PRIVACY INTERNATIONAL

Bug Off! A Primer for Human Rights Groups on Wiretapping

Archived report by Privacy International
October 1995

About Privacy International

Privacy International (PI) is a human rights organization concerned with privacy, surveillance and data protection issues worldwide. It has members in over forty countries and is based in London, England with offices in Washington, D.C. and Sydney, Australia. PI has engaged in numerous campaigns on privacy issues, publishes a quarterly newsletter, the International Privacy Bulletin, and sponsors two annual conferences.

Yearly memberships to Privacy International are US$75 for individuals. Separate subscriptions to the IPB are also available for libraries, companies and individuals. For more information on PI and the International Privacy Bulletin, please contact:

Privacy International, Washington Office
666 Pennsylvania Ave, SE, Suite 301
Washington, DC 20003 USA
Phone 1+(202)544-9240
Fax 1+(202)547-5482
Email: pi@privacy.org
http://www.privacy.org/pi/

About the author and acknowledgments

David Banisar is the Deputy Director of Privacy International and an attorney at the Electronic Privacy Information Center in Washington, DC. He is editor of the International Privacy Bulletin and the co-author of The Electronic Privacy Sourcebook, an upcoming book on cryptography and privacy policy in the US (John Wiley and Sons, 1996). Thanks to Phil Agre, Richard Claude, Simon Davies, Peter Gutman, Wayne Madsen, Marc Rotenberg, Dan Salcedo, Bruce Schneier, M.L. Shannon, David L. Sobel and Phil Zimmerman for their assistance.

PRIVACY INTERNATIONAL

Table of contents

Introduction

The explosion of telecommunications services has improved the ability for human rights groups to disseminate information worldwide. New telephone, facsimile and computer communications have created opportunities for human rights groups to improve organizing and to promote human rights faster and at a lower cost than ever before. However, these new technologies can be monitored by governments and other groups seeking to monitor the activities of human rights advocates. For this reason, human rights advocates should be aware of the dangers and measures that can be taken to limit surveillance.

The scope of this paper is limited to the interception of oral and electronic communications commonly referred to as wiretapping and other issues related to telephone communications. It will also discuss methods to avoid surveillance.

Why should groups be concerned?

Wiretapping is conducted in nearly every country in the world and is frequently abused. The US Department of State, in its annual Country Reports on Human Rights Practices for 1994, reports widespread, illegal or uncontrolled use of wiretaps by both government and private groups in over 70 countries. Human rights groups, reporters and political opponents are the most common targets of surveillance by government intelligence and law enforcement agencies and other non-governmental groups. In some countries, such as Honduras and Paraguay, the state owned telecommunications companies were active participants in helping the security services monitor human rights advocates. In other countries, multiple forms of surveillance are used. For example, in 1991, wiretaps and hidden microphones were found in the offices of the Mexican Human Rights Commission. More recent press reports estimated that there are 200,000 illegal wiretaps in Mexico currently in place.

These problems are not limited to developing countries. In the US, litigation conducted by the Computer Professionals for Social Responsibility under the Freedom of Information Act revealed that the FBI monitored computer networks used by political and advocacy groups. French counter-intelligence agents wiretapped the telephones of prominent journalists and opposition party leaders during the mid-1980s. There have been numerous cases in the United Kingdom which revealed that the British intelligence services monitor social activists, labor unions, and civil liberties groups.

Thus, there is an obvious need for human rights groups to be concerned with wiretapping: Governments often monitor human rights groups to discover what they know, who their sources are, and what their future activities will be. The lack of secure communications creates the threat of physical harm to many people in the human rights field.

Who can do it and what are the limitations?

Most types of electronic communication can be intercepted without a high level of expertise or expensive equipment. Surveillance equipment is not difficult to construct and is available in many electronics stores. Many manufacturers sell surveillance devices to any buyer, without restrictions. Thus, groups should be aware that both governments and private organizations may have the capability to eavesdrop.

This does not mean that everyone should believe that they are always under surveillance. It is not practical for any government or group to wiretap all telephones in a country and listen to every conversation simultaneously. Wiretapping is a labor intensive operation and requires considerable resources to conduct the taps, listen to, and transcribe the conversations. Because it is necessary to have a human listen to the conversation, labor and equipment costs create practical limits to surveillance. The East German secret police employed 10,000 people to conduct wiretaps and listen to conversations before the Berlin Wall fell.

