1967

# Wiretapping and Bugging: Striking a Balance between Privacy and Law Enforcement

Kent Greenawalt
*Columbia Law School*, kgreen@law.columbia.edu

# *Wiretapping and Bugging:*
# STRIKING A BALANCE BETWEEN PRIVACY AND LAW ENFORCEMENT

*Kent Greenawalt*

The conflict between individual privacy and the needs of law enforcement occurs at a number of points in our system of criminal justice. It is not unique to wiretapping and electronic eavesdropping, but the competing claims in that area do have their own special character. They are qualitatively different from those in regard to, say, confessions. The kinds of crimes and criminals affected are different, as are the relevant assertions about individual freedom.

Law enforcement officials, almost to a man, consider wiretapping and eavesdropping valuable weapons in the fight against crime. They are most helpful in regard to consensual crimes and crimes of a continuing nature, such as gambling, prostitution, narcotics offenses, and abortion. Electronic surveillance may also be effective in extortion and kidnapping cases, but in the ordinary situations at least, the victimized party will consent to police overhearing. The claim that using electronic devices is important in certain national security cases is plausible and often made, though, understandably, not well documented. Wiretapping and eavesdropping are of little assistance in solving the relatively spontaneous crimes, often committed by teenagers, which are responsible for the increase in the crime rate.

The private uses for wiretap and eavesdrop devices are varied, and mostly unpleasant. Certain firms have inserted bugs in bathrooms to check on employee loyalty. Others have stolen business secrets with electronic assistance. Private persons have hired investigators skilled in the art of surveillance to gather evidence of adultery for divorce proceedings.

In a superficial sense the harmful aspects of wiretapping and eavesdropping are obvious. Private expressions are revealed to unknown auditors. Since an electronic device cannot distinguish between guilty and innocent persons or between relevant and irrelevant conversations, the invasion of privacy is necessarily broad. So, it has been argued, is the invasion in the ordinary search, which uncovers considerable material unrelated to criminal activity. But electronic surveillance usually takes place over an extended period of time and is much more likely to sweep in things of value—the expressions—of completely innocent persons. The tap of a doctor suspected of abortion encompasses, of necessity, all the confidential words of ordinary patients.

It is said that the invasion of privacy by electronic devices is more severe than that of an ordinary search, because the person is unaware it is happening. This point, it seems to me, cuts two ways. If someone does not suspect a tap or a bug and never finds out about it, he *experiences* no invasion at all.

However, to the extent that one does fear eavesdropping, his sense of privacy will be invaded and his freedom of expression constricted whether or not anyone does actually overhear what he says. For me, at least, the simple knowledge that lines are occasionally crossed and operators are sometimes nosey makes a slight difference in my telephone vocabulary. That is not very serious, both because the incidence of such overhearing is small and because I assume if it does occur, the unknown listener is not interested in me. But if no one, or even no one with a responsible position in society, had confidence in the sanctity of his most private conversations, the sacrifice in terms of human privacy would be telling. It is difficult, perhaps impossible, to ascertain the effect of the existing level of electronic surveliance on the willingness of most persons to speak their mind, or upon their more generalized sense of privacy. No doubt important figures in government, business, and labor, as well as criminals, are consciously con-

This article is an edited version of the author's comments at a Postgraduate Conference at Columbia Law School, March 18, 1967.

strained because of the possibilities of overhearing, but most of us probably are not. More generally, the growing number of social mechanisms for overseeing individual lives, commercial use of the lie detector and psychological testing, the imminence of centralized data banks, as well as visual and audial surveillance techniques, pose a threat to, if they have not already impaired, our broad sense of freedom. The level of eavesdropping almost certainly has some effect, perhaps minimal, on the quality of life of even those who are not invaded and do not expect to be invaded.

