Digital Technology Makes Surveillance Easier, Requiring Stronger Privacy Laws

February 22, 2006
Tags: Array
Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

Against the backdrop of debate over warrantless wiretaps and Administration calls to amend the Foreign Intelligence Surveillance Act, CDT today released a report about how privacy law has failed to keep pace with technology. The report, entitled "Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology," calls for an in-depth Congressional review of the ways digital technology makes government surveillance easier and more intrusive.

(1) CDT Report Finds Changing Technology Makes Government Surveillance More Intrusive

Against the backdrop of debate over warrantless wiretaps and Administration calls to amend the Foreign Intelligence Surveillance Act, CDT today released a report about how privacy law has failed to keep pace with technology. The report, entitled "Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology," calls for an in-depth Congressional review of the ways digital technology makes government surveillance easier and more intrusive.

CDT's report focuses on three developments:

- **Online storage**: Personal information that people used to keep in paper files or on computer hard-drives is increasingly stored online, beyond the physical confines of the home or office.
- **Location technologies**: Cell phones, car navigation services and other communications devices can provide increasingly precise location information.
- **Keystroke loggers**: Programs known as "keystroke loggers" record all information typed into a computer and can be installed surreptitiously, even remotely.

Every day, Americans use the Internet and wireless services to create, access, transfer and store vast amounts of private data. More and more of our lives are conducted online and more of our personal information is transmitted and stored electronically. 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.

The report argues that, under current privacy rules, this personal information receives inadequate protection against government intrusion. Personal information held by service providers is accessible to the government under weak standards based on outdated Supreme Court decisions and statutes written before the World Wide Web even existed.

CDT calls on the courts, Congress and technology companies to respond. The Internet and communications industry, public interest groups and the government need to enter into a dialogue

to find the proper balance that will ensure that the fundamental right of privacy is protected as technology changes.

"Digital Search and Seizure: Updating Privacy Protections to Keep Pace with Technology" [1] [pdf] (Feb, 2006).

(2) Expanded Online Storage Raises Privacy Issues

Many online services -- ranging from email to online calendars to the storage of voice telephone calls made possible by Voice over Internet Protocol technology -- provide volumes of storage capacity that were unimaginable twenty years ago when current privacy laws were drafted. Although leading service providers promise consumers relatively strong protections in their privacy policies and adhere to those promises in commercial contexts, privacy policies have exceptions for government demands and the rules for government access are often weak.

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

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.

CDT questions whether this "business records doctrine" is still constitutionally sound, given the revealing nature of the huge amounts of transactional data generated by electronic systems today. 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 business records doctrine played an important role in shaping the Electronic Communications Privacy Act of 1986 (ECPA), which draws many fine distinctions that leave much stored email only weakly protected, to an extent that would surprise most users.

In particular, messages and documents stored with Webmail providers are entitled to weaker protections than those stored on users' computers. While the government needs a judicial warrant to search your computer, it may be able to peruse your Web-mail account with only a subpoena, issued without judicial review, without any specific suspicion of wrongdoing on the part of the user, and often without notice to the person whose data is being disclosed.

CDT's report urges Congress and the courts to recognize that the business records doctrine is not applicable to stored email and to protect all stored email with the warrant requirement.

(3) 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. Unlike earlier location tracking devices (such as electronic "beepers"), today's advanced tracking devices, which can be found in cell phones and car navigation systems, do not merely substitute for real-time visual surveillance -- they provide remote monitoring of movements, including in locations not visible from public spaces.

Location technologies offer consumers added safety, security and convenience. Nevertheless, the location information that these devices generate constitutes a record of the user's movements that government agents can monitor in real-time or scrutinize retrospectively.

Location information can reveal a person's acquaintances and physical destinations such as medical clinics, government services buildings and commercial establishments. Such data may imply -- correctly or incorrectly -- additional information about the individual, including preferences and associations. Without assurance that one's movements are not arbitrarily being watched and recorded by the government, full exercise of the freedom of association will be chilled.

CDT recognizes the value of location information for legitimate law enforcement and intelligence purposes. At the same time, 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.

CDT's report reviews recent decisions by federal magistrates applying a probable cause standard for all government access to location information.

(4) Keystroke Loggers: Government Spyware

Keystroke loggers are computer programs that record every keystroke on a computer. The programs have legitimate uses, such as monitoring productivity in the workplace, but when installed by government agents to monitor computer use, they are essentially government spyware. They illustrate the widening gap between privacy protections and the growing potential of surveillance tools available to the government.

With keystroke logging surveillance, the government can obtain access to a complete picture of what people are doing on their computers. In comparison to a standard search and seizure of 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. 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. In this sense, they are even more intrusive than wiretaps.

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 is 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.

CDT believes that the federal wiretap law should be amended to extend its special protections to the installation and use of keystroke loggers. Until Congress makes statutory changes, judges considering search warrant applications for installation and use of keystroke loggers should use Fourth Amendment principles to impose strict warrant requirements on the use of keystroke loggers.

Additional resources on electronic surveillance laws: Privacy Rules For Access To Personal Data [2] and The Nature and Scope of Governmental Electronic Surveillance Activity [3]

CDT's resource page on the NSA controversy [4]

-
- location
- digital fourth

Links:
[1] https://cdt.org/publications/digital-search-and-seizure.pdf
[2] https://cdt.org/security/guidelines
[3] https://cdt.org/wiretap/wiretap_overview.html
[4] https://cdt.org/security/nsa/briefingbook.php