records of commercial, associational and expressive activity.
- Among other things, cell phones can serve as location tracking devices. Automobiles also increasingly have geo-location features.
- The broadband Internet is becoming a mass medium for access to a wide range of information, including news, entertainment, and commerce. As text, audio, and video converge on this single platform, and citizens obtain publications, movies, and radio and TV programs online, the Internet also affords monitoring capabilities not available with traditional broadcast or print media.
- Miniature radio frequency identification tags are being designed for consumer products and will be linked to computer networks.
- As the cost of data storage has plummeted, more and more email and other personal information is being stored on networks, outside the home or office, accessible from any Internet device.

We benefit from the convenience, efficiency, and access to information these technologies facilitate. They offer huge benefits for democratic participation and human development as well as economic opportunities. Yet these advances also create new privacy challenges, for they make possible more intrusive surveillance. Government agencies have taken note and are both relying on the surveillance potential of consumer products and leveraging digital technologies to develop new surveillance and data analysis capabilities of their own. Of course, the government has valid, sometimes compelling, needs to collect digital information. With the nation facing a continuing threat of terrorism, these needs sometimes are urgent. But the presence of even compelling need does not obviate the questions of how, when, for how long and under what authority. In a democratic society, those are often the most important questions about governmental power, yet increasingly the standards for government surveillance provide inadequate protection against erroneous, unjustified or overbroad surveillance.

Privacy is an important constitutional value and a crucial component of the trust necessary for the flourishing of digital commerce and democracy. However, while technology has changed dramatically in the past twenty years, privacy law has not. Much of the recent debate about government surveillance has centered around the PATRIOT Act, but the changes in law wrought by that legislation are minor in comparison to the changes being brought about by technological change. The Electronic Communications Privacy Act (ECPA) of 1986 set an important precedent, establishing privacy rules for major new technologies that were emerging in the 1980s. But opportunities for government surveillance have continued to expand in ways not contemplated when ECPA and other privacy laws were written. Constitutional interpretations issued by the Supreme Court before the Internet was invented, if read broadly, would leave much electronic data outside the coverage of the Fourth Amendment's privacy protections. Court cases grappling with the new technology so far have been few in number and inconclusive in their holdings, providing few clear limitations on government surveillance and insufficient guidance to service providers.

A host of technological trends merit policy attention, including the growth of commercial data aggregators, advancements in DNA profiling, the deployment of radio frequency identification (RFID) devices, and the wider use of biometric identification. In this report, we examine in depth three developments:

1. Personal information that people used to keep in paper files or on computer hard-drives is in-

creasingly stored online, beyond the physical confines of the home or office;

2. Cell phones, car navigation services and other communications devices can provide precise location information; and
3. Programs known as "keystroke loggers" can record all information typed into a computer and can be installed surreptitiously, even remotely.

All three technologies receive inadequate attention under the current framework for privacy protection.

In his new book, "Active Liberty," Supreme Court Justice Stephen Breyer comments on the way in which technology has outpaced privacy protections. As a response to this condition, Justice Breyer concludes: "Serious complex legal change is often made in the context of a national conversation involving, among others, scientists, engineers, businessmen and women, the media, along with legislators, judges, and many ordinary citizens whose lives the new technology will affect. That conversation takes place through meetings, symposia, and discussions, through journal articles and media reports, through administrative and legislative hearings, and though court cases."

We agree that it is time for a broad-based dialogue about the ways in which technology is undermining traditional privacy expectations. Technology companies should be aware of the issues so they can design products and services in ways that promote privacy and user control. The courts should reexamine the assumptions on which Fourth Amendment interpretations have been based and should be more careful in approving government surveillance requests. And Congress should update statutory protections to ensure that the principles that govern traditional surveillance techniques continue to apply to new technologies. Just as Congress in 1968 permitted the use of wiretaps only if approved by a judge, and just as Congress in 1986 extended protections to email and wireless communications, Congress should ensure that new surveillance technologies are subject to appropriate standards.

As this report was being finalized, the President admitted that he had been, and would continue, authorizing the National Security Agency to carry out electronic surveillance inside the United States without the court orders required by the Foreign Intelligence Surveillance Act. The NSA has been described as the largest eavesdropping agency in the world. Its satellite dishes and other collection techniques are capable of scooping up billions of communications. When FISA was adopted in 1978, an international telephone call was a rarity for an ordinary person in the U.S. and email was non-existent. Now, many of the activities of daily life are reflected in electronic communications. Even small businesses are global, tens of millions of Americans have relatives or business associates abroad with whom they communicate regularly, and much of the world's email and Internet traffic moves through the U.S. All of this data lies potentially exposed to the NSA, whose computer processing power has surely grown by many factors.

Government officials often argue that changing technology requires new powers to combat sophisticated terrorists and other criminals. Sometimes that is true, but the American people also need new protections to ensure that technological changes do not result in an unjustified loss of privacy. This report discusses proposals for updating our privacy laws to permit government surveillance where appropriate while also ensuring that innocent people do not lose their privacy simply because existing law did not anticipate technological advances.

Advances in technology have outpaced the law, leaving privacy inadequately protected against government intrusion.

Chapter I

Storing Our Lives Online:

Expanded Email Storage Raises Complex Policy Issues

Internet Service Providers (ISPs) and other online service providers are increasingly offering their customers the ability to store, on the service providers' computers, very large quantities of email. Additional online storage services include Web-posting of photographs and online calendars that enable information sharing with friends and colleagues. These services provide volumes of storage capacity that were unimaginable twenty years ago. This free or low-cost storage offers Internet users the convenience of access to their email, documents and photographs from any Internet-connected computer in the world. However, it also has unintended consequences for personal privacy. Current privacy protections were shaped when consumer use of such remote storage was rare.

In terms of how they use and disclose customer information, leading service providers promise consumers relatively strong protections in their privacy policies and adhere to those promises. However, privacy policies have exceptions for government demands, and the rules for government access raise major concerns.

For this chapter, we reviewed existing rules governing stored electronic communications and data, and we examined the storage practices and disclosure policies of some of the most well known ISPs. Most importantly, we found that –

- Supreme Court cases of two decades ago, if broadly read, would leave much stored data outside the protection of the Constitution's Fourth Amendment; and
- The major statute setting rules for government access to email, the Electronic Communications Privacy Act (ECPA), no longer offers adequate privacy protections, given changes in the way people today use their email accounts and Internet storage.

In terms of the privacy practices of service providers, we found that online service providers address many privacy issues associated with storage through their terms of service and privacy policies. While there are legal gaps in what ISPs could do with the communications and other information stored by their customers, leading service providers promise consumers relatively strong protections and adhere to them. We did find that it is sometimes hard to determine what a specific provider's policy is, especially with respect to deletion of mail from inactive accounts or deletion of older mail from active accounts. We also found that, since ISPs retain data for varying lengths of time, and do not always delete email immediately upon request, customers may not be aware of whether their email is still stored and thus susceptible to disclosure. Finally, due to service providers' concerns about privacy, next-of-kin may encounter difficulties in retrieving important information held in a deceased user's account. In these non-governmental contexts, we conclude that the best approach to dealing with the privacy issues posed by increased online storage is a mix of consumer education, clear ISP policies, and perhaps some updates to pertinent privacy laws.

However, we found major concerns with the rules for government access. When it comes to government demands, the best service provider privacy policy in the world yields to a warrant or perhaps even a mere subpoena, often without notice to the customer that her personal documents are being disclosed. We conclude that, given the rapid onset of the storage revolution, consumer expectations are likely out of line with the realities of online privacy protection. In the new environment of massive storage capacity, policy reform is needed.

THE STORAGE REVOLUTION

As the Internet has moved into schools, homes, and offices, email has become a primary medium of communication and the Web has become an important means of storing and retrieving information. Unlike telephone calls, emails can be easily saved for future reference. Moreover, unlike telephone calls and traditional mail, copies of email can be stored with the service provider. Until recently, this potential of third party storage was largely unrealized; the primary means of storing older email was on one's desktop computer, after download. Due in part to cost considerations, providers of free online services used to offer their customers the ability to store only a relatively small amount of email on the service provider's computer.

However, innovations in storage technology have enabled the retention of much larger amounts of data at lower costs. As the National Institute for Standards and Technology has pointed out, the nation's digital storage industry—makers of the tapes, disks, and other gear that have become the archives and the retrieval tools of the information age—has been doubling storage capacity about every 18 months. The era of magnetic disk storage dawned in 1956 with the IBM 350 disk file; it consisted of 50 platters with a capacity of 5 megabytes.[1] In 1998, the IBM Deskstar hard drive had a 25-gigabyte capacity, which was approximately 5000 times the capacity of the first drive.[2] By 2004,

[1] See "Computer History Timeline," at www.computerhistory.org/timeline/.

[2] See "History of IBM", at www-03.ibm.com/ibm/history/history/year_1998.html.

the Hitachi Deskstar 7K250 PC hard drive stored 250 gigabytes on three 3.5-inch diameter platters.[3] The trend has been accompanied by rapidly falling prices. According to one estimate, 1 gigabyte worth of magnetic disk storage capacity cost $8.37 in 2000 and was expected to cost $0.42 by 2005 and less than a penny by 2013.[4]

In April 2004, Google started to beta-test its "Gmail" system, at first providing users with one gigabyte of storage space for free. This represented 500 times the amount of the equivalent MSN/Hotmail account at the time.[5] In response to the "Gmail" offering, Yahoo! announced that it would increase free customer storage space to 100 megabytes and that paid customers would receive two gigabytes.[6] MSN/Hotmail followed, declaring that it would upgrade the storage space of free accounts to 250 megabytes and paid accounts to two gigabytes. In April 2005, Google boosted the capacity of Gmail to two gigabytes and indicated that it would continue increasing capacity for the foreseeable future.[7]

This dramatic growth in storage capacity comes at a time when more email is being read via Web mail accounts. In the past, particularly at the time when current email privacy laws were written, email users accessed their email by downloading it onto their personal computers. That process often resulted in the deletion of the email from the computers of the service provider. Now, email – including email that has been read but which still has value to the user – often sits on a third party server accessible via the Web.

In addition, various other consumer technology developments drive the demand for greater storage space. For example, the combination of digital cameras and higher bandwidth connections encourages users not only to send photographs as email attachments but also to store photos on personal Web spaces offered on the systems of service providers.[8] Confirmations of travel arrangements, a wide range of Internet purchases and other activities are sent by email, creating records that may reside with the email service provider for a long period of time.

As one analyst stated, "The key thing about increasing storage is to make the e-mail service more of a core resource in the user's computing life. If you can put 250 megabytes worth the consumer will use it more often."[9] Further encouraging increased usage, email providers are emphasizing complementary services, such as searching capabilities, photo albums and file servers. As Google asks its Gmail users, "Who needs to delete when you have 1000 MB of storage?!"[10]

Key technologies driving the storage revolution:

- Web-based email
- Online itineraries, accounts and consumer profiles
- Voice over the Internet (VoIP)

Yet another remarkable development is now on the horizon: the routine storage of voice telephone calls. As Ohio State law professor Peter Swire has noted, this storage is likely to become far more common with the imminent growth of a new technology, Voice over Internet Protocol ("VoIP"). VoIP

[3] Wikipedia, "Early IBM Disk Storage," http://en.wikipedia.org/wiki/Early_IBM_disk_storage.

[4] Steve Gilheany, "The Decline of Magnetic Disk Storage Cost Over the Next 25 Years," www.berghell.com/whitepapers/Storage Costs.pdf.

[5] Paul Festa, "Google to offer gigabyte of free e-mail," CNET News.com (Apr. 1, 2004), http://news.com.com/Google+to+offer+gigabyte+of+free+e-mail/2100-1032_3-5182805.html.

[6] "Yahoo Ups E-mail Storage Space To 2GB," TechWeb.com (June 15, 2004), www.techweb.com/wire/26805104.

[7] Matthew Hicks, "Google Boosts Gmail Storage to 2GB," eWEEK (Apr. 1, 2005), www.eweek.com/article2/0,1895,1781392,00.asp.

[8] "Kodak Offers Wi-Fi Digital Camera, Free Photo Archiving," Washington Internet Daily (Sept. 20, 2005) (camera lets users send high-quality photos as e-mail, simultaneously uploading images for free and archiving them permanently on the company's servers).

[9] Janis Mara, "MSN Hotmail Upgrades E-Mail, Increases Storage," ClickZ News (June 24, 2004), www.clickz.com/news/article.php/3372781.

[10] This is the message that Gmail user's receive when they look in their trash folder if nothing has been deleted. In its entirety, the message reads: "No conversations in the trash. Who needs to delete when you have 1000 MB of storage?!"

uses the packet-switching network of the Internet to connect telephone calls. Broadband access makes it reliable, and its lower cost, especially for long distance calls, makes it highly attractive to both business and residential users.[11]

Prof. Swire has noted that the VoIP revolution brings with it the "likelihood that there will be systematic 'caching,' or storage, of telephone communications at the network level." One existing product, for instance, is called "CacheEnforcer." CacheEnforcer stores communications for a group of users, such as for a company or a network operated by a university. The product website says: "Because the CacheEnforcer sits in front of your WAN [wide area network] or Internet link, all outbound traffic passes through it. By setting appropriate policies on the CacheEnforcer, network managers, not individual users, determine the appropriate caching policies for the entire network."[12]

While all of these digital technologies offer a welcome set of new services, most users are not aware of the consequences that flow from the decision to remotely store their communications, personal information and files. Unless the law catches up, loss of privacy may be a hidden and unintended price of these new services.

THE CURRENT RULES FOR GOVERNMENT ACCESS TO STORED INFORMATION

The Fourth Amendment to the U.S. Constitution shields individuals from unreasonable government searches and seizures of their "persons, houses, papers, and effects." The Supreme Court has held that the Fourth Amendment protects not only a person's home or apartment and his physical person, but also the content of his telephone calls.[13] While the Court has never explicitly ruled on email, it seems logical that the same Fourth Amendment protection would apply to email in transit.[14]

However, in a series of cases in the 1970s, the Supreme Court held that the Fourth Amendment does not apply to personal information contained in records held by third parties. Once an individual voluntarily discloses information to a business, the Court reasoned, the individual no longer has a reasonable expectation of privacy in the data and the government can access the record without raising any constitutional privacy concerns.[15]

Fourth Amendment

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 Warrant 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.