New technologies, such as computerized voice recognition, that can automate surveillance are being actively developed by Western (and presumably also by other) governments. The Ottawa Citizen reported that the Canadian Communications Security Establishment has spent over $1.1 million to "isolate key words and phrases from the millions of signals the CSE monitors every day" and awarded contacts to develop systems to create a "speaker identification system." There were also reports that the US Government assisted the Columbian government in tracking down drug cartel leaders by using voice recognition technologies on cellular phone calls. These new technologies are not yet generally available to less wealthy countries or local police forces. There may also be technical limitations on conducting a large number of simultaneous taps. Recently, former members of the Soviet KGB disclosed that they only had the capability of wiretapping 1,000 phone lines in Moscow and another 1,500 for the rest of Russia.

Given this, it is not likely that every telephone can be monitored in a particular city. However, it is possible that the public and private phones nearest to the offices of human rights organizations or their staffs may be also monitored. In France, counter-intelligence officers illegally wiretapped not only the telephones of several journalists but also the phones in bars and restaurants that they frequented.

Thus, surveillance is generally limited to those wiretaps installed manually and listened to by human agents. This is not an inconsequential threat.

Standard telephones

Standard telephone systems are very vulnerable to wiretaps. It does not require a high level of skill or technology to intercept a voice communication. There are many locations where a wiretap can be placed. For example, microphones in many older telephones' handsets can be replaced with one that can also transmit to a remote receiver. Taps can also be placed at the telephone boxes in the basements of buildings, on the lines outside the house, or on the telephone pole junction boxes near the target of the surveillance. A common technique used by police forces is to remotely monitor calls by having lines run from a telephone company central office where the local switching equipment is located to a monitoring station in a government office.

Many of these techniques are undetectable to the target, especially in newer systems, where the system is run by computers. In the US, legislation requiring that all communications systems be designed with the ability to more easily intercept communications was recently enacted at the behest of the law enforcement and intelligence community. This will have a profound effect worldwide since the US is one of the largest manufacturers and purchasers of telephone switching equipment worldwide.

Scrambling voice communications

Technology is available to ensure that telephone conversations are not easily monitored. Secure phones, which use cryptography, a mathematical technique for scrambling conversations, are commercially available from many different companies including Motorola, TRW and AT&T, but these devices may not provide adequate protection. AT&T recently introduced an telephone attachment that connects to the handset cord and when used with a duplicate device on the receiving device, scrambles conversations. However, it uses a specialized computer chip, known as the Clipper Chip, for which the keys to unscramble communications are also held the US Government in a system called "key escrow." The U.S. Government has been strongly pushing other governments to adopt the system for their countries. If other countries also begin using similar systems, it is likely that keys for users in that country will also reside with their governments.

Other devices use the US Data Encryption Standard (DES) or secret company standards. DES is considered by most security experts to be secure against eavesdropping except against the most well financed opposition such as large intelligence organizations. Secret standards may not be as secure because they may have weaknesses that have not been publicly disclosed since there is no open review of the algorithms. These devices are also very expensive, costing around $US 2,000 each.

There is also the possibility that the devices are deliberately not secure. The United State and some other countries have laws that require government permission to use or export any device or software that contains encryption. In the US, manufacturers are required to design their products that will be exported so that the NSA may still monitor the conversations. Therefore, any device that is sold by a US company overseas should not be considered safe for protecting sensitive information.

These controls may be circumvented by purchasing devices designed in countries such as Sweden or Switzerland, which do not have export control laws on encryption. However, these devices may have also been compromised by their domestic intelligence agencies. Recently, there were numerous news reports across Europe that Crypto AG, a company which sells secure phone and fax devices, is in reality controlled by German intelligence and has deliberately sold weakened encryption devices. There are also international information sharing agreements – such as the Quadripartite Agreement – between intelligence agencies that could result in the weakening of encryption.

A recent advance is the development of computer based scrambling that will allow two PC (or clone) owners to talk to each other through their computers over modems or the Internet to scramble their conversations. Several freely available programs are currently under development. These programs are generally available for free and may be ideal for human rights groups to use. However, they may also require more powerful computers to use (at least a 386 or faster machine for the PC, 68030 or greater for the Mac) and high speed modems (14.4K or faster) to have understandable speech.

Wireless communications

Wireless telephones are becoming more and more popular in western countries. In the US alone, over 40 million cordless phones are in use. There are also millions of cellular telephones in use. In developing countries, wireless communications such as cellular and satellite-based telephones are also popular as a means to avoid laying new telephone lines in areas that were previously undeveloped. All of these devices are easily interceptable and should not be used by anyone who is discussing sensitive information.

