TOM CHALKLEY

Gary T. Marx

The Surveillance Society

The Threat of 1984-Style Techniques

Undercover practices have expanded in scale and changed in form in the last decade in the United States. Police have penetrated criminal and sometimes noncriminal circles in ways not previously attempted. The individual undercover worker making isolated arrests has been supplemented by highly coordinated and staged team activities involving technological equipment. Fake organizations have also appeared as key elements in many operations.

Government agents are clearly limited in the surveillance and physical coercion they can carry out, but they are free to create the impression of police omnipresence and omnipotence. What they cannot do by force or by the actual power of their technology, they may attempt to do by creating a "myth of surveillance."

People may be deceived into believing that control techniques involving computers or lie detectors are far more effective than is the case. Lie detectors, for example, are thought to be most effective when persons being tested believe that they work. A variety of tricks are used to make people believe in their power.

> Welcome to the world of undercover "sting" operations, rewards for spying on your colleagues, computer data banks, and voice analyzers to detect lying.

The impression that people are always being watched—by police agents, store detectives peering through one-way mirrors, surveillance cameras, etc.—is one way to deter illegal actions. Any tempting illegal opportunity may really be a police trap, and anyone could be a police agent. In some companies, employees receive memos stating: "Systematic checkings are made of every employee; you never know what day or what hour you are being checked."

Undercover Activities

In the United States, the federal agency showing the greatest change in attitude toward undercover operations is the FBI. Practices once considered too risky and costly (whether to the individuals involved or to the agency's reputation) for routine use are now viewed as important tools. In the words of one agent, "Undercover operations have become the cutting edge of the FBI's effort to ferret out concealed criminal activity."

In the mid-1970s, the FBI began using undercover agents in criminal investigations. The number of such investigations has steadily increased. The first appropriation request for extra expenses for "undercover activities" appeared in 1977 for $1 million. This increased to $4.7 million in 1981 and $10.75 million in 1983. The investigations have included:

- Agents posing as wealthy Arabs seeking to bribe congressmen.
- "Anti-crime decoys," or police agents disguised as a vulnerable

"No warrant is required for setting up a fake organization, for infiltrating a group, or for offering a tempting illegal opportunity."

target for assault (e.g., a derelict sprawled on the ground with an exposed wallet, an elderly person).

- Police running fake fencing operations and purchasing millions of dollars worth of stolen goods.
- An operation against Japanese companies that involved the FBI and IBM setting up a fake consulting firm that sold stolen IBM information.
- A police agent posing as a priest in an effort to elicit information from a suspect.
- Agents who act as guides to big-game hunters and then arrest them for killing animals out of season.

The expansion of undercover activity is hardly an unmitigated good, however benignly it is presented by its advocates. It is highly intrusive and difficult to supervise. The crimes it documents are sometimes an artifact of the investigation. With respect to civil liberties, the tactic is far more invasive and dangerous than electronic surveillance or a physical search. While the latter require a judicial warrant, no warrant is required for setting up a fake organization, for infiltrating a group, or for offering a tempting illegal opportunity.

REWARD!

A related, though less costly, investigative means is informing. This form of surveillance has expanded significantly in the United States. Informing has come to be seen as an element of good citizenship. Concern over both street and white-collar crime has led to new means of informing. Citizens are encouraged to report on what they see or suspect.