[11] Testimony of Professor Peter P. Swire, Ohio State University, before the Subcommittee on Crime, Terrorism, and Homeland Security of the Judiciary Committee of the U.S. House of Representatives, "Oversight Hearing on the Implementation of the USA PATRIOT Act: Sections of the Act that Address Crime, Terrorism, and the Age of Technology" (Apr. 20, 2005). http://judiciary.house.gov/media/pdfs/swire042105.pdf. CDT is grateful for the insights of Prof. Swire, who has discussed how these trends undermine the protections for the privacy of telephone conversations. "*Katz* is Dead, Long Live *Katz*," 102 Mich. L. Rev. 904 (2004), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=490623.

[12] See www.allot.com/html/products_cacheenforcer.shtm.

[13] *In Katz v. United States*, 389 U.S. 347, 351 (1967), the Supreme Court ruled that the Fourth Amendment protects "people not places." Under the Court's analysis, whether a search violates the Fourth Amendment turns on whether the individual has a "reasonable expectation of privacy," a two-part inquiry that asks first whether the individual's conduct reflects "an actual (subjective) expectation of privacy" and, if the answer is yes, whether that expectation is "one that society [objectively] is prepared to recognize as reasonable." *Katz*, 389 U.S. at 362 (Harlan, J., concurring).

[14] See, however, Patricia L. Bellia, "Surveillance Law Through Cyberlaw's Lens," 72 Geo. Wash. L. Rev. 1375, 1385-88 (2004) (reviewing arguments why electronic communications in transit might not be subject to a constitutionally-cognizable expectation of privacy).

[15] In *Couch v. United States*, 409 U.S. 322 (1972), the Court held that subpoenaing an accountant for records provided by a client for the purposes of preparing a tax return raised neither Fifth nor Fourth Amendment concerns. In *United States v. Miller*, 425 U.S. 435 (1976), the Court held that records of an individual's financial transactions held by his bank were outside the protection of the Fourth Amendment. Lastly, in *Smith v. Maryland*, 442 U.S. 735 (1979), the Court held that individuals have no legitimate expectation of privacy in the phone numbers they dial, and therefore the installation of a technical device (a pen register) that captured such numbers on the phone company's property did not constitute a search. See generally, Deirdre K. Mulligan, "Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act," 72 G.W. L. Rev. 1557 (2004);

Although these "business record" decisions predated the digital revolution, they are still cited to support the proposition that individuals have no constitutionally protected privacy interest in personal information and records voluntarily disclosed to businesses. Under this theory, everything from medical records at hospitals and insurance companies to copies of cancelled checks held by banks to records of who calls whom compiled by telephone companies fall outside the Constitution and, unless protected by statute (which some business records are), can be freely disclosed by the business entity to the government and to others.

There are serious questions whether the business records doctrine is still constitutionally sound even as applied to transactional records, given the revealing nature of the huge amounts of transactional data generated by electronic systems today. It is important to go back and see how narrow is the Supreme Court's decision in Smith v. Maryland, the case cited as holding that transactional data for communications is not constitutionally protected. In fact, the case applied only to the numbers dialed when an ordinary call is made and not to other, more revealing non-content data. The Court stressed the narrowness of its ruling:

"a pen register differs significantly from the listening device employed in Katz, for pen registers do not acquire the contents of communications. This Court recently noted:

'Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed - a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.' United States v. New York Tel. Co., 434 U.S. 159, 167 (1977).

"Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a 'search' necessarily rests upon a claim that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone.

"This claim must be rejected." 442 U.S. 741-42.

All the more, therefore, it is unlikely that the business records doctrine ever was properly applied to the content of stored communications.[16] At most, the doctrine in its origin applied to records that a business would read and use in the normal course of business. It was developed when courts did not foresee the ability of a communications service provider to store the content of communications and documents that the subscriber never intended the service provider to read or use. Nor did courts anticipate the role of the Internet in decentralizing data storage outside the home or office. The doctrine does not take into account an alternative analogy, based on Fourth Amendment cases limiting government access to items held by a third party in physical storage, such as a storage locker. When an individual stores personal property with a third party, the owner of the property retains a privacy interest in the stored items, meaning that a warrant would be required to search the storage space. Under that analogy, transactional information regarding the terms of storage might not be protected by the Fourth Amendment, but the stored items themselves – in this case, the contents of stored email – should be covered.[17]

Stored email should be analogized to items in a physical storage locker, but case law predating the Internet has sometimes been interpreted as leaving stored digital records outside the privacy protections of the Constitution.

James X. Dempsey, "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy," 8 Albany L. J. of Science and Tech. 65 (1997).

[16] The Justice Department surely takes the position that communications stored with a service provider do not enjoy constitutional protection. U.S. Dep't of Justice, Computer Crime & Intellectual Property Section, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (Search and Seizure Manual), § III. A (July 2002), www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm ("[T]he Fourth Amendment generally permits the government to issue a subpoena to a network provider ordering the provider to divulge the contents of an account."). Some commentators have accepted this position. See, e.g., Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," 75 S. Cal. L. Rev. 1083, 1135 (2002) ("Individuals . . . probably do not have a reasonable expectation of privacy in communications and records maintained by ISPs or computer network system administrators.").

[17] Profs. Patricia Bellia and Deirdre Mulligan have done the major work on this issue. For a discussion of storage cases and more on why the stored records concept should not apply to stored communications, see Bellia, *supra* note 14, 72 Geo. Wash. L. Rev. at 1403-09, and Mulligan, *supra* note 15, 72 Geo. Wash. L. Rev at 1576-82, 1593-96.

Perhaps because Congress did not foresee the ways in which storage of email would change, the business records doctrine played an important role in shaping the statutory privacy protections currently applied to email and other records when they are in storage with a service provider. In 1986, Congress adopted the Electronic Communications Privacy Act (ECPA).[18] ECPA set rules for real-time interception of electronic communications, requiring essentially the same special warrant for access to email in transit that had been required for tapping voice communications; restricted law enforcement access in real-time to transactional information about all forms of electronic communications with the Pen Register/Trap and Trace statute; and adopted rules on access to stored electronic communications and stored transactional records held by service providers.

The part of ECPA addressing stored data, known as the Stored Communications Act (SCA), set rules for the government to obtain the content of stored emails (and now voicemails), stored transactional information related to communications, such as the "To" and "From" lines on email, and subscriber identifying information about the users of electronic communications services.[19] In many ways, ECPA was a remarkable law, but some of the distinctions in the SCA that made sense in 1986 no longer seem valid. The rules are complex, drawing many fine distinctions, about which users are probably completely unaware and which no longer match patterns of Internet usage.[20] Influenced in part by the business records doctrine (even though, as noted above, it is doubtful that the doctrine should apply to the content of stored communications), ECPA's standards for government access to email messages vary depending on whether the email is "in transit" on its way from the sender to the recipient or resting in storage on the server of the recipient's ISP. If the email is in transit, it is entitled to the highest protection under the wiretap law.[21] Email, voicemail, and other communications (such as VoIP communications) stored with a service provider are entitled to less protection, and the level of protection depends on how long the communication has been stored and possibly on whether it has been accessed by the recipient or not. In general, email, voicemail and VoIP communications stored with a service provider for 180 days or less are afforded Fourth Amendment protection (although not the higher protection of the wiretap laws) and can be disclosed to the government only pursuant to a warrant issued on the basis of probable cause (but without contemporaneous notice to the customer).[22] Communications stored on the server of an ISP or other service provider for more than 180 days can be disclosed pursuant to a court order or even a mere subpoena at a much lower standard.[23] And the Department of Justice maintains that even very recent communications stored on the computer of a service provider fall under the lower standard of protection as soon as they are listened to or read by the customer.[24] (To date, the only federal appellate court to consider this issue rejected the government's position, finding that within the 180-day period opened and unopened messages enjoy uniform privacy protections.[25]) Disclosures

The rules for government access to email draw many fine distinctions that leave much email only weakly protected – to an extent that would surprise most email users.

[18] Pub. L. No. 99-508, 100 Stat.1848, http://nsi.org/Library/Comm/ecpa.txt.

[19] For further discussion of the rules on stored communications, see Orin Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 72 Geo. Wash. L. Rev. 1208 (2004).

[20] Mulligan, *supra* note 15.

[21] The government must have a court order issued on probable cause to intercept email messages in transit. 18 U.S.C. §2518.

[22] 18 U.S.C. §2703(a) requires governmental entities to use a warrant to access the contents of electronic communications in "electronic storage" for 180 days or less.

[23] If electronic communications are older than 180 days, the government may compel disclosure using a variety of less protective instruments, including a warrant executable without notice to the subscriber or a subpoena with notice or delayed notice. 18 U.S.C. §2703(b).

[24] The government's position is that if a message is opened but remains on an ISP's server, it is no longer subject to search warrant requirements under the Stored Communications Act because it is not in "electronic storage" (defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication," 18 U.S.C. § 2710(17)), which is the statutory test for full protection. Instead, the opened email is merely being held for storage purposes and is therefore accessible under the lower standards of 18 U.S.C. § 2703(b).

[25] The Ninth Circuit found that the Stored Communications Act covers electronic messages received and opened by a recipient and resting on the service provider's servers because they were "stored ... for purposes of backup protection." *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), *cert. denied*, 2004 U.S. LEXIS 5573 (U.S. Oct. 4, 2004).

to government entities by cable ISPs are governed by the same rules.[26] And, under what had been a minor and little-used provision relating to "remote computing service," documents stored remotely can be disclosed to the government with a mere subpoena.

The ECPA drafters had in mind the 1980s model of email services: users would download email off the service provider's computer and generally did not leave their email in the hands of the service provider. Today, many mail programs are accessed through World Wide Web interfaces, so email is by default stored on Web servers of third parties. As a result of ECPA's complex rules, the same email message will be subject to many different rules during its life span. These complex rules likely do not match the expectations of email users. Most users are not aware, for example, that stored email loses some privacy protection when it is more than 180 days old or that even a new email may be entitled to less privacy protection as soon as it is opened.

For all of these reasons, the courts and Congress need to reconsider the rules applicable to stored communications.[27] Courts should recognize that the business records doctrine is not applicable to stored email, and that individuals do retain a constitutionally protected expectation of privacy in their stored emails. Congress should examine the need to amend ECPA to bring it in line with these expectations, and should consider eliminating the distinctions among different classes of stored email and subjecting all stored communications to the same warrant requirement.

Recommendation:

Congress and the courts should protect all stored email with the warrant requirement.

NON-GOVERNMENTAL ACCESS

Civil Subpoenas

The use of civil subpoenas to obtain information from ISPs has recently received greater media attention, in part due to the recording industry's initiative to subpoena the ISP records of individuals who are suspected of sharing copyrighted music files. For years, however, civil subpoenas have been served on ISPs in civil disputes such as divorce or custody cases, employment litigation, defamation lawsuits and other cases between private parties.

ECPA focuses on government surveillance concerns, and it offers no clear guidance on access to records by private litigants. ECPA generally prohibits disclosures of the contents of stored email to private parties, with certain exceptions.[28] None of the exceptions expressly authorizes disclosures to private parties pursuant to a civil subpoena. On the other hand, ECPA provides that ISPs can disclose any records pertaining to subscribers other than the content of communications to private parties without the subscriber's permission and without a subpoena.[29] (As a matter of policy, many ISPs do not disclose subscriber information without a subpoena. To the extent that this policy is stated in a privacy policy or terms of service, it is legally binding.) In addition, there is no requirement in ECPA that either the service provider disclosing records or email content to a private litigant or the private litigant obtaining them via subpoena give any

The main federal statute on email privacy does not set clear rules for disclosure of email and subscriber data to non-governmental entities in civil litigation.

[26] See 47 U.S.C. § 551(c)(2)(D), added by §211 of the PATRIOT Act.

[27] The academic literature has persuasively laid the foundation for this reexamination. See Bellia, *supra* note 14, and Mulligan, *supra* note 15. Prof. Bellia writes, "In 1986, in ... the Electronic Communications Privacy Act, Congress adopted a layer of statutory protection for stored communications. Stored communications have evolved in such a way that these provisions ... are becoming increasingly outdated and difficult to apply. In addition, because the provisions were adopted amid uncertainty about whether the Fourth Amendment protects privacy in communications held by a third-party service provider, they allow law enforcement officials to compel production of some categories of communications without a search warrant. As I will show, revision of the statutory framework is urgently needed." 72 G.W. L. Rev. at 1396-97.

[28] 18 U.S.C. § 2702.

[29] 18 U.S.C. § 2702(c)(6) (permitting disclosure of subscriber information (not including the contents of communications) to "any person other than a governmental entity").

notice to the person whose information is being sought.[30] In contrast, the Cable Act, unlike ECPA, does expressly address the question of private party access to the content of stored email. If the ISP is covered by the Cable Act, that law requires parties to civil suits to obtain a court order and requires the cable operator (offering ISP service in this instance) to provide notice to the subscriber.[31]

The process surrounding civil subpoenas can be complicated. For example, a lawsuit may be filed in New York, the service provider upon whom the subpoena is served may be in Virginia, and the individual whose information is sought may live in California. Even if a subpoena is issued by a court in the same state as the user's ISP and the user is notified of the subpoena, the notice may not direct him to the court in which the lawsuit is being filed or provide information about the claims being made. To respond, even an individual who realizes that her information has been requested would probably need to hire a lawyer in the state where the subpoena is served or the state where it was issued, or both, in order to file a formal objection prior to the information being released by the service provider.

Case law and statutes make a distinction between historical data and real-time data. The government is seeking to extinguish that distinction in a way that would open communications to government access without probable cause.

Deletion from Storage

Even as service providers offer expanded storage capacity, many have tightened their rules for how long they will store information in unused accounts before terminating the account and deleting the email. This is understandable from a business perspective, since providers want to purge unused accounts in order to free up more space for those actually using it. However, users may not read the fine print and may be astonished to find that information left in an unused account has been wiped out, particularly if it was deleted without specific warning.

A second question concerning deletion is when will the provider automatically delete older mail from a still active account. It is appropriate that policies differ from provider to provider – certainly Google's competitive offer of a service that never deletes email expands consumer choice – but there is a question whether users are adequately informed of ISPs' policies.