Cordless telephone communications are especially easy to intercept. Many of the older models broadcast just above the top range of the AM radio band and conversations can be easily overheard with any AM radio. Newer models operate in the 49 MHz range and can be intercepted with an inexpensive radio scanner purchased at most electronics stores for under $US 100.00. The range of interception can extend to nearly one mile.

Several phone manufacturers now offer “privacy secure” cordless phones that they claim ensure the privacy of phone calls. However, most of these phone use a simple fifty year old technique known as “frequency inversion” that inverts the sound waves to limit eavesdropping. This system provides minimal security at best.

New digital-based cordless phones may provide a slightly greater level of protection from the common listener, but most of these phones lack any form of sophisticated scrambling that would protect eavesdropping by government agencies or wealthy opponents. In addition, it is likely that new scanners will soon be available commercially that will be able to listen in on these conversations.

Cellular phones have the same problems as cordless. They also broadcast over airwaves like a radio. Inexpensive scanners are also available to intercept conversations. A US law requires that newer scanners limit eavesdropping on certain frequencies but kits are readily available from electronic stores and mail order companies to remove those protections. In addition, some cellular phones can be programmed to act as scanners to intercept other calls. There is also equipment available to law enforcement, which can track and monitor cellular conversations as they move around a city.

New cellular phones use a digital system which will be more difficult to intercept and also provide for clearer conversations. It is also easier to secure these telephones from eavesdropping. However, intelligence agencies in the United States and other countries have attempted to restrict the use of improved scrambling technology. In Pakistan, the government shut down the cellular phone company until it provided equipment to allow easy over-the air-interception. In the US, the cellular telephone industry association agreed to adopt a weakened scrambling standard after pressure from the National Security Agency. Experts who have seen the standard state that the standard provides little or no protection against eavesdropping. Intelligence agencies in other countries have also lobbied to limit the security features in GSM – the international standard for digital cellular phones. In Australia, the federal government rejected the request of the law enforcement agencies and ordered the operator of a new digital cellular system to commence operation without the capability to intercept the over the air portion of the conversation.

Cellular phones can also provide information on the location of an individual to within a few blocks, depending on the system. When a cellular telephone is turned on, it regularly broadcasts its location to the local transmitters so that they can direct calls to the correct location. This information can be used to locate the position of a cellular phone and may also be used to track its location its owner moves around.

A related technology, the wireless pager, can also be easily intercepted. Pagers receive signals over the airways with no scrambling. Numerous programs are available for computers that can monitor the entire frequency spectrum that pagers operate on and automatically retain every message that is sent.

Facsimile (fax) machines

It is also possible to intercept facsimile transmissions. A fax machine is essentially an inexpensive computer system that uses a well known standard for sending and receiving files. Most experts describe intercepting faxes as “very easy.” Commercial devices are widely available that automatically intercept faxes. In New York City, fax intercept machines were used as far back as 1990 by local police. Defense News reports that numerous countries sell these devices including the United States, the UK, the Czech Republic, and Israel and that the “many countries are eyeing low-cost systems...also to intercept political and economic-related information....” It is also possible to intercept faxes using a computer with specialized software and a fax modem. With the widespread use of Digital Audio Tape (DAT), it may also become easier to record a fax transmission and replay it back into a machine with minimum effort. Thus, fax machines should be considered as insecure as telephones.

There are also fax machines available that provide scrambling to prevent interception. These machines usually cost around $US 3,000 and are available worldwide. Like secure telephones, fax machines from the United States must have a weakened encryption scheme to allow for their export. Companies in Sweden, Switzerland, and other European countries claim their machines are not limited because they have no export laws. An expert on encryption should be consulted before purchasing these devices to ensure their security.

It may also be illegal to use such devices. It has been reported that some countries, such as Singapore and China limit the use of encryption without providing the keys to the government. In China, the use of fax machines without a license is prohibited.

Telephone transaction information

Another area of concern is the transactional information created when a telephone call is placed.

In most countries, when a call is placed, the number of the called party is recorded in the telephone company's computers. This can provide critical information on confidential sources and others. In the US, these records are widely used by law enforcement against reporters to locate leaks of information, and monitor environmentalists and others. In the former USSR, human rights activist Anatole Sharansky reported that the authorities regularly obtained his overseas billing records to keep track of who he had spoken to.

