ELECTRONIC SURVEILLANCE: SETTING THE LIMITS†

E.P. Craig*

A NECESSARY BUSINESS

In his famous dissenting judgment in *Olmstead* v. *U.S.*[1] Oliver Wendell Holmes characterized wiretapping (and by implication all forms of electronic eavesdropping) as "a dirty business".

Ramsey Clark, former Attorney General for the United States of America, takes the position that the use of electronic eavesdropping by the police is inefficient and unnecessary, corrupting those who engage in it.[2]

With respect, both men are wrong —the former made wrong by changing times, the latter mistaken *ab initio.*

Electronic eavesdropping may now well be *the* most efficient way of combatting crime, especially organized crime. Criminals communicate verbally. There are no written records to seize, so their verbal communications — their weakest point — must be attacked. In the majority of cases there are no informants and it is impossible to get information in any other way.

In short, electronic surveillance is now a necessary business and, almost by definition, no longer a dirty one —the latter implies the luxury of an alternate choice, which is no longer true. It is becoming more and more apparent that society must engage in this form of eavesdropping to the extent found necessary to protect itself. It is the bounds of this extent, not the question of whether or not society ought to engage in such activity, with which we must be concerned.

THE DEVICES

When George Orwell wrote "1984"[3] he surfaced the possibility of total surveillance of individuals for an indefinite period

---

† Partially based on an address delivered October 25, 1974 to the University of New Brunswick Law Students' Society. The views expressed are the author's and not necessarily those of his employers.

* E.P. Craig, B.A., LL.B. (U.N.B.), temporarily in charge of the Royal Canadian Mounted Police Legal Branch, Ottawa.

1 *Olmstead* v. *United States* (1928), 277 U.S. 438.

2 Ramsey Clark, *Crime in America* (1970).

3 George Orwell, *Nineteen Eighty-Four* (1949).

of time. Twenty five years ago the idea was pure fantasy; it no longer is.

Only five years ago microphones half the size of an ordinary cigar were still being used to secretly intercept private conversations;when these "ancient" devices were implanted, a determined "bugee" could sometimes find the exposed end of microphone the size of a dime.

No more! Now a common household thimble can hold up to EIGHT extremely sensitive microphones, each capable of excellent reproduction of the human voice up to distances of 50 feet. Each is concealable so not even a pinhole need show!

Other means of eavesdropping which have developed to date, however, are not nearly so efficient and claims concerning their potential are often exaggerated.[4] There are physical barriers which, so far, are very effective in keeping limits on surveillance. Let's look at the present state of the art.

There are three broad categories of electronic surveillance devices. There are effective devices (those that work very well), ineffective devices (which will work but are impractical) and future devices (those that don't work — yet).

The effective devices include telephone taps, modified existing electrical sources (telephones, intercoms), reflectors activated by microwave beams through solid walls, tagging devices on vehicles (the so called "bumper beepers"), small radio transmitters and miniature microphones.

The impractical devices are those designed to pick up vibrations created by voices and convert them into speech (contact, radar or laser microphones). They also include directional microphones. The problem is interference, making their use unsatisfactory in practice, although they *will* work under perfect conditions.

Another technique, grossly exaggerated as to its effectiveness, is the "tagging" of individuals by secretly concealing miniature radio transmitters on their persons. Although we can miniaturize microphones, transmitters and receivers, to date we cannot do the same for power sources, especially batteries.

However, tremendous technological advances are still possible in the future. These include the perfection of tagging devices which will make it possible to monitor an individual 24 hours a day, miniature TV lenses which will permit visual surveillance,

---

4 As an example see Alan F. Westin, *Privacy and Freedom* (1967). Chapter Four deals with new techniques of physical surveillance but does not accurately portray limitations on the effectiveness of existing technology.

long range photography, use of lasers and even aerial viewing and listening devices with hovering capabilities.[5]

Some say "1984", others say the year 2000, but sooner or later there will be no limit to the degree of surveillance possible. In the continuing transition from science fiction to reality the physical barriers which are our natural protection will disappear. We must then look to an artificial protection, the law, to define the permissible degree of invasion.