A third issue is whether records "deleted" by the subscriber are actually removed from all backup storage. Actual practice may not match the ordinary user's expectation that, if he cannot retrieve a message himself, then it cannot be retrieved at all. Google's Gmail privacy policy raises an interesting point about "deletion time." Google notes that it cannot assure that all backups of information will be deleted immediately when a user requests that information be deleted. In speaking with Google representatives about this issue, they say that they are actually following industry practices, but feel impelled to advise users that it is impossible to promise that all deletion requests will be immediately implemented throughout their system. Google says that information that a user believes to have been deleted could be still available when a subpoena is issued.[32]

Next-of-Kin Requests

Access can also be a concern for family members who want access to the account of a relative who has died. Much of an individual's personal business may have been conducted through email, and surviving next-of-kin may want to gain prompt access to that information. While service providers often would like to help families, security and privacy concerns put the service providers in a difficult situation. At the least, service providers want to be sure they are dealing with the legiti-

[30] Virginia has a law requiring notification of ISP customers of a civil subpoena prior to disclosure. See Va. Code Ann. § 8.01-407.1(A)(3), available at http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+8.01-407.1. A similar proposal was considered by the California legislature in 2003 but was not adopted. See the Internet Communications Protection Act, AB 1143, available at www.leginfo.ca.gov/pub/03-04/bill/asm/ab_1101-1150/ab_1143_bill_20040621_amended_sen.html.

[31] 47 U.S.C. § 551(c)(2)(B). The PATRIOT Act amended the Cable Act to make it clear that, when a cable company is acting as an ISP, it is covered by ECPA for purposes of disclosures to government entities, but the PATRIOT Act did not change the rules for cable ISP disclosures to private parties in civil litigation.

[32] While some ISPs say that deletion is immediate, they are probably not overwriting the information instantly, leaving it available for discovery by forensic experts. Google is careful not to claim that information is instantly deleted if it could possibly be recovered.

mate heirs or executors of a deceased customer before releasing what may be sensitive and even valuable information. Some service providers have a flat rule against transferring accounts or divulging information about them, even to relatives of a deceased subscriber.[33] Email accounts may contain communications that the deceased, if given the option, would not choose to provide to relatives. As people store more information with third parties, these dilemmas will continue to grow.[34] It is unclear whether the resolution of these issues lies solely in privacy law or will be best dealt with in conjunction with property and estates law.

Service Provider Access

A June 2004 decision by a three-judge panel of the federal appeals court in Boston triggered a controversy that illustrated another way in which ECPA does not match user expectations. The case, *United States v. Councilman*,[35] noted that an ISP could read and use for its own business purposes (but not disclose to others) the emails of subscribers held in storage on the service provider's computers. The court went one step further and held that emails could be read by service providers even when they were in the very brief temporary storage that occurs as an email is being transmitted. A larger panel of the court reversed that decision, holding that the email was in transit when it was intercepted and therefore could not be read and used by the service provider.[36] But the second decision did not question the provision of ECPA that allows service providers to read their customers' email for any purpose at all once it is in storage on the ISP's server. Many in industry felt that, given the practices of legitimate ISPs, which do not read their customers' emails, the *Councilman* controversy was overblown. Nevertheless, the case drew attention to an overlooked gap in the law. ECPA's failure to prohibit ISPs from reading their subscribers' email is in contrast to the law governing telephone companies, which does prohibit them from listening to customer conversations except to ensure service quality, detect fraud, or otherwise provide service.[37]

Next-of-kin requests pose difficult questions for email service providers, but do not seem to merit a legislative response.

STUDY OF INDUSTRY PRACTICES

During the summer of 2004, the Center for Democracy and Technology conducted a study of industry practices in relation to data storage and access. We examined the policies of seven of the largest commercial email providers. We collected most of our information from the providers' Web sites, including terms of service and privacy policies. When we could not find information, we called the ISPs' help lines. We shared a draft of the results with the chief privacy officer or legal counsel for each of the service providers studied.

Our survey covered five issues:

1. Deletion Without Subscriber Request – When is an inactive account terminated and its contents deleted, and when is email automatically deleted from an active account?
2. Deletion upon Request – How long does it take to remove mail from the provider's server after the user deletes it from her screen?
3. Next-of-Kin Access – What documentation is required from relatives in order to provide access to next-of-kin records?

[33] Ariana Eungung Cha, "After Death, a Struggle for Their Digital Memories," Washington Post, p. A1 (Feb. 3, 2005); Jeffrey Selingo, "Whose Data Is It, Anyway?" New York Times, p. G1 (June 3, 2004).

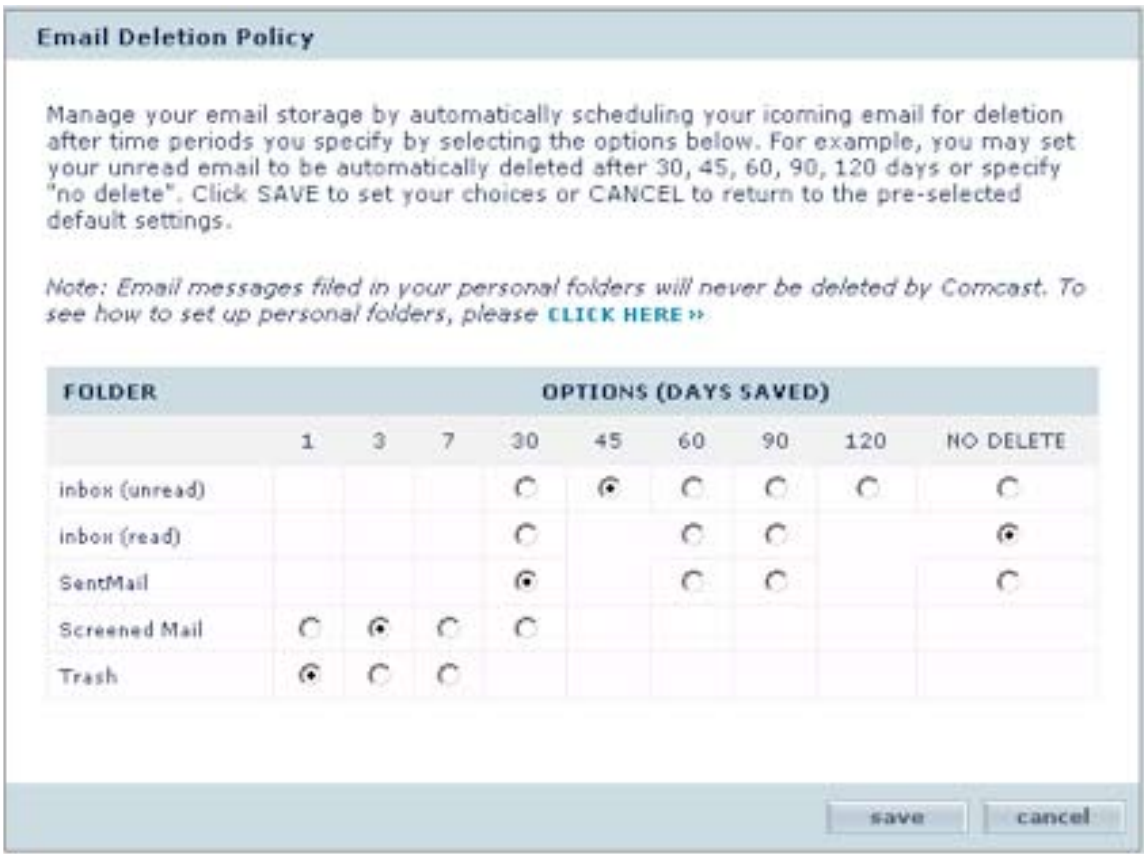
[34] The issue is complex. Stored email implicates the privacy not only of the account holder but also of those who corresponded with the account holder. The issue was illustrated when Yahoo! denied the father of a U.S. Marine killed in Iraq access to the son's Yahoo email account. The company felt bound by its terms of service, in which the company promises not to disclose private email communications of its users. Our research indicated that Yahoo's policy is to never transfer email, but a news story indicated that Yahoo! would disclose the stored data if family members obtained a court document verifying their identity and relationship with the deceased. Jim Hu, "Yahoo denies family access to dead marine's email," CNET News.com (Dec. 21, 2004).

[35] *United States v. Councilman*, 373 F.3d 197 (1st Cir. 2004), rev'd en banc, 418 F.3d 67 (2005).

[36] "Federal Appeals Court Reaffirms E-Mail Privacy Protections," CDT Policy Post 11.20 (Aug. 17, 2005), www.cdt.org/publications/policy-posts/2005/20. CDT filed an amicus brief urging reversal (siding with the Justice Department). The en banc review pertained only to the question of whether emails can be read while in temporary storage incident to transmission. The en banc reversal left untouched the rule that ISPs can read their customers' emails after they come to rest in the recipient's inbox on the ISP's server. That rule, even though it seems inconsistent with Congress' overall intent in ECPA, is statutorily based, so its revision will require legislative action.

[37] 18 U.S.C. §2511(2)(a)(i).

It no longer seems sensible to provide different protections to email depending on how old it is, or whether it has been read once or not.



Email Deletion Policy

Manage your email storage by automatically scheduling your icoming email for deletion after time periods you specify by selecting the options below. For example, you may set your unread email to be automatically deleted after 30, 45, 60, 90, 120 days or specify "no delete". Click SAVE to set your choices or CANCEL to return to the pre-selected default settings.

Note: Email messages filed in your personal folders will never be deleted by Comcast. To see how to set up personal folders, please CLICK HERE »

FOLDER	OPTIONS (DAYS SAVED)								
	1	3	7	30	45	60	90	120	NO DELETE
Inbox (unread)				○	◉	○	○	○	○
Inbox (read)				○		○	○		◉
SentMail				◉		○	○		○
Screened Mail	○	◉	○	○					
Trash	◉	○	○						

save cancel

4. Civil Subpoenas – Do email service providers give notice to a subscriber whose records are sought pursuant to a civil subpoena?
5. Reading Customer Email – Do the privacy notice and terms of service agreement explicitly state that the company does not read its customers' emails for purposes other than providing service, enforcing terms of service or protecting the rights of the ISP?

It turned out that it was sometimes difficult even from the large ISPs to track down the policies addressing our questions, which suggests that companies need to be more conscious of these issues and need to inform users in a clear manner.[38]

Some providers are explicit about giving users notice and control over deletion/storage practices. For example, Comcast permits users to set their own e-mail deletion timeframes for webmail folders. Copied above is the table of choices provided to Comcast subscribers, with the default settings checked. Other ISPs may also provide user-defined deletion policies for their webmail services.

We found that industry practices on retention and deletion vary. This is not itself a problem. It may actually offer consumers desirable choices, so long as policies are clear. Policies range from defaults to user control. Emails from terminated free accounts, which are deleted based on date of last activity, generally seem to be deleted earlier than those in paid accounts, which are removed based on date of missed payment. For the most part, emails deleted by the customer are removed from the provider's server quickly, between a few hours to 3 days after the user has deleted them. Google's Gmail service does not specify a server removal date, but that seems to be due to extra precision on the part of the drafters of Google's privacy statement, recognizing that even when mail has been deleted from the ISP's server it may still be available for forensic discovery until it has been overwritten.

[38] Our findings are reported in detail at Ari Schwartz, Deirdre Mulligan, and Indrani Mondal, "Storing Our Lives Online: Expanded Email Storage Raises Complex Policy Issues," 1 ISJLP 597 (2005), online at http://is-journal.org/articles.php (subscription required).

We also found a variety of policies with respect to next-of-kin requests. Most service providers require high levels of proof, such as death certificates, in order to verify next-of-kin requests. It is interesting to note that, even with documentation, Yahoo! does not give relatives access to the contents of a deceased person's account. This is in part because Yahoo! is a free service and does not require identifying information from subscribers.

It is also interesting to see consistency in the way major ISPs handle civil subpoena requests. In non-emergency situations, every ISP we surveyed gives its customers notice soon after receiving subpoena requests, and then allows customers generally about two weeks to challenge the order prior to releasing information. (We assume that this practice applies to disclosure of both email content and subscriber identifying information.) Under the Cable Act, cable ISPs require a court order to disclose information to private parties and must provide notice to the subscriber, giving the subscriber an opportunity to object.

Most ISPs in our survey implied that they do not read their customer's email. Policies were not always explicit. As the *Councilman* case illustrated, there may be outliers among smaller ISPs.

POLICY CONSIDERATIONS

Protection of user privacy depends on a mix of user education, industry policies, judicial rulings, and legislation like ECPA. Given some dramatic changes in technology, especially the shift to Web-based email and the offering of huge amounts of online storage, all four areas may need revision.

Many of the most troubling issues relate to government access. Some distinctions in ECPA now seem outdated. It no longer seems sensible to provide different protections depending on how old an email is, or based on the possible (but disputed) distinction between opened versus unopened email. In 1986, when ECPA was adopted, downloaded email was generally not saved on the service providers' computers. Downloaded email, whether opened or unopened, usually sat only on the user's computer and was fully protected by the Fourth Amendment.[39] Today, most corporate e-mail still works that way, so that email is still kept on users' computers (including corporate back-up computers), not on Web servers or mail servers of third parties. However, in contrast to 1986, with regard to the significant percentage of email that is Web-based (including most consumer systems like AOL, Hotmail, Gmail, and YahooMail), opened email is commonly kept on third party servers. It is no longer sensible to accord it lower protection. Accordingly, legislators should consider updates to the Electronic Communications Privacy Act to keep pace with these changes in technology. ECPA could be amended to provide, as a general rule, that the government not be able to obtain email content information or other stored communications without a search warrant. It would seem reasonable to eliminate the "180 day" distinction and any distinction between opened and unopened email, in light of the fact that, with Web-based email programs, open email is routinely kept on third party servers.[40] Similarly, the distinction between "electronic communications service providers" and "providers of remote computing service" should probably be eliminated – most ISPs are both, and most email moves from one to the other without the customer being aware that its legal status has changed.

Legislators should consider updates to the Electronic Communications Privacy Act to keep pace with changes in technology.

The recent *Councilman* decision highlights a loophole in ECPA that technically allows service providers to read and use (but not disclose to others) the content of their subscribers' email. The company whose practices were at issue in Councilman may have been one of a kind. There is no evidence that other ISPs "read" customer emails without consent. While major ISPs do not engage in this type of behavior, a narrowly-tailored reform would solidify customer confidence by making it clear that ISPs may only access subscribers' emails

[39] Corporate systems were different.