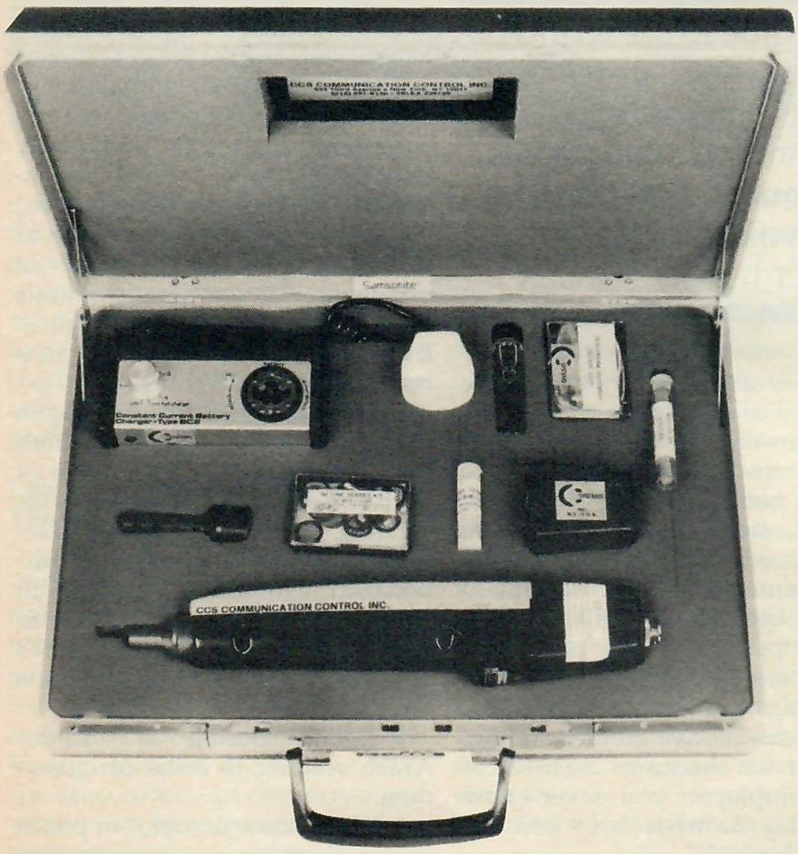
This may involve direct programs such as the leaflets passed out by the sheriff's office in one state asking, "Do you know something the sheriff should know?" A new mass-circulation publication called *Reward Magazine*, whose pages are designed to look like wanted posters, offers cash for information leading to the location of wanted suspects. Most common are toll-free hot lines that encourage anonymous offering of information to police. Respondents are given an identification number. If the tip proves useful, the source presents the number at a pre-arranged place and collects an envelope containing the cash, no questions asked.

Among the largest of these programs is TIP (turn-in-a-pusher), found in hundreds of communities. There are more specialized projects such as Connecticut's Turn-in-a-Poacher, Seattle's "dial 764-HERO" program for reporting single-passenger cars in bus and carpool lanes, and Boston's Drop-a-Dime program for anonymous tips on police involved in drug dealing.

The video equivalent of the old reward posters is a program called "Crime-Stoppers-USA, Inc.," which is found in over 450 cities. It uses televised reenactments ("the crime of the week") to encourage witnesses of unsolved crimes to come forward. There are also radio and newspaper versions. Advocates claim that the program has been highly successful in solving crimes and locating suspects. The police sergeant who coordinates one of the most successful of these programs (the Austin, Texas, Crime Stoppers Unit) reports that they "get husbands turning in wives, wives turning in husbands—we've even had mothers turn in their own sons."

This bomb-detector kit can electronically sniff out explosive vapors.

CCS COMMUNICATIONS CONTROL, INC.



Handheld mini-telescope can penetrate total darkness.

CCS COMMUNICATIONS CONTROL, INC.

Other resources have been made available to support the flow of information to the state from citizens. The Federal Witness Protection Program provides relocation and a new identity to informants. There are increased legislative and judicial protections for whistleblowers. Some legislation also makes it a crime *not* to report certain kinds of violations such as child abuse and certain hazardous working or environmental conditions.

By law, federal cabinet agencies are required to have hot lines on which citizens can report abuses. In a series of free public-service radio commercials, New York City's investigation commissioner pleads "If you know of any corrupt practices going on in New York City affairs, let us know."

Informing may be a means of keeping government in line as well as contributing to safe streets. Yet there are also potential dangers in institutionalizing such systems. They may encourage paranoia, suspiciousness, and vigilantism. They can weaken trust and offer a vehicle for malicious reporting from anonymous sources. In a different political climate, these devices would lend themselves equally well to informing on those who are merely different or unpopular rather than criminal.

Electronic "Sniffers"

Recent developments in surveillance technology permit intrusions that were once in the realm of science fiction. "Mini-AWACs"—a system that can spot a car or a person from 30,000 feet up—have been used against drug traffickers. Satellites may soon be used for this purpose as well.