Computer communications

Computer based communications is the newest and most useful tool for human rights advocates. It provides fast and inexpensive communications to nearly every country in the world. Electronic mail can be used quite effectively to communicate and distribute information worldwide at low cost. It is also possible to create private mailing lists or post information on public electronic conferences such as Peacenet or the USENET newsgroups.

Eavesdropping of computer communications is not difficult unless measures are taken to increase security. High speed modem communications (14.4K, 28.8k) are more technically difficult but can still be intercepted by law enforcement in the US. Low speed modem communications (1200,2400) are fairly easy to intercept.

Once connected to an international network like Internet, new problems arise. Messages pass through numerous machines on the way to their destination. Currently, sending electronic mail is the equivalent of sending a typewritten postcard in the mail. It theoretically can be read by anyone in the computer link between the author and the recipient and there is also no method to conclusively verify the identity of the message originator.

Encryption can also be used to protect these communications. Many human rights groups are already encrypting their messages. Groups in Central America, Ethiopia and Burma use encryption to protect their communications and files. It was also reported that the African National Congress developed and used an encrypted e-mail network for years without it being compromised by the security services of South Africa.

Encryption can be used to protect the messages and to verify the identity of the sending party. Unlike other communications technologies, encryption for computers is widely available for free or at minimal cost. It is also easy to use. Many commercial software packages such as Lotus Notes and the planned future versions of the Microsoft and Apple Computer operating systems will have built-in encryption, although the encryption in these products have been weakened to allow for export.

Pretty Good Privacy (PGP) by Phil Zimmermann, an American software engineer and human rights activist is commonly used by human rights groups worldwide. It is available for most computers and can be easily configured to work in several different languages, including Spanish, French and German. The program is small and can work on nearly all laptop and personal computers, along with larger systems.

PGP uses "public key" encryption. Each user of PGP creates two keys, a public key and a secret key. The user then gives the public key to whomever they wish to correspond with and can even publish it publicly like a phone number. The secret key is kept in a safe place usually with the PGP program – and protected by a password. The public key is used by other people to encrypt messages that they send to the secret key holder and only that person can unscramble the messages. Thus, public key cryptography avoids the need to meet in person or to carry codebooks to safely exchange keys and messages.

To use PGP, a person writes out a message using a word processor, runs PGP to scramble the message with the recipient's key, then sends the scrambled file as a mail message instead of the original message. The receiver runs PGP to covert it back to a readable form. The process only takes an additional minute or two, depending on the length of the message and the processor speed of the computer. For some computer systems, programs have been written to make it an automatic function of electronic mail.

Another feature that PGP and other public key systems can provide is "Digital Signatures," which ensure the identity of the sender of the message in the same way that a normal signature at the bottom of a letter usually verifies that a letter is from a known corespondent. Signatures are useful when an electronic message is sent to ensure that it was not modified or falsely created by someone else. Thus, readers of notices from groups which send out electronic alerts, such as Amnesty International, Americas Watch, Helsinki Watch and the Tibetan Government-in Exile, can ensure that the alerts have not been altered by people wishing to disrupt the group's activities.

PGP can also be used to protect files on a computer. It can prevent the accessing of electronically stored papers or correspondence in case there is a physical break-in and the computer is taken. Many groups in Central America use it to protect their databases of rights abuses.

Another useful program to ensure that IBM PC computers are not accessible without a password is Secure File System (SFS) by Peter Gutman. SFS is a program which sits between the disk drive and the operating system, transparently encrypting all data as it is written to disk and decrypting it again as it is read from disk. To the user, it appears – apart from a slight slowdown due to the encryption – as a normal disk drive. In order to access an encrypted drive, it must be first mounted by entering the decryption password. The drive can later be unmounted with a user-defined key combination, after a period of inactivity, or when the machine is reset or turned off.

Encrypted disks can be converted back to normal disks, or have their contents quickly and efficiently destroyed. The software includes various stealth features to minimize the possibility of other programs monitoring or altering its operation.

Conclusion

New technologies offer new opportunities for human rights advocates. These same technologies also present opportunities for enhanced eavesdropping by those opposed to the groups' activities.

Wiretapping of human rights groups is not uncommon. However, there are limits, both technical and labor related, to the number of taps that are in effect at one time. It is impracticable for every phone in a city to be monitored simultaneously. Nonetheless, human rights organizations may want to take precautions. There are methods available to prevent eavesdropping and care must be taken to ensure that the devices purchased actually provide an adequate level of protection.