How Users can Protect their Rights to Privacy and Anonymity

DOWNLOAD

CONTENTS

SUMMARY

RECOMMENDATIONS

ORDER THIS REPORT

Encryption and Human Rights

HRW HOME

Bahrain
Iraq
Jordan
Morocco
Saudi Arabia
Syria
Tunisia
United Arab Emirates

Internet communication is highly vulnerable to surveillance and interception. A government agency can violate the privacy of e-mail correspondence just as easily as it can tap a person's telephone in order to listen to conversations or intercept faxes. The equipment needed is neither costly nor complicated to operate. Authorities can monitor by tapping an individual phone line and intercepting data streams as they are sent and received. If a user has Internet access via a private ISP, employees of that ISP can open and read e-mail sent through it or allow police investigators to do so, unless special safeguards are put in place to protect privacy. If authorities have access to an ISP's server or the country's telecommunications network, they can capture e-mails while they are in transit.

Authorities can read, block, or delete messages based on such criteria as the e-mail address of the sender or the recipient, the Internet Protocol addresses identifying the sending computer and the destination computer(s), or the presence of specified character strings in the body of the message--say, the words "Emir" and "corruption" in close proximity. Such a system is analogous to a postal delivery system in which all pieces of mail are first delivered to a single location, where officials can inspect items at will.

Although data is broken up and sent in "packets," each packet contains Internet Protocol (IP) addresses. Packets can easily be reassembled while en route with the aid of eavesdropping tools.

An eavesdropper can generally identify the computer terminal that is sending or receiving data, but not the person who is typing on its keyboard. For this reason, some governments are uneasy about allowing computer terminals with Internet access in places where extra effort would be required to monitor who is using each terminal, for what, and when. A contract provided by Tunisia's state-run Agence Tunisienne d'Internet (ATI) requires institutional Internet subscribers to refrain from offering anyone remote access via their computers without prior authorization, and to declare to the ATI the names of all persons having accounts on, or access to, the computers and to inform the agency of changes in the user list.

Expression via the Internet includes the use of means that are private and others that are public. E-mail is private in the sense that the sender specifies the persons and addresses to whom it will be sent. (Of course, recipients can then re-send it to others or post it on a bulletin board, just as they can do with an ordinary letter.) By contrast, launching an open-access web site or posting a comment in a public newsgroup are acts of public speech since they are viewable by anyone who wishes to visit the web site or newsgroup.

Computer users have various means to protect their privacy and anonymity, some more effective than others. At the low-tech end, a user can try to avoid surveillance by using a computer terminal or e-mail account that is not being monitored, for example, one belonging to a friend. The user can dial into another country and bypass the local service provider or use a pseudonymous e-mail account from one of the many companies that offer web-based e-mail accounts and that do not require clients to furnish their real names, such as MSN.com's "Hotmail," Yahoo.com's "Yahoo! mail," and USA.net's "Web@ddress." These techniques may help users escape identification if they are not already under surveillance, but they are no insurance against interception if a user's computer communication is being monitored.(66)

Experts agree that there are basically three methods that, for the time being at least, make surveillance extremely difficult: direct-to-satellite and other forms of wireless transmission, anonymous re-mailers, and encryption.

Small dishes are available that enable users to transmit and receive data directly via satellite, bypassing the ground-based telecommunication system. These fit into a suitcase-sized carrying case and can be placed discreetly on a balcony while in use. They resemble in size the "pizza" dishes used to download satellite television broadcasts, but are capable of sending as well as receiving. Some countries of the Middle East and North Africa either ban or require permits for direct-to-satellite dishes. Cost also puts this technology beyond the reach of most individuals and nongovernmental organizations in the region. But as they grow more affordable and widespread, wireless communications offer a potent means of evading government monitoring and censorship.

Encryption, on the other hand, costs nothing or next to nothing. Strong and easy-to-use encryption software, such as the "Pretty Good Privacy" (PGP) program, can be downloaded for free from the World Wide Web and stored on a laptop or personal computer.(67) While experts using powerful computers have been able to break strong encryption codes, the process requires considerable resources and time and is impractical for routine monitoring. Users should nevertheless pay attention to developments in the field--as well as to local laws governing the use of encryption. The Global Internet Liberty Campaign maintains a country-by-country review of legislation at <www.gilc.org/crypto/crypto-survey.html# country>.

The right to encrypt messages is of particular importance to the protection of human rights. In many countries human rights organizations use PGP to protect the identity of witnesses and victims when sending data electronically. Rights groups in Guatemala, Ethiopia, Haiti, Mexico, South Africa, Hong Kong, and Turkey are among those that use encryption, according the GILC survey. Some groups use cryptographic techniques to digitally sign messages that they send over the Internet to ensure their integrity and authenticity, that is, to prove the messages are indeed coming from them and have not been altered in transmission.

