1972

The Coaxial Wiretap: Privacy and the Cable

Jerrold Oppenheim

Follow this and additional works at: http://digitalcommons.law.yale.edu/yrlsa

Part of the Law Commons

Recommended Citation
Available at: http://digitalcommons.law.yale.edu/yrlsa/vol2/iss3/11

This Article is brought to you for free and open access by Yale Law School Legal Scholarship Repository. It has been accepted for inclusion in Yale Review of Law and Social Action by an authorized administrator of Yale Law School Legal Scholarship Repository. For more information, please contact julian.aiken@yale.edu.
The revolution in science now requires thoughtful political change, not piecemeal and temporizing adjustments. If we delay too long . . . , the science establishment might become an acute threat rather than a rich benefit to our democratic system. An enlargement of individual freedom . . . is more likely to be produced through the rational ordering of scientific activity than through maintaining its subsidized disorder. It took almost a century to learn this lesson and to devise flexible controls over our economic activity. Let us hope that the lead-time will be greatly reduced when we come to experiment with effective political controls over the nation's scientific and technological assets.


The Coaxial Wiretap: Privacy and the Cable

Someday we may be shopping, banking, taking medical examinations and reading over cable television. Terminals will be installed in every living room, just as telephones and televisions are today. The cable will have two-way capability that means while you are watching the hockey game, your TV set may be keeping track of you. The cable system manufacturers' boasts are ominous: "[I]t is essential that it be kept in mind that the TOCOM (cable TV) system . . . does have the capability of interrogating literally any information at remote points and transmitting this information back to a Central Data Terminal." As the advertising literature for this new system points out, its computer "is programmed to determine if the TV Receiver is on or off and what channel has been selected." The use of technology to invade privacy is not new, of course. Cable TV, in fact, will simply be the latest in an array of implements which rob us of our right to be solitary. The average American is the subject of 10 to 20 dossiers in government and private files. Files are maintained by the Justice Department (including the FBI), the Army, Internal Revenue Service, Passport Division, Social Security Administration, state and local police, welfare agencies, motor vehicle departments, and credit bureaus. The Association of Credit Bureaus alone keeps 105 million dossiers—thus accounting for at least half the American population.
The Army maintains files on the membership, ideology, program, and practices of virtually every activist political group in the country. These include not only such violence prone organizations as the Minutemen and the Revolutionary Action Movement (RAM), but such non-violent groups as the Southern Christian Leadership Conference, Clergy and Laymen United Against the War in Vietnam, the American Civil Liberties Union, Women Strike for Peace, and the National Association for the Advancement Colored People.

In Illinois even Senator (then candidate) Adlai Stevenson III and Congressman Abner Mikva were watched.7 When you make a reservation on American Airlines, it is recorded on a computer so that a seat will be held for you. According to a magazine report on the airline’s system: “American’s computer can be queried about any traveler’s movement in the last two or three months... 10 to 15 investigators a day (Federal, state, local and other) are permitted to delve into the computer for such information.”8 Thus investigators can and do determine who sat next to you and with whom you stayed in each city of departure (you leave a contact telephone number with the airlines). Similar information may be revealed by the computer which keeps track of your credit card purchases.

Computers and other technological developments have contributed substantially to the snoopers’ standards of living. But the secret police must be holding their collective breath for cable television.

The TOCOM cable system described above can interrogate up to 180,000 home televisions in 30 seconds. Then, according to its manufacturer, “based upon information received from the Remote Transmitter Receivers, we can automatically alert the police department.”9 “Since we can determine who is turned to what channel... If customer 741 in Group 1 turns on his switch and turns to Channel 13... at 10:30 in the morning then we will know within 30 seconds of when he turns his set on... and likewise we will know within 30 seconds of when he changed to a different channel.” “For the future of the system, with very little modification,” the same manufacturer says, “we see the capability of... the control of devices at remote locations... we may in one condition disable every remote home transmitter receiver throughout the system... or we can, by transmitting an identification code, along with a separate code, selectively enable or disable each respective remote transmitter unit.”9

This future is not very far away. The president of K’Son Corp., an electronics firm in Fullerton, California, recently wrote about a new piece of equipment of which he is very proud:

> It automatically responds to interrogations from the head-end with information on what channel is being watched and when. Also it has the built-in capability of being turned on and off from the head-end by the transmission of a unique code.10

A similar unit is currently being used experimentally on the Sterling (Time-Life) cable system on the southern portion of Manhattan. Sterling’s computer can determine whether or not an identified television set is on and to which channel it is tuned.11 Tokyo’s Takanaw Prince Hotel uses its cable TV system to monitor the missing contents of room refrigerators, thus simplifying its billing procedures.12 Not long ago, President Nixon suggested a civil defense warning system that would automatically turn on every radio and television in the nation and, of course, tune them to the same emergency message. He did not say what might constitute an “emergency.”

