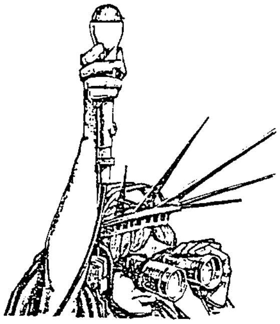

# Are We Becoming a Maximum Security Society?

## WE'RE ALL UNDER SURVEILLANCE
## High-Tech Snooping puts Democratic Principles at Risk

GARY T. MARX, MIT

The Soviet Union's use of an invisible chemical dust to monitor the whereabouts of Americans raised eyebrows last summer. Yet this technique is only one in a broad family of methods that are revolutionizing surveillance — and not only in the Soviet Union. Their application in democratic societies should raise serious concern about whether the principles of liberty and privacy will endure.

Consider, for example, the electronic "leashes" marketed for children and convicts. One device consists of a tiny transmitter (complete with animal and balloon decals) that fastens to a child. A monitor gives off an alarm if the child goes beyond a specified distance. An electronic anklet that signals a central computer if the device is removed, or if the wearer goes more than a short distance from home, is being tested on probationers. Beepers can be covertly attached to cars or property without a warrant.

Other devices measure people's internal states as presumed indicators of behavior. Police in New Jersey are testing a machine that scans brain waves to detect drug use. Virginia police are testing a "passive electronic sensor" in a flashlight that automatically measures alcohol levels in the breath when merely pointed at a person. There are a variety of other new "truth verification" mechanisms that draw inferences from voice microtremors and stomach flutters.

Satellites, mini-radars, conventional aircraft and night-vision devices have greatly extended visual surveillance. Subminiature tape recorders the size of a match box and video cameras the size of a deck of cards facilitate covert surveillance. By picking up sound vibrations on a window, lasers and parabolic mirophones permit eavesdropping without physically entering the premises. Current efforts involving computer speech recognition are likely to further enhance surveillance.

Certainly some of these innovations may prove impractical for routine use. The average American may never encounter them. But this is not the case with other forms of surveillance because broad new categories of persons and behavior have become fit subjects. The categorical monitoring associated with computers, video cameras, metal detectors, urine analysis for drug screening and electronic markers on consumer goods and even library books, is creating a society in which everyone, not just those that there is some reason to suspect, is a target for surveillance.

The new domestic forms of surveillance have been generally welcomed by business, government and law enforcement. Stirring examples of their effectiveness are readily available: The elderly heart-attack victim who was saved when her failure to open the refrigerator sent an alarm through her telephone to a centralized monitor, or the monitoring of factory compliance with pollution emission standards through satellite photography. Computer matching of everything from fingerprints to Social Security numbers may be saving taxpayers' dollars. Americans seem increasingly willing, even eager, to live with intrusive technologies because of the benefits that they expect to result.

There has been insufficient attention to the negative aspects of these trends. One of the most important involves implications for privacy. Traditionally, to invade privacy required crossing an intact barrier, be it physical or temporal — doors, darkness, someone's "forgotten" past or the right to remain silent. We tend to take these privacy supports for granted without realizing how technology is making them irrelevant.

Privacy is also difficult to protect because much of the surveillance either is almost impossible to detect or truly invisible. Counter-surveillance devices that can locate a tap on a telephone wire because of a change in electrical current, for example, are useless in locating the interception of microwave and satellite transmissions. Techniques that once required the subject's cooperation, such as the polygraph or breath analyzer, can now be used surreptitiously and/or involuntarily, as with the voice stress analyzer.

The need for new approaches to protect privacy is clear when the nature of these intrusive technologies are considered. The things we wish to keep private increasingly consist of intangible information stored in large bureaucracies rather than in our desk drawers; and telecommunications are increasingly sent in legally and technically unprotected digital form via microwave and satellite transmissions.

A report on electronic surveillance and civil liberties released by the Congressional Office of Technology Assessment makes it clear that new technologies have outstripped existing statutes and policies. There are no easy answers. But if we are to remain a society with individual liberty and limits on government, there must be greater awareness of the changing nature of privacy and emerging threats to it.

*This is an article written by our speaker and published by the LA Times on December 1, 1985.*

GARY T. MARX

Gary T. Marx is Professor of Sociology at MIT. He has taught at Harvard University and the University of California at Berkeley. He is currently involved in research on technology and society with a particular interest in civil liberties and privacy questions. His most recent book is *Undercover: Police Surveillance in America.* His articles have appeared in a large number of academic and popular publications and his work has been translated into Japanese, French, Italian and Spanish. He has been a consultant to several national commissions, the House Committee on the Judiciary, the Justice Department, the General Accounting Office, the Office of Technology Assessment, foundations and state and local governments. He has received grants from the Guggenheim Foundation, National Institute of Justice, National Science Foundation and the Center for Advanced Study in the Behavior Sciences.

The meeting of the Social Implications of Technology Chapter is scheduled for 6:00 pm on Monday, November 21, at MIT Room 4-149 (enter from Mass Ave. through the main entrance, walk straight down the main corridor past the Cashier's Office, about halfway, and turn right at the next hallway). A dinner will be held after the meeting at a local restaurant to continue the discussion. For more information call IEEE-SSIT chair Alex Brown at (617) 435-6851.