[40] Some of these changes passed the House Judiciary Committee in 2000 as part of H.R. 5018. www.cdt.org/wiretap/tapstraps.php

with consent or as required to provide the service or protect the ISP's rights or property.[41]

In the 108th Congress (2003-04), legislation was introduced to address some of these issues. The E-mail Privacy Act, sponsored in the House by Representative Inslee (D-WA), would have ensured that law enforcement officials have to obtain a wiretap order in order to gain real-time access to Internet communications. The Inslee bill also would have prevented ISPs from reading their customer's email except in cases where it is necessary to provide service or with consent. With the same intent, Representative Nadler (D-NY) introduced the E-mail Privacy Protection Act. However, while both bills would have helped to close the loophole highlighted by the *Councilman* decision, they did not address other shortcomings of ECPA.

It might also be desirable to have legislation addressing the rights and obligations of ISPs served with civil subpoenas. ECPA currently prohibits ISPs from disclosing the email of their subscribers without some legal process, but it does not prohibit them from disclosing identifying information or transactional records to private parties. This could be addressed by requiring at least a subpoena for disclosure of subscriber identifying information and transactional data. In addition, even though major ISPs as a matter of policy give notice to their subscribers when information is subpoenaed, this could be codified and it could be made clear that notice must be given whether the subpoena is for content or identifying or transactional information. Legislation could place the responsibility for providing notice on the subpoenaing party unless the subpoenaing party does not know the subscriber's address, in which case the ISP could afford notice, with compensation for its expense in doing so. The law could specify what would be an adequate time for the subscriber to contest the subpoena prior to the information being released. It could also require that the subpoenaing party provide the subscriber, or the ISP to pass on to the subscriber, sufficient information to understand the charges and to identify the court in which they are being sued. The consensus standard found in our study -- immediate notification and a 14-day waiting period prior to disclosure -- would be a good benchmark for such legislation.[42] Legislation dealing with notice probably should provide ISPs with the right to recover their reasonable costs incurred in processing and replying to private and government requests for customer information, whether resulting in a positive or negative response.

At this point, it seems that account termination and email deletion questions do not require legislation. As a matter of industry practice, each ISP should clearly communicate to customers what are its termination and deletion policies. These policies should be available on their Web sites and in terms of service and privacy policies. A good practice may be to give users control, allowing them to set retention periods.

In part, the "next-of-kin" access issues stem from the fact that identifying information is relatively easy to obtain, so ISPs feel compelled to require people claiming to be relatives to provide high levels of authentication in order to prove their relation to the account holder and their need to access the account. But ISPs that decline any next-of-kin requests may recognize that the privacy interests at stake include not only those of the deceased but also of those persons (including non-family members) with whom the deceased corresponded. One solution is for users to leave a copy of their passwords with relatives, but this too raises privacy and security issues. Another solution is for individuals to address this issue in their wills. Alternatively, ISPs could include in their terms of service some kind of standard language, similar to the beneficiaries clause in an insurance policy, stating that, upon death of the subscriber, stored data would be provided to designated persons. Clarifica-

[41] One way to accomplish this would be to add to the end of section 2701(c)(1) the language in 18 U.S.C. § 2702(b)(5): "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service." This is essentially identical to the language applicable to telephone companies, 18 U.S.C. § 2511(2)(a)(i).

[42] In California, in 2003, legislation was introduced to codify the obligation, but did not pass. See the Internet Communications Protection Act, AB 1143, available at www.leginfo.ca.gov/pub/03-04/bill/asm/ab_1101-1150/ab_1143_bill_20040621_amended_sen.html.

tion of policies regarding deletion times may help the situation by making it easier for next-of-kin to realize how quickly they need to request access to a deceased's email account. It seems that the thorny questions about privacy in the context of a deceased subscriber are worthy of further industry dialogue to develop appropriate practices and perhaps more consistent approaches.

Chapter II

Location Technologies:

The Future of Surveillance

Clandestine electronic tracking devices have been widely used by government agents for many years, but today's location tracking capabilities are qualitatively unique. The earliest location tracking devices–electronic "beepers"–were planted by government agents on an automobile or in a container and monitored in real-time to determine the location of the carrier. Those early electronic beepers had limited range and were generally used while tailing a suspect to relocate the target after the investigator's view had been obstructed. More advanced tracking devices do not merely substitute for real-time visual surveillance, but provide remote monitoring of locations, including locations not visible from public spaces. They also may store such location information for retrieval and review long after the time in question. Global positioning system (GPS) technology substantially increases the accuracy of location devices.[43]

Location technologies offer consumers added safety, security and convenience.

[43] GPS technology uses a series of satellites in stable orbits above the earth. These satellites emit signals that a GPS locator passively receives. The GPS locator device itself sends out no signal to the satellites. The distance to the GPS satellites can be determined by calculating the amount of time it takes for their signals to reach the receiver.

Whereas in the past government agents had to secretly plant a tracking device on a suspect, today many individuals willingly carry location devices with them, in the form of cellular phones and other mobile communications devices, or install them in their cars, in the form of in-car navigation systems.[44] These devices offer substantial safety, security and convenience benefits to users. Nevertheless, the location information generated by these devices constitutes a record of the user's movements that government agents can monitor in real-time or scrutinize retrospectively.

One technologist recently summed up the trend:

"We are on the cusp of a new era in technology where the location of computing and communications devices can be determined accurately and inexpensively. This will have particular importance for location-aware mobile devices such as cell phones and PDAs [personal digital assistants], and will raise a large number of privacy issues related to the collection, retention, use, and disclosure of location information. Drivers of the issues we will face include: (1) technologies such as geographical positioning systems (GPS) that can be inexpensively incorporated into even very small portable devices; (2) government mandates such as Enhanced 911 (E911) in the United States that require the incorporation of location-determination capabilities in certain devices such as cell phones; and (3) marketplace opportunities for products and services that exploit location information and fall under the rubric of mobile commerce or e-commerce."[45]

The government often has a compelling interest in using cell phones and other devices to track individuals in real-time.

This chapter addresses the privacy issues associated with government access to location information generated by consumer wireless technologies, and focuses specifically on cellular phones and car navigation systems. Not far behind, however, are location-aware computers and the linking of radio frequency identification (RFID) devices with computer networks. The development of what may soon be ubiquitous location-based capabilities and applications for a wide range of products illustrates how market-driven changes in technology can augment government's reach.

In this chapter we:

- describe how cellular phones and car navigation systems provide location information;
- highlight the sensitive nature of location information and the privacy concerns raised by different types of location devices;
- explain the distinction among various legal standards that apply to different types of government surveillance;
- identify inconsistencies in the case law addressing government use of various location identifying technologies; and
- explore options for resolving this lack of clarity and establishing clear rules to apply to government access to location data.

We recognize the value of location information for legitimate law enforcement and intelligence purposes. At the same time, the potentially broad and covert nature of this method of surveillance requires special attention. Location tracking reveals sensitive information about a person that may have no relation to criminal activity. Accordingly, appropriate legal standards must be established by the courts and, in the absence of judicial action, by Congress to safeguard privacy rights against indiscriminate government surveillance of individuals' movements and activities.

Based on a review of the law, and in light of the increasing power of location technology to locate people in non-public places, we conclude that government acquisition of location information, either from a consumer device or a government-installed tracking device, should be permitted only pursuant to a search warrant issued on a finding of probable

When a receiver estimates the distance to at least four GPS satellites, it can calculate its position by latitude, longitude and altitude. New GPS technology can pinpoint locations even inside buildings, which was not previously possible. See www.qualcomm.com/qis/qpoint/; Vicki Lipset, "Sensing Location" (Dec. 1, 2003), available at www.ultrawidebandplanet.com/technology/article.php/10850_3114391.

[44] For purposes of this paper, we do not consider other systems that collect periodic location information, such as automatic toll payment systems.

[45] Robert P. Minch, "Privacy Issues in Location-Aware Mobile Devices," Proceedings of the 37th Hawaii International Conference on System Sciences (2004), http://csdl2.computer.org/comp/proceedings/hicss/2004/2056/05/205650127b.pdf.

cause to believe that a crime has been, is being or is about to be committed and that the surveillance will result in information pertinent to its investigation.[46] Such orders should impose a time limit on the duration of the surveillance. Furthermore, prospective access to real-time location information and access to detailed logs of retrospective location information should be treated the same for purposes of the applicable legal standard.

TYPES OF LOCATION TECHNOLOGIES

Two general categories of location technologies and applications exist that can aid government investigators. One type consists of devices that are installed by government agents and directly track the location of objects or monitor the location of people. The other includes wireless consumer devices such as cellular phones and car navigation systems that are equipped with built-in location capabilities. Devices in this second category do not need to be installed by law enforcement because their location capabilities are built-in by the manufacturer as part of the product.[47]

Cellular Phones

While a cell phone is turned on, whether or not it is making a call, it is regularly seeking out the nearest antenna and sending to it its identification numbers. The carrier uses this data to calculate the location of the phone and thereby to route calls to the antenna tower for the appropriate sector (or "cell") for wireless transmission to the phone. Cell phone networks may identify the cell site or tower used at the beginning of a call, during the progress of the call as the phone moves from cell to cell, and at the end of the call. They may also identify the general direction from which the call is coming to the tower. They may also permit determining a person's location and movements so long as the cell phone is on, regardless of whether a call is in progress.[48] In addition, even though carriers use the cell tower with the strongest signal to manage and deliver calls, the service provider (or the government, if given access) can compare the signals for all towers "lit up" by the phone and more precisely locate the phone through a process called "signal triangulation."[49] Finally, a wireless service provider's logs may store cell site information retrospectively, allowing anyone with access to trace callers' past movements.

The accuracy of cell site location information varies. According to one court, in suburban or rural areas, towers can be many miles apart. In urban areas, towers may be anywhere from several hundred feet to as many as 2000 feet or more apart.

Another type of cell phone location information is now becoming much more accurate. To enhance the response capabilities of emergency personnel to 911 calls made from cellular phones, the Federal Communications Commission (FCC) has adopted regulations mandating that, by the end of 2005, wireless carriers be able to locate callers who dial 911, and to do so with much greater accuracy than mere cell site.[50] There are two different ways that carriers are complying with this requirement. The caller's position may be determined by the phone itself using a built-in GPS receiver, which receives satellite signals to determine its location. That location information is then transmitted with the 911 call. Alternatively, the wireless provider may locate a cell phone through triangulation data collected by its network of antennas and pass that on to the public safety answering point when 911 is called. A combination of the two approaches may also be used. While the network-based solution is

[46] In foreign intelligence investigations, a similar standard would require probable cause to believe that the target of the surveillance was a terrorist or other agent of a foreign power.

[47] The National Workrights Institute also has drawn attention to the issue of employers tracking the locations of their employees using cell phones, car navigation systems and other devices. National Workrights Institute, "On Your Tracks: GPS Tracking in the Workplace" (2004), www.workrights.org/issue_electronic/NWI_GPS_Report.pdf.

[48] Brad Smith, "GPS-based Games Raise Privacy Concerns," Wireless Week (Sept. 1, 2003), www.wirelessweek.com/article/CA319406?spacedesc=Departments&stt=001. It is also possible for the government to track a cell phone with the government's own equipment, without having to enlist the aid of the cellular provider.

[49] Al Gidari, Esq., Perkins Coie LLP, Electronic Surveillance Update (Dec. 24, 2005).

[50] See www.fcc.gov/911/enhanced for the latest FCC rules on 911 location information.

As location technology becomes more precise, it supports ongoing monitoring that continues into places where there is a reasonable expectation of privacy.

always active, the GPS handset solution can offer users greater control, since users can be given the ability to choose when to transmit their GPS location (except when dialing 911, when transmittal is automatic). However, as noted, the marketplace is developing attractive services that encourage users to disclose their location (whether generated by triangulation or by GPS) even when not calling 911. (And phones that incorporate GPS technology also generate location data as they register with the cellular network every few seconds while powered on, whether or not a call is in progress.)

Location aware devices:

- Cell phones
- Automobiles
- Computers

Car Navigation Systems

GPS navigation systems like General Motors' OnStar offer car owners a multitude of useful services including mapping capabilities, stolen vehicle tracking, remote door unlocking, directory information, and emergency roadside assistance. These systems determine location with GPS and communicate with an assistance and services center through the cellular network, offering two-way transmission of both voice and data (including location data). Depending on how the system is managed, law enforcement officials may be able to obtain location information from the service provider, either in real-time or after-the-fact.[51]

Location Aware Computing

Location based services have thus far been centered around wireless phones and PDAs. Computers are the next step. "With the transition of the notebook from just being a portable computer to being a mobile computing device, LAC [location aware computing] holds a lot of promise towards growing the value and excitement of the mobile notebook platform."[52] Prompted by the FCC's E911 rules, wireless carriers and others who are required to make enhancements to their networks to incorporate location capabilities for emergency response purposes are looking for revenue-generating applications for the same technology. Recently, the FCC extended its E911 rules to Voice over Internet Protocol (VoIP) services, increasing the push to design location capabilities for computers. Meanwhile, industry pioneer Steve Wozniak is reportedly developing a wireless platform for location aware computing, marrying GPS and wireless technologies to create a wireless network that will serve as a backbone for location applications.[53] Other technologists are working on tracking systems for high-density urban areas and indoor settings, where GPS capability is limited.[54] "With numerous factors driving deployment of sensing technologies, location-aware computing may soon become a part of everyday life."[55]

PRIVACY CONCERNS RAISED BY ELECTRONIC LOCATION DEVICES

Location information can reveal a person's acquaintances and physical destinations such as

[51] For a brief explanation of how such systems work, see *In re Application of the U.S. for an Order Authorizing Roving Interception*, 349 F.3d 1132 (9th Cir. 2003). A related category of devices are Event Data Recorders (EDRs), which are intended to record data associated with car crashes and which in the past stored only 5 seconds of data. However, EDRs are being designed with GPS and communications capabilities. See "Comments of the Electronic Privacy Information Center before the National Highway Traffic Safety Administration," Docket No. NHTSA-2004-18029, August 13, 2004 www.epic.org/privacy/drivers/edr_comm81304.html.