Viewers of the experimental cable system in Dennisport, Massachusetts, select programs by dialing on an instrument similar to a telephone. Each dial moves a mechanical switch in the central office and anyone sitting in that office can see exactly to which channel every set is tuned and whether or not each set is on. Furthermore, there is no safeguard against a person in

Jerrold Oppenheim is chairman of the Cable TV Committee of the ACLU in Illinois and Electronic Media Editor of the Chicago Journalism Review. He is a graduate of Harvard College and Boston College Law School.

http://digitalcommons.law.yale.edu/yrlsa/vol2/iss3/11
the central office moving the mechanical switches until each set is tuned to the channel he has chosen. 13

Cable television may become the method of distribution for library books, newspapers and news magazines within 20 years. 14 One of the simplest things for a cable system to record will be the names of books and periodicals each household has requested. Similarly, a system could monitor political speeches watched. Senator Samuel J. Ervin has recently warned:

When people fear surveillance, whether it exists or not, when they grow afraid to speak their minds and hearts freely to their Government or to anyone else, then we shall cease to be a free society. 15

"The right to be let alone," echoed Justice Douglas, "is indeed the beginning of all freedom." 16 Each individual has, in the words of the Restatement of Torts, a protected "interest in not having his affairs known to others." 17 Canadian Justice John Turner explains the problem clearly:

"The right to dissent becomes a very difficult right to maintain if there aren’t those areas in which one can discuss without the fear of being overheard. A democratic policy depends on a lot of confidential relationships, conversations, the ability to muster support in private, and so on." 18

Surveillance, or the threat of surveillance, makes men circumspect. Citizens engaged in unpopular activities are especially vulnerable. In fact, FBI surveillance has been used in the hope of producing a chilling effect on dissenter activity. FBI agents, for example, received instructions to increase the frequency of interviews of New Left members because "it will enhance the paranoia endemic in these circles and will further serve to get the point across that there is an FBI agent behind every mailbox." 19

It was not very long ago that I. F. Stone was explaining to his readers:

Since you never know what organization may some day be regarded as suspect, better join none. Since almost any cause may some day be regarded as subversive, better keep away from all. Since there are now informers everywhere, including the campus, say as little as possible, avoid the discussion of dangerous subjects. Be careful what books you have in your library and what publications you read. These may be held against you. 20

Stone went on to report instances of government excesses. McCarthy’s famous list of subversives included a man in whose raincoat pocket were found Russian lessons and a man who had signed a “radical” petition. A woman was held up to public ridicule for buying one copy of the Daily Worker. An economist died in the midst of deportation proceedings brought because he was on a 31-year old Communist membership list. "A man who had once worked for Amtorg, with two sisters in Russia, whose name had been on the mailing list of several 'front' organizations during the war would never be freshly hired." Men were refused military commissions because their mothers had once belonged to the Communist Party. HUAC kept up-to-date a Guide to Subversive Organizations and Publications for one’s reading guidance. "Aliens found themselves deported; foreign-born citizens, denaturalized; citizens, blacklisted, on the basis of allegations which often included the reading of the Daily Worker." 21

New York Civil Liberties Union attorney Burt Neuborne recently summed it up: “The tone of spontaneity of spirit that characterizes a free society cannot survive in an atmosphere where all deviations from the norm are immediately noted by the state and stored for future reference.” 22

Fortunately, there is some legal support for that position. 23 "Privacy," Justice Douglas has written, "though not expressly mentioned in the Constitution, is essential to the exercise of other rights guaranteed by it." 24

Douglas’ opinion in Griswold v. Connecticut spelled out the Constitutional theory behind the right of privacy:

[The First Amendment has a penumbra where privacy is protected from governmental intrusion. . . . The right of "association" like the right of belief [citation omitted] is more than the right to attend a meeting; it includes the right to express one’s attitudes or philosophies by membership in a group or by affiliation with it or by other lawful means. Association in that context is a form of expression of opinion; and while it is not expressly included in the First Amendment its existence is necessary in making the express guarantees fully meaningful. . . . Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people. . . . The Fourth and Fifth Amendments were described in Boyd v. United States as protection against all governmental invasions "of the sanctity of a man's home and the privacies of life." 25