THE LAW

Until very recently the existing law was in a most unsatisfactory state. English and Canadian tort law failed to develop a cause of action for invasion of privacy, creating a ". . . notable gap in our legal armoury".[6] Some provinces filled the gap by legislatively creating torts;[7] another solution was the creation of quasi-criminal offences in some provincial Telephone Acts.[8] But criminal sanctions were almost non-existent.

The *Protection of Privacy Act*[9] is the first attempt to set the limits by federal legislation. It is described in detail elsewhere.[10] Generally, the Act is designed to establish control over the kind of eavesdropping achieved by artificial aids or enabling devices referred to in the Act as "electromagnetic, acoustical, mechanical or other devices", thus taking direct aim at electronic eavesdropping. Its basic approach is the forbiddance of all artificially aided interceptions of private communications (protection of the individual) with the provision of limited exceptions for law enforcement (protection of society).

It was the quest for the proper balance between the protection of individual privacy and the security of the state that was one of the major factors delaying passage of the Act for a number of years. In the end a compromise was reached with which no one is completely satisfied. Some are unhappy because the practice was not totally forbidden; others feel the police are unduly fettered. One thing is certain —the ban on electronic eavesdropping by the *public* was long overdue!

---

5 *Ibid.*, 85-89.

6 John G. Fleming, *The Law of Torts*, 4th Ed. (1971), 533.

7 *Privacy Acts*, Stats, B.C. 1968, c.39; Stats. Man. 1970, c.74; Stats. Sask. 1974, c.80.

8 See in particular the *Manitoba Telephone Act*, R.S.M. 1970, c.T40; *Alberta Government Telephone Act*, R.S.A. 1970, c.12.

9 *Protection of Privacy Act*, Stats. Can. 1973-74, c.50, afterward interchangeably referred to as the *Privacy Act*. It became law on June 30, 1974.

10 See Morris Manning, *The Protection of Privacy Act* (1974); E.P. Craig,"The Protection of Privacy Act" (1974), 36 R.C.M.P. Gazette No. 4, 2.

PUBLIC MISUSE

Some of the factors which accelerated public use and misuse of electronic eavesdropping devices in recent years were the growth of the private detective trade, simplification of equipment and techniques, miniaturization, a decrease in cost, and aggressive promotion —all in the absence of legal controls.[11]

While the existance of misuse is certain, its true extent is unknown. In Canada some insight may be gained from the Sargent Report[12] —the result of a judicial inquiry into the use of listening devices by private business firms and private detectives in British Columbia. Among other things, the inquiry disclosed secret monitoring of conversations by car dealers, dance studios, real estate agencies, finance companies and health spas. The reasons for monitoring included protection of employees, checking sales methods and listening to customers to find out what factors would induce purchases or signing of contracts. For example, it was a common practice for a car dealer to leave a man and his wife "alone" in a sales booth where a modified intercom would often reveal the price to which they would go to buy a car. In the United States the nature, if not the extent, of use and misuse by the public is well documented in Alan F. Westin's book, *Privacy and Freedom.*[13]

There was extensive use of electronic eavesdropping, especially by private business, for three basic reasons. The first was industrial espionage, the attempt to gain an edge on competitors. The second was internal monitoring of executives and employees to check efficiency or to prevent theft. This could be extensive; Westin cites as an example the fact that the American Telephone and Telegraph Company monitored 36 million long distance calls in 1965.[14] The third reason was surveillance of customers to control shoplifting or to increase sales by finding out what the customer was thinking. An extreme example of the latter was the bugging of a casket selection room![15]

Westin also documents the use of electronic surveillance by professionals, in schools and universities, in personal, family, civil and political matters, by scientific researchers, by manage-

---

11 Westin, 90.

12 British Columbia, Report of the Commission of Inquiry into Invasion of Privacy (1967), commonly known as the Sargent Report.

13 Westin, 104-118.

14 *Ibid.*, 113.

