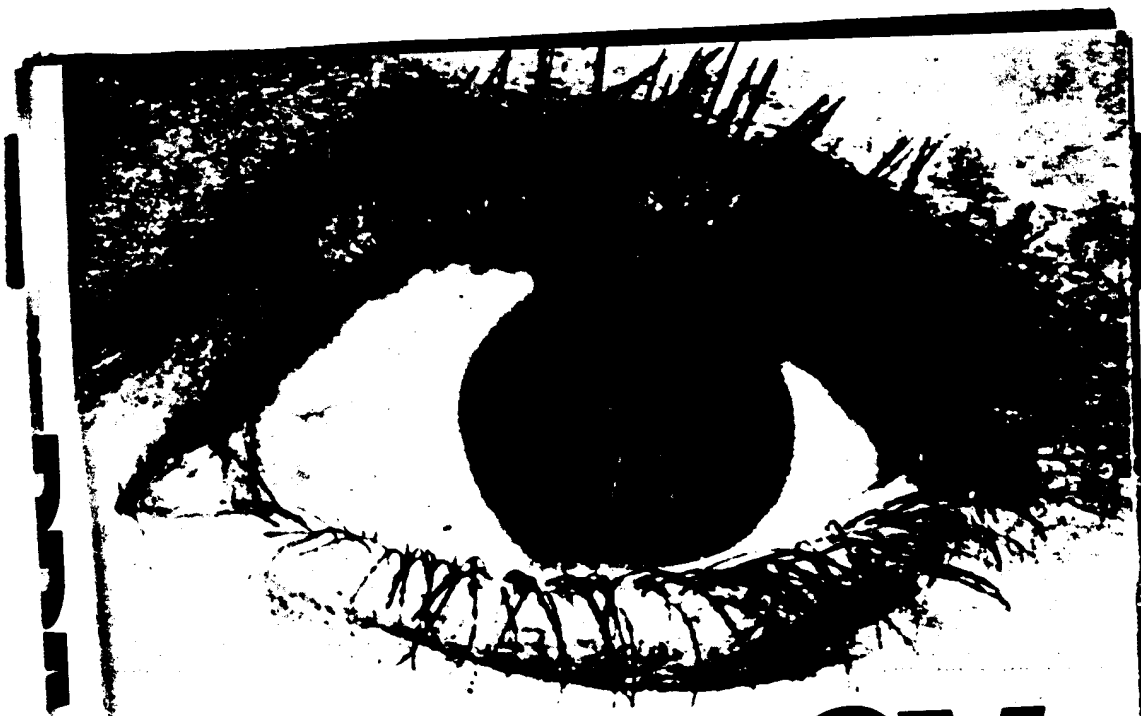
Jan. 1979



PRIVACY

HOW TO PROTECT WHAT'S LEFT OF IT

ROBERT ELLIS SMITH

publisher of PRIVACY JOURNAL

Contents

that it routinely discloses Southern California unlisted telephone numbers to more than one hundred federal, state, county, and city agencies, without ever informing subscribers. The company said that it will confirm to a subscriber that the number had been disclosed but will not volunteer the information. Among the agencies that regularly received unlisted numbers on request are the Federal Bureau of Investigation, Central Intelligence Agency, Border Patrol, Forest Service, Food and Drug Administration, county probation offices, local police and fire departments, Internal Revenue Service, county health departments, county and city welfare departments, military services, and volunteer "crisis" and suicide prevention centers. Pacific Telephone provides about one hundred unlisted numbers a day to these agencies. New York Telephone Co. admitted doing the same thing, even to a cop on the beat in a nonemergency. Telephone companies in all parts of the country have much the same policies.

Another instance of generosity on the part of telephone companies is their co-operation with government snoopers who ask for a list of toll calls made from a particular telephone number. Telephone companies provide these "telephone logs" freely to the government without notifying the customer. The most notorious incident occurred in 1971, when the Chesapeake & Potomac Telephone Co., in Washington, D.C., gave to the government a list of toll calls made by news columnist Jack Anderson, the St. Louis *Post-Dispatch*, and Knight Newspapers. In 1974 the C. & P. Co. co-operated again, giving long-distance records from the New York *Times* Washington bureau for the preceding seven months to the Internal Revenue Service. The IRS thus had a list of 2,400 calls made by *Times* reporters, to see whether an IRS agent might have talked to a *Times* staff member. The telephone company also turned over a similar log on the home telephone of a *Times* reporter.

These logs are useful investigative tools. They don't reveal the contents of a conversation, but they can help identify contacts and associates of a caller and lead investigators to sources of information.

Since 1974 the Bell Telephone System says it has been re-

ton, wiretaps with the consent of one of the parties to a conversation are legal. Anybody may wire his or her own telephone with a recording device and record his or her *own* conversations on that telephone, without violating the law. The police may wire their own phones, dial your number, and record the call. A regular beep tone to alert you is no longer necessary.

The law clearly allows telephone companies to monitor any telephone calls they wish, in order to check the working order of equipment. The telephone employee rarely cares about the content of the conversation or knows the identity of the callers. The telephone companies also use this authority to detect people who are defrauding telephone companies by using devices that avoid toll charges.

The consent concept in the federal law has been extended to authorize users of telephone equipment to monitor their own lines, even though each individual employee has not provided consent, or even knows about the eavesdropping. Federal law says that this monitoring is legal, without a warrant or individual consent, to check on "the rendition of . . . service." "Service monitoring" is discussed in Chapter 16. Eavesdropping to detect employee dishonesty has been regarded as legal under this provision of the law. However, it is not valid for one member of a household to consent to electronic eavesdropping in behalf of the other members of the household.