Just how far this Constitutional right of privacy can be carried in still a subject of hot judicial dispute. 26 It is said, for example, that the federal right of privacy is left to the states to protect, along with the protection of safety and property. 27

Wire tapping—which presumably would include interception of pictures, of orders placed, or of programs billed on cable, though the question has never been raised judicially 28—is restricted by the Communications Act of 1934. 29 Furthermore, conversation is protected by the Fourth Amendment against unreasonable seizure even where there is no physical trespass. 30 In fact, damages are recoverable. 31 The Communications Act even prohibits the mere registration of numbers called where there is no recording of conversation. 32 In addition, harassment by means of persistent and unwanted telephone calls has been held to be an actionable invasion of privacy. 33

But the President may authorize a tap in the interests of "national security," 34 and a judge may do so under a wide variety of circumstances. 35

Published by Yale Law School Legal Scholarship Repository, 1972
Apart from the restrictions against wiretapping, there is a body of law restricting visual surveillance by any means electronic, mechanical or in person. But the doctrine is hedged by the necessity to prove actual damages and to prove an obtrusive invasion that would be offensive to a person of ordinary sensibilities. Thus, if the federal and/or state wiretap statutes do not apply to cable-tapping, the present eavesdropping law barely deals with the problem.

The legal protections which do exist have not been a terribly effective shield against invasions of privacy, especially by governments. There is no reason to believe present law will work any better after the introduction of two-way cable television.

With two-way cable TV so close on the horizon, it is surprising and disappointing that so little attention has been paid to the privacy issue. The Illinois Commerce Commission, for example, held extensive hearings on cable television last spring. The Commission heard from three highly qualified engineers, its own very able and public-spirited technical consultant, and representatives from two of the most substantial cable TV equipment manufacturers. It also received extensive testimony from four scholars of law and communication. None of these people presented information relating to the protection of privacy. Of those cross-examined, not one had given any serious thought to the problem.

Similarly, the Federal Communications Commission has not formally considered the protection of privacy on cable TV, although it has received information on the subject.

The worst record is at the municipal level—where most of the regulation of cable television currently takes place. In Chicago, for example, Alderman Paul T. Wigoda held four days of hearings on cable regulation, during which he heard from one engineer (who merely offered his services and sat down), no manufacturers and scholars. Other cities have not even had hearings.

Agencies such as the American Civil Liberties Union are overburdened. ACLU is pressing its battle against political surveillance, but few people, if anyone outside the FBI, are paying attention yet to cable TV as an instrument of that surveillance.

Yet there are some reasonably simple technological protections available. For example, under questioning before the Illinois Commerce Commission, one manufacturer (who had not thought about the problem before) estimated that one-fourth of a system could be effectively set aside and made relatively private for an increase in construction cost for the entire system of about 7%—an addition of perhaps 70 cents to a $10.00 monthly charge. The technology for this is reasonably simple. For example, Gulf-Western Industries has a scrambling system (used also for Pay-TV) which costs $25.00 per unit to manufacture. For even less, a cable operator can install a light and bell which will notify the subscriber when his television is being monitored to determine which channel is being tuned. A switch to prevent such monitoring is also inexpensive. The Illinois Commerce Commission is proposing to require both devices. It may even be feasible to construct an inexpensive home device which would detect most, if not all, taps of telephone or cable lines.

In fact, according to the Electronic Industries Association, the electronic manufacturers' trade group, a cable "network . . . can enjoy any desired degree of privacy that can be economically justified." However, whatever a clever engineer can devise to protect privacy on the cable, an equally clever engineer can undo. Thus, at best, you are guaranteed of being monitored (i.e., surveyed as to channel watched, cassette requested, etc.) and tapped (overheard) on the cable only by professionals. Perhaps that is better than no privacy at all. Yet, in the long run it may be the "professionals" who concern us most of all.

Certainly, if a portion of the cable spectrum is reserved, by statute or ordinance, for private communications, then scrambling devices of relatively high sophistication should be installed on these channels. In addition, locks and armored cable should be installed to deter access to terminal boards and cable drops from pole to house and within the house. Anyone who has prowled around in basements knows how easy it is to tap into a naked telephone line strung along the beams in the cellar below an apartment or office building.