15 *Ibid.*, 112.

ment and labour, and even in the courts.[16]

The full extent of private use, as mentioned, is impossible to estimate. Without doubt it was fast becoming a recreational pastime before laws to curtail the practice were passed. One small insight came from an American manufacturer of electronic eavesdropping equipment, which stated that out of total sales of $30 million by his company in 1965, $4 1/2 million came from sales in Canada.[17] Even if over-estimated by half, it is still a frightening figure!

POLICE USE

When we talk about the police use of electronic eavesdropping devices prior to the the *Protection of Privacy Act* we may employ the word "use" in two ways. In one sense there was *extensive* use against *criminals* — particularly those criminals involved in more serious crimes, such as drug trafficking and armed robbery. In another sense there was *limited* use, when negative influences such as lack of manpower and the expense of equipment are taken into consideration.

Security matters aside, police have used electronic investigative means only against criminals, and then only against some criminals. If a hypothetical may be used to illustrate the point: in a Canadian city with a population of 1000 criminals it might be technically possible to put only 15 under electronic surveillance at any one time!

Some of the statistics presented to the Justice and Legal Affairs Committee during its deliberation on the *Protection of Privacy Act* are illustrative. During the 10 year period from 1963 to 1973 the Royal Mounted Police conducted 1,912 electronic intrusions,[18] with wiretapping used only by consent of one of the parties. In 1972 the R.C.M.P. Security Service used wiretapping 152 times and electronic eavesdropping 84 times.[19] In Montreal, during the 16 month period from January, 1972 to April, 1973, 355 wiretaps were used, resulting in the arrest of 657 persons on 1353 criminal

---

16 In 1954-55 five jury deliberations in the U.S. were monitored with the permission of the judge and the attorneys. Intense criticism resulted in the passage of laws forbidding this practice. See Westin, 118.

17 Stanley M. Beck, "Electronic Surveillance and the Administration of Criminal Justice" (1968), 46 Can. Bar Review 643, at 646 quoting the Toronto Star, August 31, 1966.

18 Minutes of the Standing Committee on Justice and Legal Affairs, June 12, 1973, Issue No. 15, at 8.

19 *Ibid.*

charges.[20]

These figures hardly support the widespread misconceptions concerning the extent of police activity. Many members of the public believed that the use of electronic eavesdropping by the police was both indiscriminate and widespread. In fact, as the statistics indicate, it was purposeful and concentrated.

The primary purpose of police use prior to the *Privacy Act* was the gathering of intelligence. It is a truism that a police force is only as good as its sources of information. It is also true that the foremost function of the police is, or should be, the prevention of crime. Prevention of particular crimes can only be accomplished through prior knowledge; if the police learn beforehand that a crime is going to be committed they can prevent it, but if they do not, they must deal with a *fait accompli.*

There are two basic methods of obtaining information: indirectly through the informants, or directly from the source. Of the two, the direct method is far more efficient because the reliability of the data is capable of immediate evaluation. Informants are notoriously unreliable. Both methods, of course, are repugnant to a degree but there is no alternative if society is to protect itself.

The secondary purpose of police use before the *Privacy Act* was the gathering of evidence. However, there are less than a dozen reported cases in Canada where evidence obtained electronically was introduced in court; this illustrates the positive emphasis placed on obtaining intelligence.

The police, self-admittedly, were quite happy to use listening devices to find out what certain criminals were up to. Steps could then be taken to either prevent the intended crime or to catch the perpetrators in the act. This method had the distinct advantage of preserving the effectiveness of the devices — the nature and extent of their use was not compromised by testimony in open court.

In passing the *Privacy Act*, our lawmakers, in spite of strong police objections, reversed the emphasis. Evidence gathering is now the primary purpose of electronic eavesdropping and the intelligence gathering purpose is severely limited, if not curtailed completely. This was accomplished by a combination of two factors; one intentional and the other not. The former is the require-

---

20 Brief presented to the Standing Committee on Justice and Legal Affairs by the Montreal Urban Community Police. See Minutes June 7, 1973, Issue No 14, at 15. This excellent brief accurately portrayed the importance of electronic surveillance to the detection and control of crime but was largely ignored by the members of the Committee in their final report.

ment that police must know what *the* offence is before seeking permission to make an interception,[21] thus making it necessary to determine this information by other means — often impossible. The latter is the controversial necessity of notification.[22]

This reversal of emphasis, although prompted by the best of intentions, may cause many of the most serious crimes to remain undetected. In an attempt to control abuse, real or imagined, of electronic surveillance by the police, a severe price may be paid.