The power of encryption to foil monitoring has led a number of governments to impose restrictions on the use, sale, and export of encryption software. Tunisia, Saudi Arabia, and Israel are among those countries that ban the use of encryption without prior authorization.(68)

Encryption has an Achilles heel: it may effectively shield a message's contents from an eavesdropper but not the fact that something has been encoded. This alone may lead to harsh consequences if the authorities wish to punish the sender or recipient, or coerce them to disclose the message's contents or their "private keys." Upon obtaining the latter, authorities could then read every message encrypted with the user's "public key" or use the compromised private key to impersonate that user in corresponding with others.

One way to circumvent this danger is to camouflage encrypted messages by using steganography. This type of program hides one form of data inside another--for example, text inside a graphic image or a video or audio clip--in such a way that makes it more likely to escape detection by interlopers. For example, a sensitive document proving that a police unit moonlighted as a death squad can be encrypted and embedded in a photograph of a soccer team, and then e-mailed to a person outside the country who has the means to extract the document. Steganography software can be downloaded for free from the World Wide Web.(69) However, some experts warn that sophisticated eavesdroppers can detect when a file has something steganographically hidden in it.

The third anti-surveillance strategy is to route communications via secure and trusted web-based re-mailing services that forward them to the designated recipient only after expunging the original address and other identifying data.(70) To reduce traceability further, users can select re-mailers that keep no records of the addresses from which they receive, and to which they send, data. They can also program messages to pass through more than one re-mailer; some re-mailers do this automatically. And if their browser supports strong encryption, they can choose a re-mailer that encrypts all messages as they are sent to that re-mailer, which then sends them on to the intended recipient in decrypted form. In the latter scenario, even if an eavesdropper is "sniffing" a person's Internet activities, the eavesdropper can at most discern

that the person is visiting a particular web site but not the content of the messages that the person is sending, the intended recipients, or whether the person has encrypted messages before sending them.

For obvious reasons, some governments see anonymizing re-mailers as undesirable and have blocked them.(71) The governments of China, Singapore, and the United Arab Emirates block the web site of www.anonymizer.com, one of the best-known such services, according to Lance Cottrell, president of Anonymizer.com.(72) Another potential problem with anonymizers is that they do not guarantee that the user's identity will remain unknown to the anonymizing service itself or to the user's ISP. Researcher are addressing this concern. One tool that is still in prototype form is "Crowds." It works by collecting Web users into a geographically diverse group that performs Web transactions on behalf of its individual members in a way that prevents Web servers, other "crowd" members, and eavesdroppers from identifying the sender of a particular communication.(73)

---

66. Most web-based free e-mail services are not encrypted. Users could enhance security when using these services by encrypting and/or anonymizing the messages they send. See below.

67. See Patrick Ball and Mark Girouard, *Safe Communications in a Dangerous World: Cryptographic Applications for Human Rights Groups* (Washington, DC: American Association for the Advancement of Science, expected 1999). For information about how PGP, a "public key" encryption program, works, see the FAQ (frequently asked questions) sheets at <http://www.arc.unm.edu/~drosoff/pgp/pgp.html> and <www.cam.ac.uk.pgp.net/ pgpnet/pgp-faq>; see also David Banisar, *BUG OFF! A Primer for Human Rights Groups on Wiretapping* (London: Privacy International, October 1995), <www.privacy.org/pi/ reports/bug_off.html>.

68. According to GILC's encryption survey, other countries with laws restricting encryption include Belarus, Singapore, Russia, Pakistan, China, and until January 1999, France. In the United States, encrypting is not regulated, but laws bar U.S. companies from freely exporting strong encryption software without a license, on the grounds that encryption will be used by terrorists, drug traffickers, and organized crime groups to conceal their deeds.

69. For more on steganography, see <http://members.iquest.net/~mrmil/stego.html>.

70. Useful information about anonymous re-mailers can be found in the Anonymous Re-mailer FAQ (frequently asked questions) by André Bacard, <www.well.com/user/abacard/remail.html>. See also <www.anonymizer.com>, which offers anonymizing re-mailer and web-browser services, a FAQ, and links to other sites that deal with privacy on the World Wide Web. For a list of active anonymizing re-mailers, see <www.cs.berkeley.edu/~raph/remailer-list.html>.

71. On concerns in the law-enforcement community about anonymity on the Internet, see Steve Lohr, "Privacy on Internet Poses Legal Puzzle," *New York Times*, April 19, 1999.

72. Lance Cottrell, "Commercial Anonymity," paper presented at the Computers, Freedom and Privacy conference in Washington, DC on April 6, 1999, <www.cfp99.org/ program/papers/cottrell.htm>.

73. "Crowds" and other new tools for protecting privacy online are described in *Communications of the ACM*, February 1999 (vol. 42, no. 2). The ACM is the Association for Computing Machinery.