Technological solutions of this character are feasible if they are built into the system when the system is constructed, but they are worthwhile only if methods for circumventing them are not built into the system or added later. Legislation is clearly in order, since there is little incentive to the operator either to include such solutions in the cable system or to prevent their circumvention.

While legally required technological protections will discourage monitoring and tapping, they should be supplemented with purely legal protections. For one thing, disclosure of information obtained via cable could be forbidden or allowed only after notice and opportunity to refuse consent. No disclosure would be permissible except with express consent (which might even be bought, as, for example, by audience rating services). Consent would preferably be required at each occasion (simply a matter of pushing a button on a two-way cable set) and in either case should not be made a condition of subscribing to a cable service. Minimum mandatory penalties should be high and enforceable either by the District Attorney, the FCC or the injured individual. Indeed, new rights of action should be specifically established—invasion of privacy by unauthorized monitoring or tapping of a cable.

One problem in enforcing such a right is detecting when information is being obtained from the cable. In the case of monitoring, detection is relatively simple since an interrogating signal must be sent to the set. Taps
of the cable, on the other hand, are extremely difficult to detect, since tapping merely deflects a minute proportion of the transmitted signal. Only very expensive, sophisticated equipment can detect the presence of the tap. Because of this, tapping can probably only be eliminated by rigorous policing, a function which can be performed most efficiently by the operator of the system himself.

The operator of any cable system must maintain the physical security of the cable to insure adequate service to subscribers; he therefore is in a position to provide at least coarse physical surveillance against taps. Furthermore, to prevent pirating of his own signal the operator will have to install sophisticated electronic gear to detect any loss of signal due to unauthorized connection of additional sets to a cable terminal in a home. It is an easy additional function to attune such equipment to detecting taps which invade the privacy of the subscriber.

To encourage operators to do this policing, it might be appropriate to reward him for each tap he detects. To increase incentive, the operator could be strictly liable in tort to all persons whose communications are monitored or tapped. High mandatory punitive damages assessable no matter what the actual damages could be included under such liability.

The telephone company apparently cares little whether its lines are tapped. In fact, it cannot even get excited about unauthorized use of telephone credit cards. Obviously, Bell has no economic incentive to worry about the right of its subscribers to privacy. With sufficient incentive, Bell could be quite efficient about smoking out taps on its lines.

There is no reason why telephone subscribers should not be protected in a similar way. But such protection may be more important in the case of cable. First, the cable subscriber may come to rely on his new instrument for functions which his telephone cannot perform. Most people, for instance, prefer their medical examinations and banking transactions to be maintained in utter secrecy. And few relish the thought of a government agency having ready access to a list of a person's reading material. Cable TV will make these and other functions terribly more convenient to the subscriber, since cable will supply visual as well as audio information.

Secondly, in comparison with the telephone, cable provides a significant increase in convenience to those who want to tap the cable. For instance, in a number of applications of two-way cable, information will be solicited from all subscribers at one time; telephone inquiries, on the other hand, are singular and occur at random intervals. Furthermore, due to the nature of the wiring and switching systems employed with cable, and the fact that most cable messages will contain an identifying code, large scale tapping on major cable trunk lines will be far easier than in the case of the telephone. These factors alone provide the "tapper" with a previously unknown efficiency, increasing significantly the likelihood of invasions of privacy via cable.

Since most of tomorrow's cable systems are not yet built, especially in the bigger cities, it is relatively easy now to build in protections of privacy such as scramblers and warning signals. It is possible to add these safeguards later—as it is theoretically possible to add similar protection to the telephone system—but it is more expensive in both technological and political costs. There is no reason to think that the government will act any differently about the cable than telephone lines.

The social benefits of two-way cable television could be immense, just as the telephone has been a great boon. But—just as with the telephone—cable TV will open vast new opportunities for privacy invasion.

Certainly there is no technological way to prevent all such invasions. And legal prevention depends in the last analysis on enforcement of existing law. Therefore, my parting word is Jefferson's: vigilance. Not only must we act now to protect the security of our private thoughts and lives against the curiosity, suspicion and paranoia of our government and our neighbors. But, even having acted, we must not assume that the problem is solved.


3. Prof. Arthur Miller (University of Michigan), Hearings before Senate Subcommittee on Constitutional Rights (Senator Erwin, Chairman), March, 1971, reported in press.