[52] Sundeep Bajikar, "New Notebook Capability: Location Aware Computing" (February 2003) www.intel.com/design/mobile/platform/downloads/lac_white_paper.pdf.

[53] Mark David, "I Was Where Woz Was: Location-Aware Computing" (Nov. 6, 2004) www.macnewsworld.com/story/I-Was-Where-Woz-Was-Location-Aware-Computing-37878.html.

[54] Tom Spring, "Location Reigns Supreme With Future PCs; MIT conference looks at the future of location-based computing," PC World (October 1, 2004) www.pcworld.com/news/article/0,aid,118031,00.asp. For additional sources, see Location Privacy Workshop - Individual Autonomy as a Driver of Design (August 2004), www.spatial.maine.edu/LocationPrivacy/backgroundReadings.html and www.spatial.maine.edu/LocationPrivacy/program.html.

[55] Mike Hazas, James Scott, John Krumm, "Location-aware computing comes of age," Computer, Vol. 37, Issue 2, pp. 95-97 (Feb 2004).

medical clinics, government services buildings, and commercial establishments. Such data may imply–correctly or incorrectly–additional information about the individual, including preferences and associations. Informational privacy about one's movements in society implicates the constitutional right to travel and the freedom to associate. Without assurance that one's movements are not arbitrarily being watched and recorded by the government, full exercise of these liberties will be chilled.

The capability of current location technologies to record both present and past movements of individuals raises greater privacy concerns than older electronic beepers. Beepers emit an electronic signal that police can monitor with a receiver; the signal becomes stronger or weaker depending on how close the receiver is to the beeper. This basic technology is not conducive to long-term, remote surveillance. With newer technologies, however, tracking can be done automatically by a remote computer, making it possible for law enforcement to monitor the movement of many more people for longer periods of time. It is now possible to compile and retain comprehensive records of individuals' movements over a period of years. And the technology will continue to improve in the coming years, making it easier and easier to monitor individuals' precise locations over prolonged periods of time.

In some ways, location tracking is more intrusive than a traditional physical search. Whereas a search warrant restricts the physical areas police may enter to search, a record of a person's movements cannot be similarly limited so as to provide only location information that may relate to criminal activity. Police can monitor a person's movements continuously. Also, location tracking is often covert. In the execution of the traditional search warrant, an announcement of authority and purpose ("knock and notice") is required so that the person whose privacy is invaded can observe any violations in the scope or conduct of the search and seek to halt or remedy them. In contrast, an individual whose movements have been monitored by law enforcement agents might never be aware that she was a target of surveillance. [56]

LEGAL STANDARDS

No existing statute sets explicit standards for government location tracking. There is a federal statute on tracking devices, 18 U.S.C. § 3117, but it does not provide a particular standard for approving use of a tracking device.[57] However, in the Communications Assistance for Law Enforcement Act of 1994 (CALEA), Congress specified that law enforcement agencies could not use an order authorizing a pen register or trap and trace device to acquire location information.[58] While it did not specify what authority could be used to acquire location information, Congress made it clear that the very low standard of the pen/trap law, which is addressed below, was inadequate. Congress reaffirmed that location tracking information is entitled to special treatment in 1999, when it specified that telecommunications carriers cannot disclose wireless location information for commercial purposes except with the prior express approval of the customer.[59] By requiring prior express authorization, Congress set a higher standard for location information than for other telephone transactional data.

How, then, should the courts and Congress develop an appropriate standard for access to

[56] See Hiawatha Bray, "GPS Spying May Prove Irresistible to Police" (Jan. 17, 2005), www.boston.com/business/technology/articles/2005/01/17/gps_spying_may_prove_irresistible_to_police.

[57] Section 3117 merely states: "If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction." It was enacted as part of the Electronic Communications Privacy Act of 1986. It was "intended to permit the installation of tracking devices which may move from district to district" but "does not affect the legal standard for the issuance of orders authorizing the installation" of mobile tracking devices. House Rept. 99-647, at 60 (June 19, 1986).

[58] 47 U.S.C. § 1002(a)(2). A pen/trap order permits law enforcement to obtain transactional, non-content information about wire and electronic communications in real time. 18 U.S.C. § 3121-3127.

[59] 47 U.S.C. § 222. The limitation, however, only applies to telecommunications carriers. It does not apply to other entities that since 1999 have been emerging to collect or use location information from wireless devices in the course of providing location-based services. In a way that Congress perhaps did not foresee in 1999, increasingly telecommunications carriers are less important to the acquisition and processing of location information than other entities.

location information? There are essentially five different legal standards for government access to information:

- the high "probable cause plus" standard required for wiretaps;
- the probable cause standard for basic search warrants;
- the "specific and articulable facts giving reason to believe" standard under 18 U.S.C. § 2703(d) for court orders for access to certain stored records;
- the certification of relevance standard for court orders for pen register and trap and trace devices; and
- the relevance standard for subpoenas.

In the following discussion of each of the five levels of protection and their applicability (or inapplicability) to location information, we explain why we believe that location tracking should be subject to the relatively high standard for search warrants.

"Probable Cause Plus" Under the Wiretap Statute

In response to the uniquely invasive nature of wiretaps and hidden microphones ("bugs"), which involve covert, wide-ranging, and ongoing intrusions on an individual's privacy interests, Congress in 1968 established stringent procedural protections in the federal wiretap law (the "Wiretap Act" or "Title III").[60] Under the Wiretap Act, prior judicial authorization is required for interception of the content of communications. Approval can be granted only when law enforcement shows probable cause of criminal activity. Parties whose conversations are intercepted are entitled to after-the-fact notice. The wiretap laws apply to real-time interception of voice communications, face-to-face or over a phone, and to interception of electronic communications such as e-mail or other computer-to-computer transmissions.[61]

By its terms, the wiretap law applies only to the interception of the contents of oral, wire, or electronic communications in real-time.[62] Title III does not apply to transactional information about the conversation, such as the time or duration of a call or the number to which a call is placed. Magistrate Judge Stephen Smith, in a detailed and well-reasoned opinion last year, concluded that cell site information associated with a cell phone call is not content and therefore is not covered by Title III.[63] As Judge Smith noted, cell site information is generated even when no communication is in progress. Also, Judge Smith noted, the definition of "electronic communication" in Title III explicitly excludes "any communication from a tracking device," thereby taking information transmitted from tracking devices outside the coverage of Title III.[64] (Different considerations may apply

[60] 18 U.S.C. §§ 2510-2522. Congress enacted the wiretap law in response to a 1967 Supreme Court decision, *Berger v. New York*, 388 U.S. 41 (1967), which found that in the context of electronic surveillance the Fourth Amendment required procedural protections beyond those of a basic search warrant, in order to protect against the uniquely intrusive aspects of wiretaps and bugs. The federal wiretap law is sometimes called "Title III" because it was enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Separate legislation, the Foreign Intelligence Surveillance Act, established probable cause requirements for wiretaps in foreign intelligence and international terrorism investigations.

[61] For more information about the federal wiretap law, see the Center for Democracy and Technology's overview of electronic surveillance, www.cdt.org/wiretap/wiretap_overview.html.

[62] Certain car navigation systems have a feature that allows the service provider to open a cellular connection to the vehicle and listen to oral communications within the car. Title III very likely applies to the use of car navigation systems for surveillance in this manner, since the system is being used as a bug to collect the content of conversations. In *In re Application of the U.S. for an Order Authorizing Roving Interception*, 349 F.3d 1132 (9th Cir. 2003), the Ninth Circuit held that the in-car navigation service provider was not required to enable this function to assist the FBI in eavesdropping on conversations occurring inside a vehicle equipped with the system even though the FBI had obtained a Title III order, but the ruling was not based on privacy grounds. Rather, the court held that the wiretap order could not be enforced because the FBI's use of the passive listening feature disabled other system services and therefore the surveillance could not be completed with "a minimum of interference" with the system's operation, as required under the wiretap law. 18 U.S.C. § 2518(4). Under the court's rationale, if the technical problem of conducting surveillance without disabling other features can be overcome, a police agency will likely be permitted to invoke the authority of Title III to use these systems to monitor conversations taking place in the targeted vehicle.

[63] *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747 (S.D. Tex. 2005). In *United States v. Forest*, the defendants argued that the government violated Title III by intercepting cell site data that revealed their general location while traveling on public highways. The Sixth Circuit did not decide whether the wiretap law applies to cell site data. Instead, the court held that even if cell site data falls within the definition of electronic communication, the defendants could not invoke the suppression remedy under Title III because it is available only for voice communications. *United States v. Forest*, 355 F.3d 942, 949-50 (6th Cir.), *cert. denied*, 125 S.Ct. 174 (2004). The court also found that the Fourth Amendment did not apply because the defendants were tracked only on public highways. *Id.* at 951-52.

[64] 18 U.S.C. § 2510(12).

to GPS data that is communicated as the "content" of a communication, which is what happens when an in-car navigation system makes a cell phone call in order to send the car's GPS data to a service center and which may also happen when users of cell phones and other portable devices invoke other location-based services by transmitting location coordinates as part of the content of a wire or electronic communication asking for certain information.)

As a policy matter, some of the same privacy concerns underlying Congress's intent in adopting the special protections of the wiretap laws arise with equal force in the context of location tracking. Like wiretapping, location tracking proceeds without notice to the suspect and involves an ongoing intrusion on privacy. Location monitoring technology also poses the risk of overly broad searches. By using location-based devices for surveillance, the government can observe every movement of an individual in real time, including location information unrelated to criminal activity. Thus, there are some good arguments that location monitoring is sufficiently similar to wiretapping that Congress should amend Title III to apply its stringent procedures to real-time tracking of someone's location over an extended period of time. In the meantime, however, as we explain below, we conclude that a probable cause warrant is necessary for government use of location devices, except when they are limited to tracking movement on the public highways.

Pen Register and Trap and Trace Device Orders

Pen registers and trap and trace devices are used to collect phone number information in real-time. A pen register collects the numbers dialed and related signaling information for outgoing calls, while a trap and trace device captures the originating number and related signaling information for incoming calls.

Courts have found that, in contrast to the *contents* of a telephone conversation, individuals have no "expectation of privacy" in the digits they dial on a telephone because such information is conveyed to telephone companies and routinely kept in company records for various business purposes.[65] Congress responded in the Electronic Communications Privacy Act of 1986 by requiring a court order for use of a pen register and trap and trace device. The standard, however, is very low. To obtain a pen register and trap and trace device order, the government needs merely to certify "the information likely to be obtained is relevant to an ongoing criminal investigation."[66]

Development of surveillance law

1967: Supreme Court extends Fourth Amend. to wiretapping and bugging.

1968: Congress adopts Title III, the Federal Wiretap Act.

1986: Electronic Communications Privacy Act (ECPA) extends Title III rules to cell phones and email in transit; stored email accorded lower protection.

1994: CALEA imposes design mandates on telephone companies; creates intermediate standard for some customer data; bars use of pen/traps for location.

2001: PATRIOT Act clarifies reach of pen /trap law; lowers standard for pen/traps in intelligence cases.

[65] The validity of this business records doctrine as applied to communications is being called into question, especially in light of the growing richness of communications transactional data. See Deirdre K. Mulligan, "Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act," 72 Geo. Wash. L. Rev. 1557 (Aug. 2004).

[66] 18 USC §§ 3122-3123. The pen register/trap and trace standard essentially reduces judges to mere rubber stamps. A judge *must* approve any request for a pen/trap order by law enforcement upon a mere certification of relevance, which is far lower than the probable cause required for searches under the Fourth Amendment. Investigators are not required to present any facts supporting their applications, nor is the judge required to determine whether the relevance standard has been satisfied. CDT has long argued that the standard for pen/trap devices should be increased to require a judicial finding of specific and articulable facts giving reason to believe that a crime has been, is being or is about to be committed and

In comparison to the kind of signaling information traditionally collected by pen registers and trap and trace devices, location surveillance reveals an entirely new category of information about the target that law enforcement cannot determine simply from phone numbers dialed. Accordingly, in CALEA, Congress made it clear that courts could not apply the pen/trap statute to the real-time monitoring of wireless location data, recognizing that the standard for a pen/trap order fails to address the intrusive nature of location tracking.[67]

As we discuss further below, in 2005 four magistrate judges issued opinions on the standard for government access to location information and all four concluded that the CALEA language meant that the pen register authority is not sufficient.

Search Warrant, Probable Cause

Absent special circumstances, under the Fourth Amendment, law enforcement officials must demonstrate to a judge probable cause of criminality in order to obtain a warrant to conduct a search. Courts will find that a particular intrusion or collection of information is a search or seizure if they conclude that the individual has a reasonable expectation of privacy in the place or information being examined by the government.

Courts require a search warrant based on probable cause for the government to install and monitor a tracking device that will monitor the movement of a person or object onto private property.

In *United States v. Knotts*, the Supreme Court held that no warrant was necessary to monitor a beeper installed by police on the outside of the defendant's car.[68] The Court stressed that the subject's movements were tracked only on the public roads. The Court concluded that traditional visual surveillance could have provided the same information that the police obtained by monitoring the beeper and that no reasonable expectation of privacy was infringed upon since the defendant "voluntarily conveyed [his course of travel] to anyone who wanted to look" by traveling on public roads.[69]

In contrast, in *United States v. Karo*, the Supreme Court held that the Fourth Amendment did require a warrant when the government installed a beeper in a container and used it to locate the container in a private residence.[70] The Court held that the monitoring of beeper signals from private enclosures to learn the location of objects constitutes a search under the Fourth Amendment.[71]

The *Karo* opinion has been read by federal and state courts as requiring a search warrant based on probable cause for the government to install and monitor a tracking device that will monitor the movement of a person or object onto private property.[72] Following the distinction between *Knotts* and *Karo*, no warrant is required where an electronic tracking device was attached to a car while in an individual's driveway and used to track him only on public highways.[73] Also, a warrant was not required where the beeper was placed in a mail pouch that the target later stole; the court held that the defendant had no reasonable expectation of privacy in the stolen mail pouch.[74] With these

that the surveillance will reveal information relevant to the investigation of that crime.

[67] 47 U.S.C. § 1002(a)(2).

[68] *United States v. Knotts*, 460 U.S. 276, 285 (1983).

[69] *Id.* at 281. See also *United States v. Forest*, 355 F.3d at 951 (finding no legitimate expectation of privacy in cell site data for Fourth Amendment purposes because it was used only to track defendant's movements on public highways).