Before commenting further on the intelligence question, let's examine police "misuse" of electronic surveillance to see if it was irresponsible action by the police which brought on the severe restrictions of the *Privacy Act.*

POLICE MISUSE

With few recorded exceptions, the police did not use electronic eavesdropping indiscriminately. Self imposed controls (policy), together with physical limitations, served to protect the general public (and even a large part of the criminal population) from electronic surveillance. The public was in far greater danger from itself than it ever was from the police.

To be fair, however, the existence and extent of police misuse is unknown — even to the police. There are no comprehensive statistics, no scandals, no glaring examples of flagrant misuse. From all that appears on the surface one could argue that the police have used the technique with discretion and restraint and whether the reported examples can actually be classified as misuse depends entirely upon one's point of view.

In 1968 a public inquiry held in Toronto resulted in the Grant Report.[23] One author described the report as ". . . a classic example of official interference with an individual's right to privacy without due process of law."[24] The inquiry was induced by a police telephone tap on a well-known criminal, one Alexander. He was the prime suspect in a rash of burglaries and a tap was placed on his telephone after other investigative means failed. The tap was left on for two months and 60 hours of conversations

---

21 *Protection of Privacy Act*, ss. 178.12(c) and 178.13(2)(a).

22 *Ibid.*, s.178.23. All persons who are specified subjects of a judicially authorized interception of their private communications must eventually be told. The police are not seeking authorizations against some of the most highly placed criminals because the requirement of notification would probably destroy any chance of a future conviction.

23 Ontario, Inquiry Re Magistrate Frederick J. Bannon and Magistrate George W. Gardhouse (1968), commonly cited as the Grant Report.

24 Beck, 658.

were taped. The tap revealed a relationship between Alexander and a Magistrate Bannon, including discussions on dispositions and sentences in cases pending before the courts. The police felt compelled to disclose the relationship and the inquiry eventually found Magistrate Bannon totally unfit for his office.

Public reaction virtually ignored the corruption exposed and centered on demands for legislation.[25] The catalyst was the realization that the police could tap a telephone for two months with no one knowing about it, as indeed no one outside the police would have known if the fact had not voluntarily been disclosed in the larger interest of removing an unfit magistrate.

Were the police blameworthy? Did they violate any inherent right to privacy in the absence of any law forbidding the practice? The questions are now academic, but the situation certainly illustrates the reason the police welcomed the advent of enabling legislation when the *Privacy Act* was in the formulation stage.

Another example of police misuse, if it can truly be called that, is found in the case of *R.* v. *Steinberg.*[26] The police executed a search warrant on a betting house, secretly installed a recording device while there and retrieved it the next day. A conviction resulted in a sentence of three months in jail plus a fine of $10,000. On appeal the fine was reduced to $5,000 because "We are not satisfied that that which occurred has the appearance of justice and we feel that the appearance of justice is an important element to be considered in criminal matters".[27] *R.* v. *Steinberg* is but another mild illustration of the police dilemma prior to the *Privacy Act* —when, and when not, to use the devices.

A lot has been said about "fishing expeditions" in relation to the invasion of privacy by the police. An example of a true fishing expedition would be placing a listening device and waiting for anyone to come along and incriminate himself. A partial fishing expedition would be "bugging" a known criminal or a criminal haunt to find out what is going on; in other words, you know something illegal is going on but you're not sure what.

Related cases which illustrate a partial fishing expedition are *R.* v. *Pearson,* and *R.* v. *Black et al.*[28] A telephone was installed in

---

25 *Ibid.,* 648.

26 *R.* v. *Steinberg,* [1967] 1 O.R. 733 (Ont. C.A.).

27 *Ibid.,* 736.