4. Id.


7. Interview with John O'Brien, former Army intelligence officer (February, 1971).


10. Cable News 3 (February 12, 1971).


13. Personal observation, Sept., 1970. At least the sets cannot be taken from the central office.

14. For example, Chicago Tribune Editor Clayton Kirkpatrick recently wrote that he thinks that the newspaper "might eventually be reproduced on screens which could be read in the home. There might be provisions for reproducing portions of news which might appear on the screen through an instant facsimile process so that any part of the written record could be taken off the screen for study, filing for future reference, or passed on to others who might share the same interest." Big City Newspaper, Chicago Tribune Educational Services Dept. (1971).

15. The Progressive, 23 (June, 1971).

16. Dissenting in Public Utilities Commission v. Pollack, 343 US 451 at 467 (1952). "The makers of our Constitution... declared, as against the Government, the right to be let alone—the most comprehensive of rights and the most valued by civilized man." Brandeis dissenting in Olmstead v. US, 277 US 438, 478 (1928).


21. Id. at 26-33, 75-86, 253.

22. Constitutional Rights Hearings, supra at note 3.

23. A more thorough treatment of the subject of privacy will be found in e.g. W. Prosser, Torts (4th ed. 1971) sec. 117; R. Pound, The Fourteenth Amendment and the Right of Privacy, 13 W. Res. L.R. 34 (1961); Restatement, Torts (1939), sec. 867.


28. 47 USC 605 prohibits unauthorized reception of "any... communication by radio" (except general broadcasts) if information gained thereby is used or divulged improperly. Interception of wire communications is not explicitly prohibited, although divulging the contents of a "communication by wire or radio" is restricted. See also 18 USC 2511. Is cable television communication by wire or communication by radio?


31. Rhodes v. Graham, 238 KY 225, 37 SW2d 46 (1931) (no statute). 18 USC sec 2050 permits punitive and actual damages as well as costs. Actual damages are liquidated at $100 per day, minimum $1000.


34. 18 USC sec 2511 (3).

35. 18 USC sec 2511 (a).


39. For example, the Illinois statute prohibits using a device to "hear or record oral conversation" and arguably does not deal with pictures. Ill. Rev. Stat. c. 38 sec 14-1.


41. Irving Kahn, former President of TelePrompter Corp. (largest US cable operator), predicts four years from now. Oral remarks, Beardsley Ruml Colloquium, University of Chicago.

42. Docket No. 56191 Proposed rule (January, 1972). The transcript is about 2800 pages long, excluding exhibits.


45. Unpublished data collected from transcripts, which are available at Chicago City Hall, Room 302.


48. Donald G. Chandler, executive vice-president, Electronic Industrial Engineering, Inc. (N. Hollywood, Calif.), April 11, 1971, estimated that the allocation of three private channels on a 12 channel system would cost about $10 out of a total per subscriber construction cost of about $150.


50. Docket 56191, supra, at note 42.

51. Comment to FCC, supra, at note 43.


53. E.g., 18 USC sec 2511 with regard to illegal wire-tapping. The common law has dealt with such problems as announcements of unpaid debts, Brents v. Morgan, 221 Ky 765, 299 SW 867 (1927), revivals of lurid past, Melvin v. Reid, 112 Cal App 285, 297 P 91 (1933), and the distribution of medical pictures, Banks v. King Features Syndicate, 30 F Supp 352 (SDNY 1939). But distribution must be to a large number of people, eg. Brent v. Morgan, supra, Melvin v. Reid, supra, French v. Safeway Stores Inc., 247 Or 554, 430 P2d 1021 (1967).

54. 18 USC sec 2520 provides $1000.

55. The dynamics of cable tapping become even more disconcerting when one considers the quality of information which could be obtained from broadcasting a series of programs which cover a predetermined range of political perspectives. By noting when the viewer quits tuning in the series of programs which progressively move further and further toward the fringes of acceptable political behavior, the "tapper" identifies the private political biases of each viewer. Computer analysis of individual viewer habits could develop complex yet reliable indicators of private personal political preferences. Similar analyses could be done of other personality profiles.

7
columbia survey of human rights law

VOLUME III

"State Remedies for Racial Imbalance"

"Federal Law and Indian Tribal Law"

"Conspiracy: Instrument or Weapon"

"Invalid Disruption Rules for C-O Alternative Service"

$4.00
Columbia Survey of Human Rights Law
Columbia University School of Law, Box 54
435 W 116th Street
New York, New York 10027