[70] *United States v. Karo*, 468 U.S. 705, 714 (1984).

[71] *Id.* at 718.

[72] See *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747 (S.D. Tex. 2005), citing *United States v. Mixon*, 717 F. Supp. 1169 (E.D. La.), *aff'd*, 891 F.2d 904 (5th Cir. 1989); *In re Application for Tracking Devices on a White Ford Truck*, 155 F.R.D. 401, 403 (D. Mass. 1994); and J. Carr & P. Bellia, The Law Of Electronic Surveillance § 4:83, at 4-205 (West 2005). See also *U.S. v. Moran*, 349 F.Supp.2d 425 (N.Y. 2005) (holding that a warrant is not required to attach a GPS device to a person's car and use it only to track his movements on the public roads). For state cases, see *Washington v. Jackson*, 76 P.3d 217, 262 (Wash. 2003) (holding that the Washington state constitution requires a warrant before police may attach a GPS device to a car); *Oregon v. Campbell*, 759 P.2d 1040 (Ore. 1988) (requiring a warrant under the Oregon state constitution before police may attach a radio transmitter to an individual's car); *New York v. Lacey*, 3 Misc. 3d 1103A (N.Y. County Ct. 2004) (holding that the Fourth Amendment requires police to obtain a warrant prior to attaching a GPS to a suspect's car, and stating that with regard to manufacturer-installed GPS devices on vehicles, the prudent course would be to obtain a warrant prior to tracking such a device); see also *Johnson v. Florida*, 492 So. 2d 693, 694 (Fla. Dist. Ct. App. 1986) (finding that installation of second tracking device on an aircraft violated the Fourth Amendment when the relevant warrant authorized only one device); *Colorado v. Oates*, 698 P.2d 811 (Colo. 1985) (holding that installation of a beeper in a drum of chemicals purchased by the defendant was a search requiring a warrant under the Colorado state constitution).

[73] See *United States v. McIver*, 186 F.3d 1119 (9th Cir. 1999).

[74] See *United States v. Jones*, 31 F.3d 1304 (4th Cir. 1994). See also *United States v. Gbemisola*, 225 F.3d 753, 757-59 (D.C. Cir. 2000) (finding no Fourth Amendment violation when officers used beeper installed in a Federal Express package containing narcotics to track the individual who picked it up). On the other hand, another federal court suggested that GPS locators, which can both show real-time location and store "movements moment-

caveats, the majority rule is that if a government-planted device is going to be used to track a person or object into a place where there is a reasonable expectation of privacy, a warrant is required.

The question, then, is what should be the standard for government access to location data generated not by a device planted by the government, but a device owned by the target of the surveillance. If anything, the privacy interest should be greater. A cell phone clearly goes places where an individual has a reasonable expectation of privacy.

Until recently this issue had not been directly addressed in judicial decisions, and government agents were routinely obtaining orders for disclosure of cell site information on less than probable cause. However, in 2005 four federal magistrate judges addressed the issue in published opinions. Three ruled that a warrant is required for government agents to obtain real-time location information from service providers.[75] A fourth, stressing that his opinion applied only to cell site information at the beginning and ending of a call, and not to autonomous registration information generated between calls, nor to more precise data available from triangulation or GPS capabilities, ruled that a pen register order in combination with an order under 18 U.S.C § 2703(d) was sufficient.[76] We believe the decisions requiring a warrant are correct and should serve as the basis for a new approach to location information.

In one of the cases, arising in the Southern District of Texas, U.S. Magistrate Judge Stephen Smith began his careful parsing of federal surveillance statutes with the definition of "tracking device" in the Electronic Communications Privacy Act: "As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or thing."[77] Judge Smith concluded this definition fits a cell phone when it is used by law enforcement to track location. Judge Smith went on to conclude that cell site information is not content, and therefore not covered by the Wiretap Act. Nor, Judge Smith concluded, is cell site information covered by the Stored Communications Act. Judge Smith rejected a convoluted argument by which the government claimed a hybrid authority to get real-time cell site information using a combination of the pen register statute and Section 2703(d) in the Stored Communications Act. Only a warrant, Judge Smith held, is available for cell site information. Judge Smith concluded, "Denial of the government's request for prospective cell site data in this instance should have no dire consequences for law enforcement. This type of surveillance is unquestionably available upon a traditional probable cause showing ... . On the other hand, permitting surreptitious conversion of a cell phone into a tracking device without probable cause raises serious Fourth Amendment concern."[78]

Three federal magistrate judges ruled in 2005 that search warrants are required for real-time government access to cell phone location data – a high but not onerous standard.

"Reason to Believe" Under Section 2703(d)

As explained above in Chapter I, the Stored Communications Act governs the disclosure to government of stored records or other information pertaining to a customer of an electronic communication service.[79] To obtain transactional information from stored communications records (other than basic subscriber identifying information, which is subject to a lower standard), law enforcement officials must obtain a court order under 18 U.S.C. § 2703(d). That provision requires a government

by-moment for days, weeks, even years," might be subject to the Fourth Amendment when attached to a car even though less sophisticated beepers would not be. Ultimately, though, the court did not decide that issue. See *United States v. Berry*, 300 F. Supp. 2d 366, 368 (D. Md. 2004).

[75] In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747 (S.D. Tex. 2005); *In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005); and *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (Sealed) and Production of Real Time Cell Site Information*, 2005 *WL 3160860 (D. Md. Nov. 29, 2005). Several of the opinions, and other supporting materials, are online at www.eff.org/legal/cases/USA_v_PenRegister/.*

[76] In re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Tap and Trace, 05 Mag. 1763 (S.D.N.Y. Dec. 20, 2005).

[77] 18 U.S.C. 3117(b).

[78] In re Appplication for Pen Register and Trap/Trace Device with Cell Site Location Authority, Magistrate No. H-05-557M (S.D. Tex., Oct. 14, 2005), slip opinion at 30.

[79] 18 U.S.C. §§ 2702-2703.

official to offer "specific and articulable facts showing that there are reasonable grounds to believe that ... the information sought is relevant and material to an ongoing criminal investigation."[80]

The U.S. Justice Department, admitting that as a result of CALEA the pen register law is not sufficient authority for obtaining real-time access to cell phone location information, has argued that Section 2703(d) is the preferred source of such authority.[81]

Judge Smith held that this use of the Stored Communications Act to acquire real-time location information is inconsistent with the text, structure and legislative history of the Stored Communications Act. We agree. It is clear that the Stored Communications Act was intended to cover only the seizure of stored records. Use of the Stored Communications Act to acquire real-time, ongoing location information from cell phones (or other consumer devices) is also inconsistent with the Supreme Court decision in *Karo*, since modern cell phone location information permits real-time location of someone or something that is not in public view, and therefore requires a warrant.

Case law and statutes make a distinction between historical data and real-time data. The government is seeking to extinguish that distinction in a way that would open communications to government access without probable cause.

In contrast, federal Magistrate Judge Gabriel W. Gorenstein of the Southern District of New York held that Section 2703(d) does apply to disclosure of cellular location information. Judge Gorenstein based his decision on his conclusion that the cell site data "is not obtained by the Government directly but is instead transmitted from the provider digitally to a computer maintained by the Government. That is, the provider transmits to the Government the cell site data that is stored in the provider's system. The Government then uses a software program to translate that data into a usable spreadsheet."[82]

Judge Gorenstein's logic would destroy all distinction between real-time monitoring under Title III or the pen register statute, on the one hand, and access to stored records on the other hand. Almost always today, under Title III and the pen register statute, communications are not obtained by the government directly but are transmitted from the provider digitally to a computer maintained by the government. In many cases, those communications (such as email) and transactional data are stored in the provider's system. But as Mark Rasch has noted, "The law makes a distinction between historical data and real time data. That the government would seek to extinguish this distinction in this case does not bode well for the government's position in other cases. The government could then argue that it could listen in on your VOIP calls with nothing more than a subpoena (for which no probable cause is required) because all it is doing is looking at "historical" packets - albeit merely hundredths of a second in the past. This is clearly the opposite of the delicate balance Congress sought to strike."[83]

Despite our disagreement with Judge Gorenstein's reading of Section 2703(d), we believe he contributed an important observation to the debate over access to cell site information. Judge Gorenstein concluded that the pen register statute as currently written must be used as part of the process of obtaining cell phone location information. As a result of CALEA, a pen register order cannot be the sole authority for accessing cell site information – the government must have both a pen register order and some additional authority. Judge Gorenstein concluded that such additional authority could be found in Section 2703(d). As explained above, we believe Section 2703(d) is inapplicable and the additional authority must be

[80] 18 U.S.C. § 2703(d).

[81] U.S. Dep't of Justice, Computer Crime & Intellectual Property Section, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," § III.C.3 (July 2002) (indicating that "cell site data for cellular telephone calls" is covered by Section 2703(d)), www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm; "Memorandum Opinion Issued By Department of Justice Concludes that Commission's Recently Adopted Wireless Enhanced 911 Rules are Consistent with Wiretap Act," FCC Public Notice, CC Docket No. 94-102 (Dec. 10, 1996) ("Section 2703 . . . applies to a carrier's transmission of location information"), www.fcc.gov/Bureaus/Common_Carrier/Public_Notices/1996/da962067.txt; Al Gidari, "Locating Criminals by the Book," Cellular Business at 70 (June 1996).

[82] *In re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Tap and Trace*, 05 Mag. 1763 (S.D.N.Y. Dec. 20, 2005), slip opinion at p. 4.

[83] Mark Rasch, "Tracked by cellphone," The Register (Dec. 22, 2005) www.theregister.co.uk/2005/12/22/tracked_by_mobile_phone/.

a search warrant. However, as Judge Gorenstein noted, the pen register statute includes important protections, notably a time limitation on the duration of the surveillance and a sealing requirement. And the reality is that the government almost always will want the additional information about dialed numbers that it can obtain only with a pen register order. In practice, in almost all cases where the government is seeking real-time location information associated with calls, it is also seeking other transactional data about those calls, most especially the dialed number information and the time and duration of the call. Combining a search warrant with a pen register order reconciles the pen register statute, the Stored Communications Act, and the limiting language in 47 U.S.C. § 1002.

One additional point: It is unclear whether Section 2703 applies to the gathering of *stored* location information from cellular phone providers[84] or from operators of car navigation systems.[85] Given the precision of new location functions in cell phones and other devices and their capabilities for long-term storage, we believe the warrant standard should apply not only to real-time monitoring of location information but also to the retrospective acquisition of location information by the government and that Congress should accordingly adopt such a rule.

Subpoenas

All of four of the magistrate judges' decisions in 2005 concerned access to location data in real-time. It is somewhat unclear what standard should apply to access to stored location data. At a minimum under current law, it should be Section 2703(d).

However, if Magistrate Judge Smith is correct, and Section 2703(d) does not apply to cell phone location data even in storage, then it is unclear what standard would apply. As a matter of policy, the low standards for issuance and execution of subpoenas are woefully inadequate to protect privacy given the sensitivity of location information and the great detail it can reveal about an individual if analyzed over time. The only limits on issuance of grand jury subpoenas are that they must seek relevant information and not be overbroad. No probable cause showing or court approval is required. Once served with a subpoena ordering disclosure of its records, a company must either comply with the subpoena or initiate court proceedings to vacate or modify it. The company is not required to notify its customer that his records are being sought by the government. And a company has little incentive to challenge a grand jury subpoena for customer data.

This gap in the law needs to be addressed, either by judicial interpretation or by Congress setting a minimum probable cause requirement for all government access to stored location information covering an individual's movements over a period of time. In this regard, it is important to note that Magistrate Judge Smith, in his opinion on real-time tracking, concluded that *Smith v. Maryland* did not apply to cell site information, because cell site information is unlike other business records, in that it is not voluntarily conveyed by the user to the phone company, but rather is automatically transmitted, independent of the user's input, knowledge, or control.

The standard for government access to stored location information is unclear.

CONCLUSION

The type of location tracking possible in the twenty-first century is quite different from anything previously available to government agents. Through the use of location-based technologies, the government has the capacity to track the movements of individuals over long periods of time to a degree that is qualitatively different from traditional methods of visual surveillance. Under current law, the rules for location tracking are both

[84] Section 2703 only covers providers of electronic communication services, which, as Judge Smith noted in his decision on real-time tracking, is defined in the statute to exclude tracking devices. 18 U.S.C. § 2510(12)(C). A tracking device is broadly defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b).

[85] *In re Application of the U.S. for an Order Authorizing Roving Interception,* 349 F.3d 1132 (9th Cir. 2003) has an inconclusive discussion of the question.

ambiguous and inconsistent. The lack of definite guidelines as well as the covert nature of location tracking affords government agents an undesirable amount of discretion.

As some courts have recognized, in contrast to older electronic beepers, the use of modern location tracking devices does more than merely augment visual surveillance capabilities, "but rather provides a technological substitute for traditional visual tracking."[86] There is a critical difference between "the kind of uninterrupted, 24-hour a day surveillance possible through use of a GPS device" and mere sense-enhancement devices like binoculars or flashlights, which do not enable law enforcement agents to determine what occurred in the past.[87] With traditional methods of visual surveillance, the limited capacity of law enforcement to physically follow individuals' movements acted as a natural check against abuse. Concern about detection by the target restrained police from maintaining tight, continuous surveillance. By enabling police to monitor location information precisely and remotely, however, advanced location-tracking technologies have eliminated any meaningful physical or financial constraints on government surveillance.

Recommendation:

Courts and the Congress should adopt a single probable cause standard for all government access to location information showing a person's movements over time, whether collected by a government-installed device or a consumer service.

Based on a review of standards applicable to various types of government surveillance, we conclude that a probable cause warrant, with a temporal limitation, is the appropriate standard for government acquisition of location information. The very low standards for subpoenas and for pen registers and trap and trace devices are inadequate for the sensitive nature of location information, as is the intermediate standard of Section 2703(d). For location monitoring, a basic probable cause requirement with limits on the duration of the surveillance would safeguard location privacy against unjustified or overbroad searches without denying government agencies the use of an important investigative technique.

The same probable cause standard should apply regardless of whether law enforcement is monitoring location via a consumer device or a law enforcement-installed device. Although cell phone and car navigation service users understand that their service providers may be able to access their location information for purposes of supplying those services, they do not expect that information to be passed on to law enforcement absent appropriate legal compulsion.