The best-known category of wiretaps includes those installed by law enforcement officers, with a warrant approved by a judge in advance under federal or state law.[41] The warrant must be specific as to the targets and the location of the surveillance. The judge may order the wiretap if satisfied that there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular crime—espionage, sabotage, murder, kidnapping, extortion, bribery, gambling, jury tampering, obstructing justice, theft from interstate shipments, counterfeiting, drug dealing, bankruptcy fraud, illegal union activities, conspiracy, or other *violent felonies.*

There must also be probable cause to believe that electronic surveillance will provide good evidence. The judge must certify that other investigatory techniques have been tried unsuccess-

not. Drugstore clerks take polygraph tests; store managers do not.

Even though the polygraph, which measures three bodily changes, has not gained scientific acceptance, we have moved into the second generation of "lie detection" with devices that measure only one bodily change. The voice analyzer records changes in the vibrations of the human voice, on the theory that when a person is under stress these vibrations change. A similar device, called the psychological stress evaluator, measures changes in the inaudible frequency modulation of the human voice. These devices have been with us only since 1970, but business managers desperate for a short cut to truth have shown interest in them because they can be used without the knowledge of the subject. The machine fits into a briefcase. No obtrusive rubber hose around the stomach, no cuff around the arm here—a hidden microphone will do. Some users claim that the machines work on telephone or tape-recorded voices. They have even used the technique on the voices of persons long since dead to tell us who really killed President Kennedy. Clearly these devices are less reliable than even the polygraph because they measure only one bodily change. A study for the U. S. Army Land Warfare Laboratory in 1974 reported that the machines were not nearly as reliable as not only the polygraph but also the tried-and-true method of simply observing a subject's behavior. Accuracy rates in this test of voice analysis for the Army, the most recent pertinent research, ranged from 19 to 33 per cent. The technique is less successful, in fact, than mere chance. The Department of Defense and the Central Intelligence Agency, whose pursuit of new investigative toys is well known, have both found voice analyzers and psychological stress evaluators wanting. Neither agency relies on them.

They are thought to be rarely used. Throughout the federal government there were fewer than a dozen machines in 1974, and the companies that make them are far from candidates for *Fortune*'s Top 500 (or 5,000) companies. But because they can be used behind the back of an individual—or long after the subject has uttered words—who can say where or when they are used? An entrepreneur in the northwest United States has re-

Consulate of Chile in San Diego. Assorted others read mail out of idle curiosity.

The latest word from the Department of Justice is that reading mail requires a warrant. (The U.S. attorney in the southern district of New York claimed that the restriction applied only to sealed mail and that the Customs had already unsealed the mail and therefore the restriction wasn't applicable.)

A Customs Bureau official told Congress in 1977 that other federal investigating agencies laughed at Customs when told they couldn't read mail that was opened. From 1953 to 1973, in violation of federal statutes and the Constitution, the Central Intelligence Agency conducted an extensive program of opening and reading first-class mail passing in and out of the country through Hawaii, San Francisco, New Orleans, and New York City. The Federal Bureau of Investigation got to take a look as well. Mail to and from the Soviet Union was automatically suspect.

Under this institutionalized nosiness (code-named HTLINGUAL and SRPOINTER), the CIA copied at least 215,000 letters and distributed them to other federal agencies for leisure-time reading. The CIA took down the names of every person mentioned in the correspondence—1.5 million persons in all—and stored them in its computer data bank in McLean, Virginia. Among those whose mail was read and photocopied were John Steinbeck, author of *The Grapes of Wrath*; Jane Fonda, film actress and political dissident in the early 1970s; Senator Frank Church of Idaho, whose mother wrote to him from Moscow; a sociology professor at Amherst College who notified two colleagues at Moscow State University about an academic conference; an American exchange student in Moscow writing back home to his father; and an American woman who wrote to a Soviet dissident whom she had met on a trip to Russia. Can the United States adequately crusade for the freedom of dissidents in the Soviet Union if American agents themselves are reading the mail of the Soviet citizens?

The CIA claims to be able to read mail without even opening the envelope. It uses a chemical to decipher the writing in-

side, according to secret testimony in 1975 by William E. Colby, then director of the CIA. But as long as postal authorities allowed the CIA to read mail in the States, there was no need to use the special potion in the United States.

The CIA's routine reading of mail within the United States was said to have stopped in 1973, and the Postal Service said in 1975 that it no longer permits CIA agents to get a look at the mail. The FBI somehow does get hold of mail, most of it from overseas, and reads it. Until 1977 it even had a special office behind the Capitol in Washington, D.C., for translating when necessary. Most of this mail is personal correspondence between American families and friends in Russia or China.

The extent to which federal agents open and read domestic mail is not known. About two hundred times a year, court orders allow federal authorities to do so. Federal agents are not supposed to do so without warrants.

The FBI makes use of the Postal Service's change-of-address records. FBI documents about a friend of mine showed that the Denver Field Office reported to headquarters the new address to which my friend had asked the Post Office to forward his mail. (The FBI also received the co-operation of a Denver moving company to find out where my friend was shipping his furniture.)

In addition to opening and reading mail, federal agents also use "mail covers," the interception of mail to a particular address to copy down all information on the outside of the envelope. About three hundred postal inspectors conduct the monitoring. Return addresses and the date of the postmark are copied and forwarded to the agency that requested the cover. Sometimes a fugitive will disclose his or her whereabouts by placing a return address on correspondence to the family. A mail cover on a company suspected of mail fraud may turn up the addresses of victims who could provide evidence for prosecution. The Postal Service takes the position that such surveillance does not violate the Fourth Amendment and requires no warrant, because the mail is not opened. The service will monitor mail only for law enforcement agencies and only to protect