28 *R.* v. *Pearson* et al (1969), 66 W.W.R. 380 (B.C.S.C.); *R.* v. *Black et al* (1970), 72 W.W.R. 407 (B.C.C.A.).

the clubhouse of a motorcycle gang. Telephone calls were recorded and the tapes were checked at intervals. While the tap was in place, members of the gang kidnapped a "butler", and forced him to engage in sordid and degrading acts ". . . of a disgusting character for the most part of a sexual or quasi-sexual character."[29] The gang members were convicted, partially on recordings of telephone calls. As in the case of the unfit magistrate, does the end sometimes justify the means?

This takes us directly back to the question of whether or not intelligence gathering is an integral part of police work, for partial fishing expeditions and intelligence gathering are the same thing.

Does the *Privacy Act* give any scope at all to electronic intelligence gathering? None whatsoever. The Act eliminates it completely. It requires an offence, a known quantity, before an authorization to use electronic surveillance may be sought. The difficulty, in many cases, is that the police may know something is being planned but may not know what offence is involved. Practice may modify the effect somewhat, but in theory if you don't know what the suspect is planning you shouldn't ask for an authorization.

Surely there is a concurrent, if not paramount, necessity for the intelligence-gathering function in police work. In the war against crime —a war society is in danger of losing —the taking away of the most potent weapon in the hands of the police, who are confronted already by enemies who play by no rules at all, may prove to be an extremely serious mistake. We are now in the process of finding out.

SETTING THE LIMITS: SUMMARY AND CONCLUSION

Prior to the passage of the *Privacy Act* three factors were operating. First, improved technology meant increasing availability of sophisticated listening devices, at low cost. Second, there was ever increasing use of the devices, by police *and* the public. Third, there was lack of control —very little in the nature of legal sanctions existed.

The third factor created a moral dilemma for the police. What use should be made of the new devices in the absence of any law forbidding their use? If it was not legally wrong to use them, was it morally wrong? The only guidelines, in many cases, were those formulated by police themselves. Each police force, in setting policy, had to decide how far to go. In this atmosphere the police were as anxious for legislative guidance as anyone.

---

29 *R.* v. *Black*, 411.

It soon became evident by virtual consensus that use of the devices by the public should be totally forbidden. This consensus, however, had the effect of shifting attention away from public use, where most of the abuse had occurred, and focussing it completely upon police use.

The burning issue became whether or not law enforcement agencies should ever be permitted to use electronic eavesdropping as a means of investigation. The potential for disagreement had been illustrated by a report of the President's Commission on Law Enforcement,[30] which divided its opinion. The majority approved police use subject to stringent limitations. The minority felt there was ". . . insufficient basis to strike this balance against the interests of privacy".[31] The same arguments erupted in Canada.

The Canadian Committee on Corrections recommended that the police should be allowed to use eavesdropping devices under controlled conditions.[32] In the end Parliament, after considering the moral and ethical issues, agreed and opted to strike a balance, permitting exceptions to a total ban. It did, however, severely restrict the ability of the police to prevent crime, causing concern to many that the bounds had been too narrowly set.

Electronic surveillance, to the extent which it may be legally used, is now legitimized; as such it should no longer be considered a dirty business — it is a necessary business within the limits established by law. These limits are set — for a time.

Who will determine what the limits eventually will be? We all will, at some time, directly or indirectly, whether as lawmaker, prosecutor, defence counsel, policeman, civil libertarian or just plain citizen. For the immediate future, law enforcement officers will be primarily concerned with the legal issue — operating within the limits as they now exist — and only secondarily involved with the moral and ethical issues. In the long term we must remain concerned with all three considerations, because of the inevitable revision of the *Protection of Privacy Act.* Experience will then tell us whether we must cut back or extend the degree of electronic surveillance now allowed.

---

30 United States, *The Challenge of Crime in a Free Society.* Report by the President's Commission on Law Enforcement and Administration of Justice. Washington (1967).

31 *Ibid.,* 203.

32 Report of the Canadian Committee on Corrections (1969), 83, commonly known as the Ouimet Report.