Moreover, given the possibility for long-term storage of detailed retrospective location data, we believe that a probable cause standard should also be applied to stored location information obtained from third party providers, such as cellular phone companies and car navigation system companies. Viewing an individual's movements over a long period of time, even if done after the fact, can reveal sensitive and detailed information about the individual's activities and associations. A probable cause standard is appropriate in those circumstances.

[86] *Washington v. Jackson*, 76 P.3d at 262.

[87] *Id.* See also *Berry*, 300 F. Supp. 2d at 368 (reasoning that GPS locators, unlike beepers, do not just aid police in tailing a car they are already following; they substitute entirely for the personnel necessary to follow a car in real time and therefore might require a probable cause search warrant to be used).

Chapter III

Keystroke Loggers:

Government Spyware

Keystroke loggers are computer programs that record every letter and command typed – every keystroke – on a computer. The programs have legitimate uses, such as monitoring productivity in the workplace. However, in the hands of government agents, their use well illustrates the widening gap between privacy protections and the growing potential of surveillance tools available to the government. Many Internet users have recently become concerned about remotely installed "spyware" programs, which can become embedded in their computers and track their activities online, whether to send advertising or to steal sensitive information. Keystroke loggers, when installed by government agents to monitor computer use, are essentially government spyware. Under current law, to install keystroke loggers surreptitiously, whether remotely or by physically accessing the target's computer, agents have to obtain so-called "sneak and peek" search warrants.

In some ways, keystroke loggers are even more intrusive than the interception of phone or e-mail communications – they record information not intended to be conveyed to any third party.

However, keystroke loggers are not only secretive, they also represent an ongoing surveillance, and a prying into a person's very thoughts, that are far more intrusive than an ordinary search. In this chapter, we argue that a mere warrant is not enough and that Congress or the courts should apply additional protections to keystroke loggers.

Once installed, keystroke loggers enable the government to record information entered into a computer within the sanctity of one's home and to access a person's most private matters, including letters, diary entries, e-mails, and financial information, whether conveyed to a third party or not. Thus, in some ways, keystroke loggers are even more intrusive than the interception of phone or e-mail communications. In addition to implicating privacy concerns, electronic surveillance tools, if implemented without appropriate rules and safeguards, may chill free speech. Fear that the government might secretly be monitoring computer use may lead individuals to become overly cautious about what they write in e-mails or other personal files kept on their computers.

A 2001 case opened a window on the government's use of keystroke loggers in criminal investigations.

Such fears may be heightened because governmental agencies have disclosed little information about keystroke loggers, citing the desire to protect law enforcement and national security interests. While CDT recognizes the compelling need to take preventative measures against terrorism and to investigate criminal activity, full disclosure and open debate about the government's use of invasive surveillance technologies is crucial for oversight and accountability.

In this chapter, we:

- describe how keystroke logging operates;
- examine the privacy concerns raised by different types of keystroke loggers;
- identify gaps in the current law that fail to clearly safeguard against the abuse of keystroke loggers by the government; and
- consider what legal standard would better protect privacy when the government uses keystroke loggers.

WHAT IS KEYSTROKE LOGGING TECHNOLOGY AND HOW DOES IT WORK?

A keystroke logging program is a computer software application that captures every keystroke a user enters into a computer. Most keystroke loggers also record the name of the application with which the keystrokes are associated and the time and date the application was opened. These programs are commonly used for relatively benign purposes to detect sources of error in computer systems, as a means for companies to assess their employees' work habits, and as a parental control device to monitor children's Internet use. Loggers can also be used, however, to obtain passphrases to encryption programs, in order to decrypt computer files or messages scrambled by the user.[88]

Unsurprisingly, the government has explored the potential of keystroke loggers as a surveillance method. By recording the passwords used to encrypt data, a keystroke logger permits law enforcement to access the content of otherwise indecipherable documents without having to crack the encryption through traditional decoding techniques. Keystroke loggers can be physically installed on a computer or they can be remotely installed without obtaining physical access to the computer.

Little is known about the development and use of keystroke logging surveillance by the government. One of the few publicly known instances of government use of keystroke loggers surfaced in 2001 with the first court decision to deal with this new method of surveillance, *United States v. Scarfo*.[89] In *Scarfo*, a keystroke logger was installed when the FBI broke into the target's office and

[88] In June 2003, the anti-virus and anti-spam software vendor Sophos reported that the W32/Bugbear-B virus contains a keystroke logger that allows confidential information, including passwords and credit card numbers, to be stolen from infected computers. When users who have been hit by the virus log onto password-protected websites – such as online banks or e-commerce sites – their passwords and account details are secretly stored. Robert Vamosi, "Bugbear.b is on the prowl" (June 5, 2003) http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2913939,00.html

[89] *United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001).

obtained physical access to his computer. Following increased press attention in response to *Scarfo*, the FBI acknowledged that it had developed an even more sophisticated type of keystroke logger code-named Magic Lantern.[90] According to press reports, Magic Lantern can be remotely installed on a computer via e-mail containing a virus disguised as a harmless computer file, known as a "Trojan horse" program, or through other common vulnerabilities hackers use to break into computers. Keystrokes recorded by Magic Lantern can be stored to be seized later in a raid or can even be transmitted back to the FBI over the Internet.[91] Law enforcement agencies will likely continue to develop enhanced methods of remote installation that are harder to detect.

PRIVACY CONCERNS RAISED BY KEYSTROKE LOGGING SURVEILLANCE

With keystroke logging surveillance, the government can obtain access to a complete picture of what people are doing on their computers. As computers have increasingly become a fundamental part of our daily lives, our privacy interest in what we type into those computers also has heightened. Computers are used to store financial records, diary entries, medical information, and wills. They include drafts of letters never sent and other information never intended to be shared with anyone. People communicate via Instant Messenger programs without storing the contents of those communications on their computers at all. Keystroke loggers place the full content of such highly confidential data within the reach of government investigators. And they do so without safeguards appropriate to this type of surveillance.

In comparison to standard methods of accessing computer evidence, keystroke logging programs are especially intrusive because they are installed and operated without contemporaneous notice to the person whose files are being seized. (A normal search and seizure requires notice at the time of the search.) They can record documents and messages that individuals choose to delete or never send, thereby allowing the government to view the inner thoughts of its surveillance targets, even those thoughts that have been abandoned. As an ongoing interception of an individual's complete computer usage, keystroke logging is like a wiretap and if anything is more intrusive, for it captures drafts never communicated to anyone. Keystroke loggers may capture communications, documents and drafts that are not relevant to the criminal investigation. The authority for installation, a sneak and peek search warrant, is controversial because, among other reasons, it is available in virtually any case.[92]

Depending on how it is used, the technology also could capture information from individuals other than the target. Many personal computers located in homes and businesses are used by multiple people. Keystroke loggers could be installed on public computers at libraries or Internet cafes.[93] Until

In contrast to a normal search and seizure of one's papers or computer files, keystroke logging occurs without notice.

[90] Ted Bridis, "FBI Is Building a 'Magic Lantern'; Software Would Allow Agency to Monitor Computer Use," Washington Post, A15 (Nov. 23, 2001).

[91] In order to send Magic Lantern or a similar keystroke logger as a virus, the FBI may have to secure the cooperation of anti-virus software companies to ensure that their programs will not identify and destroy the virus carrying Magic Lantern. The FBI would have to provide a sample of code for anti-virus vendors to know what to overlook. Any holes left open for a keystroke logger could also be exploited by hackers. McAfee Corporation came under criticism after a source at Network Associates told the Associated Press that the company had contacted the FBI "to ensure its software wouldn't inadvertently detect the bureau's snooping software and alert a criminal suspect," leading other major anti-virus vendors to assure consumers that they will scan for all viruses, regardless of their source, unless ordered not to do so by the courts. "FBI 'Fesses Up to Net Spy App," Wired News (Dec. 12, 2001), www.wired.com/news/conflict/0,2100,49102,00.html; Robert Vamosi, "Warning: We know what you're typing (and so does the FBI)," ZD Net (Dec. 5, 2001), http://reviews-zdnet.com.com/4520-6033_16-4206694.html.

[92] If the government uses a sneak and peek warrant under the criminal rules, it would eventually be required to notify the individual that it had broken into her home or office. 18 U.S.C. § 3103a(b)(3). If the government obtained a warrant for a secret installation of a keystroke logger pursuant to the Foreign Intelligence Surveillance Act, however, notice would never be required unless evidence gathered using the keystroke logger was used against the individual in a criminal proceeding. 50 U.S.C. § 1825(b), (d).

[93] In 2003, an individual placed keystroke loggers on computers at various New York City Kinko's to obtain peoples' banking passwords. Anick Jesdanun, "Kinko's spy case highlights risks of public Internet terminals," Detroit News (July 23, 2003), www.detnews.com/2003/technology/0307/23/technology-224836.htm. Internet Explorer and anti-virus software were unprepared for two recent keystroke loggers, while a third targeted bank accounts. David Berlind, "Keystroke Loggers Must Send Microsoft Back to Firewall Drawing Board," ZDNet (July 1, 2005), http://techupdate.zdnet.com/techupdate/stories/main/microsoft_firewall.html. Virus experts recommend that people using the Internet from cafes or other public-access computers be very careful in accessing bank accounts and

None of the existing laws are directly responsive to the unique features of keystroke logging when used by the government.

they closely examine the entire stream captured from a multiple-user computer, law enforcement officers have no way of determining which captured keystrokes the surveillance target entered. In other contexts where such overbroad collection is likely to occur, such as payphones or phones in a home or business, the wiretap laws require trained personnel to minimize, in real-time, the recording of innocent conversations, to protect against abuse. As discussed below, such procedures are appropriate here as well but are not explicitly required under current statutes (although, as we argue below, they very well may be constitutionally compelled).

EXISTING LAWS FAIL TO PROVIDE ADEQUATE SAFEGUARDS AGAINST ABUSE OF KEYSTROKE LOGGERS

The use of keystroke loggers raises privacy concerns not contemplated by the current legal standards courts apply to determine whether a search has been conducted in a lawful manner. None of the existing laws are directly responsive to the technology's unique features; they all fail to address some of the most egregious privacy invasions that could result from this method of surveillance. While, at a minimum, the Fourth Amendment's basic search warrant requirement clearly applies to surveillance conducted with a keystroke logger, courts have not yet properly applied the Fourth Amendment's particularity and other requirements to limit the use of keystroke loggers in criminal investigations.[94]

At a minimum, the Fourth Amendment requires a court order based on probable cause before the government can install and monitor a keystroke logger.

In the *Scarfo* case, the only court to rule so far on government use of keystroke loggers held that law enforcement officers do not have to obtain a wiretap order before installing a keystroke logger on a targeted computer. In *Scarfo*, where the FBI had obtained a search warrant to enter the target's office and physically install the keystroke monitor, the court denied a challenge to the introduction of evidence.[95] The court failed to recognize that keystroke logging surveillance involves a level of intrusiveness not addressed by an ordinary search warrant but rather is closer to, and in some ways even more intrusive than, a wiretap and therefore should be subject to enhanced protections.

To understand why currently-applied standards are inadequate, it is necessary to explore the two basic levels of protection for searches of one's home and communications: baseline search warrant protections, and stricter requirements in the wiretap laws for the ongoing, real-time interception of voice and electronic communications.

Search Warrants

Under the Fourth Amendment, law enforcement officials must demonstrate probable cause of criminality to obtain a warrant to conduct a search. A search warrant must describe with particularity the place to be searched, and the persons or things to be seized, in such a manner that it leaves little to the discretion of the officer executing the warrant. The particularity requirement exists to constrain law enforcement officers from undertaking a boundless and exploratory rummaging through one's personal property.

In *Scarfo*, the FBI had obtained a sneak and peek (also called delayed notification) search warrant, which authorizes police to physically enter into private premises to conduct a search without the knowledge of the owner or the occupant and to provide notification only after the fact.[96] At a minimum, a Fourth Amendment search warrant would be required if the keystroke logger were installed remotely without physically entering the home or business where the computer is located.

double check that the PC they are using has an updated anti-virus software. "Kinko's Keystroke Caper Underscores Need for Diligence" (July 23, 2003) www.bankersonline.com/technology/techalert_072303.html.

[94] See Daniel J. Solove, "Reconstructing Electronic Surveillance Law," 72 Geo. Wash. L. Rev. 1264, 1294 (2004).

[95] *Scarfo*, 180 F. Supp. 2d at 583.

[96] Broad authority for this type of search warrant was codified by the USA PATRIOT Act at 18 U.S.C. § 3103a(b), and has since become quite controversial. CDT has consistently argued that sneak and peek is a departure from fundamental Fourth Amendment principles and, if ever permissible, should be authorized under narrower standards than those in the PATRIOT Act.

Because the Fourth Amendment "protects people, not places," the Supreme Court made clear many years ago in *Katz v. United States* that a search occurs even if there is no physical trespass.[97] More recently, relying on *Katz*, the Supreme Court in *Kyllo v. United States* concluded that where the government "uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[98] Given the strong presumption of an expectation of privacy in the keystrokes entered into one's computer, the Fourth Amendment certainly applies to the use of keystroke loggers, and the legal standard should be the same regardless of whether the keystroke logger is installed on-site or remotely.

However, keystroke loggers are different in crucial ways from an ordinary search. They perform the electronic equivalent of general searches. Yet in *Scarfo*, the court held that use of the keystroke logger did not constitute an unlawful general search, even though it recorded every keystroke typed.

Traditional search warrants are normally executed at a specified time and place and are limited to a search for specified items. Previously disposed of or destroyed items obviously cannot be subject to seizure. Nor does a search warrant permit ongoing surveillance. In contrast, keystroke loggers can record even deleted communications. And they entail an ongoing search, over a period of days, weeks or longer. Keystroke logger surveillance essentially amounts to police gathering all documents, whether or not listed in the warrant, and sifting through them all, staying in one's office or home, day after day as normal activity goes on. Surveillance with keystroke loggers is too pervasive and ongoing to be aptly addressed by procedures suited to a simple search.