Lasers, parabolic mikes, subminiature tape recorders, remote camera systems, videotapes, periscopic prisms, sensor and tracking devices, heat-sensing imaging devices that can tell if a house is occupied, voice analyzers, light-amplifying night vision devices, and techniques for reading mail without breaking the seal are among the new devices. Dogs trained to smell contraband could soon be replaced by electronic "sniffers."

Parking meters in the near future might have small radios to alert police when the meters expire. A system of electronic sensors under city streets could be capable of monitoring when and where a specific car is driven, and the use of "inference" technology based on body clues (e.g., blood and urine analysis for drugs) will doubtless increase.

These new devices can send information to a central source, permitting a few persons to monitor a great many. The information is recorded and used as needed. The monitor need not literally be attending at the instant a transmission occurs to be able to use it. In addition, many surveillance devices are self-actuated by the unknowing subject through movement or sound.

Some of the devices are hidden. This is the case with cameras disguised as chandeliers, fire extinguishers, or mannequins, as well as the "beepers" that the Supreme Court has ruled can be attached, without a warrant, to the vehicles or possessions of suspects. Or, if visible, the apparent surveillance device may not be the real one. For example, in some banks the highly visible camera with the blinking red light pointing down at you may have no film in it and the real camera may be hidden. In other cases the devices are hidden, but wide publicity is given to the fact that they are in operation.

People may gladly consent to the monitoring of their behavior. Information may be willingly given to a data bank in order to obtain consumer credit or some benefit (welfare, driver's license) with no concern about how the information will be used or who will have access to it. Persons may choose to be in places where they know such surveillance is present—in city streets or shopping malls. Surveillance may be welcomed because it is benignly presented as a means of protecting people from crime.

Former President Nixon was unsuccessful in his attempt to require all television sets sold in the United States to be equipped with a device that would permit them to be turned on from a central location. The purpose was to warn the public in the event of a crisis or disaster.

Persons found guilty of crimes may agree to surveillance rather than an alternative such as confinement. In one ongoing U.S. experiment, an electronic bracelet is worn by persons who are confined to their homes rather than prisons [see THE FUTURIST, December 1984]. If they go beyond a few hundred feet from their home, or take off the bracelet, a message is sent to a central monitor.

New Technology and Laws

Even when we have the desire to limit intrusions, technology often develops faster than we can control

TOM CHALKLEY

appearances. Students are instructed on "the use of disguises, cameras, citizens band radios, tape recorders, binoculars that 'see' in the dark, and microphones that block out background noise as the suspect talks," says the *Boston Globe*.

A Surveillance Society

Today's surveillance technology can prod ever deeper into physical, social, and personal areas. It hears whispers and penetrates walls, windows, clouds, and darkness. The technology also covers not only deeper, but larger areas. Previously unconnected surveillance threads now are woven into gigantic tapestries of information. Broad new categories of persons and behavior have become subjects for information collection and analysis.

The categorical monitoring associated with video cameras, metal detectors, electronic markers on consumer goods and even library books, and the computer are creating a society in which everyone, not just a few suspects, is a target for surveillance.

Our infatuation with technical progress and the positive uses of many surveillance devices can mask the negative side. With a different government and a more intolerant public, the same devices could easily be used against those of the "wrong" political ideology, ethnic groups, religious minorities, or those with lifestyles that offend the majority.

But even without this danger, the low visibility of surveillance technology makes privacy much more difficult to protect. Forms of technology that once required the subject's cooperation, such as lie detection with polygraph, can now be done surreptitiously, as with a hidden voice-stress analyzer.

And with computer technology, one of the final barriers to total control is crumbling—the inability to retrieve, aggregate, and analyze vast amounts of data. Inefficiency is losing its role as the unplanned protector of liberty.

The first task of a society that would have liberty and privacy must be to guard against the misuse of physical coercion. The second task must be to guard against manipulation. The subtle ways in which surveillance technology threatens us make guarding against manipulation the more difficult task.


CCS COMMUNICATIONS CONTROL, INC.

Concealed tape recorder in a briefcase can be operated without the knowledge of others in the same room.

About the Author

Gary T. Marx is a professor of sociology at the Massachusetts Institute of Technology.