There is one way in which a keystroke logger could be used that is closer to standard searches: the logging program could be configured to operate only on a particular application and to seek only to capture a specific category of information – for example, a password. Judges reviewing search warrant requests that would involve use of a keystroke logger should inquire into the capability of the technology and should, at a minimum, require in the warrant that the keystroke logger be configured to minimize the number of irrelevant keystrokes captured, perhaps by limiting keystrokes recorded based on the application that the target is using.[99]

Wiretap Orders

Unless the keystroke logger is specifically programmed to capture only a limited amount of information, the installation and use of a keystroke logger is closer to a wiretap than it is to an ordinary search. In very important ways, ongoing surveillance has always posed greater threats to privacy than the physical searches and seizures that the Fourth Amendment was originally intended to cover.

Keystroke loggers, like wiretaps, involve ongoing, surreptitious monitoring.

Keystroke loggers are like other methods of electronic surveillance in that their usefulness depends on lack of notice to the suspect. In the execution of the traditional search warrant, an announcement of authority and purpose ("knock and notice") is required so that the person whose privacy is being invaded can observe any violation in the scope or conduct of the search and immediately seek a judicial order to halt or remedy any violations.

Electronic surveillance involves an ongoing intrusion in a protected sphere, unlike the traditional search warrant, which authorizes only one intrusion, not a series or continuous surveillance. Officers must execute a traditional search warrant with dispatch, not over a prolonged period of time; if they do not find what they were looking for in a home or office, they must leave promptly and must

[97] *Katz v. United States*, 389 U.S. 347, 361 (1967).

[98] *Kyllo v. United States*, 533 U.S. 27, 40 (2001).

[99] Several keystroke logging programs, including PC Tattletale, Spector Pro and IamBigBrother, categorize keystrokes captured by the application into which they were entered. Laura Delaney, "Monitoring Software," PC Magazine (Aug. 3, 2004), www.pcmag.com/article2/0,1759,1619184,00.asp. Other programs, such as Perfect Keylogger Lite, may be configured to limit logging to specific programs or windows. See www.snapfiles.com/get/perfectkl.html.

obtain a separate order if they wish to return to search again. Electronic surveillance, in contrast, may go on around-the-clock for days or months.

In response to the uniquely intrusive aspects of electronic surveillance, the Supreme Court in 1967 imposed additional Fourth Amendment requirements on electronic surveillance.[100] A year later, Congress implemented those requirements by enacting the federal wiretap law, which imposes special privacy protections on electronic surveillance to comply with the Fourth Amendment: wiretaps are available only for the most serious cases; authorization to conduct a tap is issued only when all other investigative techniques have failed; applications are subject to rigorous judicial scrutiny; wiretaps are conducted in such a manner as to minimize the interception of innocent conversations; and parties whose conversations are intercepted are entitled to obtain after-the-fact judicial review of the authorization and conduct of wiretaps.[101] For example, the wiretap laws require that all persons named in a wiretap application receive notice that a wiretap was executed "within a reasonable time but not later than ninety days" after the expiration of the order, regardless of whether or not incriminating statements were made or criminal charges were filed.[102] The wiretap laws apply both to voice communications face-to-face or over a phone and to electronic communications such as e-mail or other computer-to-computer transmissions.

The privacy concerns underlying the Supreme Court's strict interpretation of the Fourth Amendment requirements for purposes of electronic surveillance and Congress's intent in subjecting law enforcement to wiretap laws arise with equal force in the context of keystroke logging surveillance. Thus, the strong protections against abuse provided by wiretap laws should be extended to the use of keystroke loggers – indeed, they may be constitutionally required.

[100] *Berger v. New York*, 388 U.S. 41 (1967).

[101] 18 U.S.C. § 2518.

[102] 18 U.S.C. § 2518(8)(d); *United States v. Donovan*, 429 U.S. 413, 439 n.26 (1977).

According to the district court's holding in *Scarfo*, the more stringent protections of the federal wiretap laws were not applicable to the keystroke logger surveillance at issue because the logger did not record keystrokes entered into the computer while the modem was operational. The court's decision was based on the fact that the wiretap laws cover communications, not data stored on the hard drive of a personal computer. In *Scarfo*, the FBI had configured the keystroke logger not to record while the modem was in use, specifically to prevent the interception of any electronic communications.

The court in *Scarfo* erred in two respects. First, it failed to account for the recording of keystrokes that compose documents to be sent later as e-mail or as attachments to e-mail messages. There is no rational basis for according a higher level of protection to communications contained in an e-mail at the moment of transmission over the Internet than to the very same message while it is being composed. A person's expectation of privacy regarding that communication remains the same. If anything, the privacy interests implicated by accessing keystrokes that have yet to be conveyed to a third party should be higher.[103] Second, the *Scarfo* court disregarded the constitutional problem of allowing precisely the type of general search that the Supreme Court attempted to prevent when it imposed strict requirements on wiretaps and bugs, including minimization requirements. A keystroke logger effectively facilitates government access to the inner thoughts of its surveillance target, even those thoughts that have been abandoned (that is, deleted), and even those thoughts entirely irrelevant to the investigation.

[103] In October 2004, a federal judge in California dismissed criminal charges under the Wiretap Act against a company employee who installed a keystroke logger on another employee's computer. The court held that interception of a transmission between a keyboard and a computer's processing unit was not covered by the Wiretap Act because a personal computer is not a system affecting interstate commerce, as required by the statute, regardless of whether the computer is connected to the Internet or another network and regardless of whether the logger captures e-mails being composed on the computer. *United States v. Ropp*, Cr. No. 04-3000-GAF (C.D. Cal., Oct 8, 2004) (unpublished). In our view, the case contains a cramped interpretation of the statute. It is inconsistent with the premise in *Scarfo* that keystroke loggers should not be used to capture emails without a Title III order when a computer is connected to the Internet. It is also inconsistent with longstanding understanding that computers connected to the Internet are in interstate commerce.

Accordingly, Congress should unambiguously extend the privacy protections of the wiretap laws to keystroke logging surveillance. Until Congress does so, judges should impose additional requirements when authorizing the installation and monitoring of keystroke loggers to ensure the Fourth Amendment has been satisfied.

RECOMMENDATION: A MORE SUITABLE APPROACH TO KEYSTROKE LOGGERS

For these reasons, CDT believes that the federal wiretap law should be amended to extend its special protections to the installation and use of keystroke loggers. This could be accomplished by a single amendment making it clear that an electronic communication includes the entry of information into a computer. Suggested language is set forth in the Appendix. A similar amendment to the Foreign Intelligence Surveillance Act would make comparable improvements in the use of keystroke loggers in foreign intelligence investigations.

Until such a statutory reform is made by Congress, judges considering search warrant applications for installation and use of keystroke loggers should use Fourth Amendment principles to impose strict limits on the use of keystroke loggers. To enforce the Fourth Amendment's particularity requirement, judges should require where technically possible that the logger be configured to capture only information specified by the government as relevant to the investigation. Judges should in all cases require strict minimization procedures to ensure that only the information authorized for surveillance is retained and reviewed by the investigating law enforcement officers. Judges should put time limits on the use of the loggers, and should require detailed and frequent reports on the execution of searches that show what is being captured, to enable judges to monitor the scope of searches and to call them to a halt as soon as the information being sought is obtained or it appears there is no such information. Only with these additional protections will the use of keystroke loggers satisfy the Fourth Amendment.

Use of Keystroke Logger Evidence at Trial

When evidence gathered using keystroke logger technology is used in a criminal prosecution, information about the technology should be made available to the defendant. In *Scarfo*, the government successfully argued that disclosure of information about the technology would jeopardize domestic criminal investigations and national security interests, and that it had a right to keep information on how the keystroke logger operated classified under the Classified Information Procedures Act (CIPA). The court limited the scope of discovery to granting the defendant an unclassified summary about the keystroke logger written by an FBI agent, which simply stated that keystrokes were not recorded while the modem was operational, without providing any evidence to substantiate that assertion.[104]

This level of secrecy seems unjustified when keystroke technology is essentially commercial in nature: the capabilities available to the government are not significantly different from those in legitimate, commercially available keystroke monitors or in less legitimate but still publicly available spyware. The adversarial process is an essential aspect of oversight with regard to how surveillance is conducted. Judicial control of keystroke logger surveillance will be ineffective unless normal discovery is available to support challenges to abuse of keystroke logging surveillance. As discussed earlier, the way a keystroke logger is configured has substantial implications for Fourth Amendment concerns. Without the ability to understand the way the surveillance tool was used, if necessary in a classified setting with appropriate security clearances for defense counsel, the defense has no means of verifying whether or not the search was conducted in compliance with limits protecting the privacy interests of the surveillance target.

Installation and use of keystroke loggers should be regulated under the wiretap act, with its additional protections.

[104] *Scarfo*, 180 F. Supp. 2d at 582-83.

Until Congress acts, judges approving government applications for use of keystroke loggers should impose tight controls.

CONCLUSION: NEW LEGAL PROTECTIONS AGAINST PRIVACY INTRUSION ARE NEEDED

New technologies like keystroke logging surveillance enhance the ability of law enforcement to acquire intimate details of our activities and thoughts. Used appropriately, they can be important tools in the law enforcement arsenal. However, the uses of these powerful surveillance technologies often outpace the law in ways that threaten privacy. As technology enhances surveillance capabilities, the legal standards for government use of these new technologies must evolve to adequately protect privacy.

The current statutory framework fails to provide concrete guidelines for the application of existing law to new surveillance technologies. Vital questions about the government's use of keystroke loggers remain unanswered. How often is keystroke logging surveillance employed and under what circumstances? Are judges carefully overseeing how the devices are being used? Mere FBI assurance that it will comply with all existing privacy laws when employing keystroke loggers does not alleviate concerns about governmental intrusion on privacy interests, since existing standards do not explicitly address the intrusive potential of these new surveillance technologies.

Keystroke logger surveillance should not be used without sufficient safeguards against abuse and mechanisms for oversight. At a minimum, installation and use of keystroke loggers requires a search warrant. However, to fully satisfy the Fourth Amendment, rules that address the unusually intrusive aspects of keystroke logging technology are needed. Statutory changes would create a clear set of rules. In the absence of legislative action, judges issuing warrants for keystroke loggers should understand the capabilities of the technology and should require where technically possible that the logger be configured to capture only particularly described information. Where such minimization before the fact is not possible, judges should require that it be done afterward so that irrelevant information is not retained and reviewed by prosecutors. Judges also should require regular, even daily, reports on what is being captured, and they should ensure that the surveillance is terminated as soon as the information specified in the warrant is acquired or it becomes apparent that there is no such information to be had. To institutionalize such protections, Congress should amend the Wiretap Act to extend its full protections to the use of keystroke loggers by governmental agencies, and should require regular reporting on the frequency of government use of keystroke loggers.

Conclusion

The Internet has already demonstrated its potential to promote democratic values, spur economic activity, support innovation, and enhance human development. Individuals, businesses and governments are all rushing to use the Internet for work, politics, education, social services, human contact, artistic expression and commerce. The Internet has become a necessity in most workplaces and a fixture in most schools and libraries. With wireless devices, it is becoming nearly ubiquitous.

Information and communication technologies have been changing so rapidly that they have outstripped Constitutional interpretations and privacy laws. The leading judicial decisions and federal statutes on privacy date from the 1970s and 1980s, before the rise of the Internet and the explosion of digital technology. Remarkably, the Electronic Communications Privacy Act of 1986 was the last time privacy standards were comprehensively strengthened. Astonishing and unanticipated changes have occurred since. In his recent book, "Active Liberty," Supreme Court Justice Stephen Breyer finds that "advancing technology has made the protective effects of present law uncertain, unpredictable, and incomplete."

Other technologies beyond those discussed here are eroding privacy in ways that require a policy response.

While the government frequently emphasizes the ways in which digital technologies pose new challenges to law enforcement, the fact is that, on balance, the digital revolution has been a boon to government surveillance and information collection. More information is more readily available to government investigators than ever before. In the PATRIOT Act, Congress focused exclusively on the ways in which the laws had to be updated to take account of the government's needs in the face of technological change. It is time to address the opposite side of the coin and re-establish privacy protections that have been eroded by the development of technology.

The issue is not about trying to limit innovation. All of the technologies that we examined here have legitimate uses. They afford convenience, support new lines of business and even enhance security. Their deployment should be applauded.

Nor is the issue about denying any authority to the government. Especially in the face of terrorism, the government needs the authority to monitor advanced communications technologies. The concern is with assuring that new surveillance capabilities are subject to appropriate checks and balances.

This report addresses three areas in which the privacy laws have not kept pace with technology:

- **Online storage:** Increasingly, private information is stored on networks rather than in the home or office, yet strong privacy protections have not been applied to information stored online. Congress (and the courts) should provide enhanced protection for information on networks, by requiring probable cause for seizure without prior notice, and a meaningful opportunity to object to subpoenas in both civil and criminal cases.
- **Location tracking:** Today tens of millions of Americans are carrying (or driving) mobile devices that could be used to create a detailed dossier of their movements over time – without an appropriate legal standard for government access. For government access to wireless location information, the law should require, in the absence of the consent of the individual, that a judge find probable cause to believe that a crime has been, is being or is about to be committed.
- **Keystroke logging:** Computer programs can be installed in a computer, surreptitiously and even remotely, that record every single keystroke typed by a user, collecting not only communications but also purely private thoughts. Government installation and use of keystroke loggers should be authorized only pursuant to a wiretap order, issued by a judge.

This is not a comprehensive review of issues that need to be addressed in order to keep privacy protections current with technology changes. CDT has previously noted other concerns, especially the need to adopt a meaningful standard for use of pen registers and trap and trace devices, which collect transactional data about voice and data communications, showing who is talking to whom. The current standard is minimal – judges must rubber stamp any government application presented to them. A more appropriate standard would require a judge to find that specific facts reasonably indicate criminal activity and that the information to be collected is relevant to the investigation of such conduct. There are other ways in which the surveillance laws should be improved to protect privacy in the face of the increasing power of technology, and new ones will emerge as technology continues to develop in unanticipated ways.

The three issues we raise here represent clear and immediate threats to privacy. With adequate checks and balances, the interests of industry, the government and private citizens can be accommodated.

For more information, contact James X. Dempsey or Ari Schwartz, (202) 637-9800.

CENTER FOR
DEMOCRACY
&
TECHNOLOGY

1634 EYE STREET, NW SUITE 1100
WASHINGTON, DC 20006
TEL 202.637.9800
FAX 202.637.0968
WWW.CDT.ORG