Recent concern with electronic surveillance is the product of our growing concern for privacy, some unsettling revelations about the extent of wiretapping and eavesdropping, and frightening advances in the art. Electronic surveillance is not a new phenomenon. Soon after the invention of the telegraph, wiretappers were intercepting messages and as early as 1862 California passed legislation prohibiting interception. Effective techniques for tapping telephones have been with us since the 1890's. What is striking about our time is the miniaturization and sophistication of snooping devices. Defense is becoming increasingly difficult, if not impossible. Wiretappers can now use, in addition to direct connection and ordinary induction coil taps, devices that fit within a telephone handset and allow a person in a waiting room or lobby to record calls going on inside an office. The technological advance in bugging devices is even more significant. A detectaphone placed on a party wall or a spiked mike inserted into it will pick up what is said in the adjoining room. Telescopic and parabolic microphones permit one to overhear conversations at distances of over 100 yards. An even more astonishing advance within the range of existing technology, but not now practical, is the use of ultrasonic waves or laser beams to pick up minute vibrations from window panes and thin walls, allowing the eavesdropper, without physical intrusion, to listen from a safe distance to what is said in a closed room. The miniaturization of microphones and transmitters has made the task of discovering an ordinary bug exceptionally arduous. Microphones the size of a sugar cube can be secreted in furniture and attached to the electrical system. If the eavesdropper prefers to avoid wiring, he can employ transmitters of the same size. One of the more imaginative varieties is in the form of an olive and can be dropped into a martini. Miniature microphones and transmitters can even be built into a person's clothing, if the eavesdropper is fortunate enough to have access to it. In one unit, a microphone, subminiature transmitter, and battery source are placed in each of three buttons; conductive wire that matches the thread of seams and decoration serves as the antenna.

The capacity for secretive visual surveillance, outside the scope of this discussion, has grown apace. Summarizing the development of modern techniques for physical surveillance, Professor Alan Westin has written:

> Technical and physical difficulties in the application of the new devices are more in the nature of obstacles to be overcome by ingenuity than fundamental blocks to surveillance. Nor have available counter-measures yet been developed as effective protections for the average citizen . . . the capacity to provide reasonable safeguards for individual and group privacy, a central assumption of man's social interaction since the dawn of civilization, has been overtaken by modern surveillance devices.[1]

As significant as the qualitative advancement in sophistication of eavesdropping gadgets is their economical production and mass distribution. The microphone the size of a piece of sugar can be bought for $10. Wide-

1. Westin, "Science, Privacy, and Freedom: Issues and Proposals for the 1970's" (Part I), 66 *Colum. L. Rev.* 1003, 1009 (1966).

*KENT GREENAWALT is assistant professor of law at Columbia University Law School and was formerly law clerk to Mr. Justice Harlan. He has served on the staff of the Law Enforcement Task Force of Mayor John Lindsay and is a member of the Civil Rights Committee of the New York City Bar Association and its subcommittee on wiretapping and eavesdropping.*

spread advertising in such magazines as Popular Mechanics and Popular Science informs the public of the general availability of these devices, and they are openly sold to private individuals and firms as well as to law enforcement officers. Perhaps the most significant safeguard against surveillance is the time and difficulty involved in setting up and monitoring an eavesdropping system. For ordinary law enforcement purposes, normal investigative techniques are simply more efficient. Needless to say, the time and energy it takes to eavesdrop must also limit the amount of private snooping.

By almost any reckoning, existing legal rules concerning wiretapping and eavesdropping are in something of a mess, though some would argue that the mess is a viable one. The Supreme Court, 5–4, in 1928 sustained the constitutional validity of wiretapping by government agents in *Olmstead v. United States*.[2] It held that the fourth amendment—which protects "the right of the people to be secure in their persons, houses, papers and effects," was not violated: first, because words cannot be "seized," and second, because the tapping of wires at a place removed from the defendant's house is not a search within the amendment. In his classic dissent—much quoted by wiretap opponents—Justice Brandeis concluded:

> The makers of our Constitution undertook to secure conditions to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the rights to be let alone—the most comprehensive of rights and the right most valued by men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[3]

In 1942 in *Goldman* v. *United States*,[4] a case involving a detectaphone, the theory of *Olmstead* was extended to bugging. But in 1961, in *Silverman* v. *United States*,[5] the Court distinguished a spiked microphone from the *Goldman* detectaphone. The microphone had penetrated the party wall to a heating duct in the defendant's house. The Court declined to go beyond *Goldman* by, in its own words, "even a fraction of an inch," and decided that overhearing accomplished by "an unauthorized physical penetration" does violate the Fourth Amendment. In 1964 *Clinton* v. *Virginia*[6] presented the embarrassment of a record that did not indicate whether a smaller spiked microphone inserted only a small distance into a party wall had accomplished a physical penetration. The Court deftly disposed of the case without opinion, reversing the state court determination of admissibility.

The black letter law now is that the Constitution is not violated by wiretapping or eavesdropping in the absence of physical intrusion of a constitutionally-protected area. But these black letters, if we judge by the language of *Silverman* and the disposition of *Clinton*, are rather shaky. On March 13, 1967 the Court granted certiorari in a case presenting this issue, among others.[7] Under existing constitutional decisions, one party to a conversation may record it or transmit it to law enforcement officers even if the conversation takes place on the premises of the party against whom the evidence is used, but the durability of this rule—at least in the present broad form

2. 277 U.S. 438.

3. 277 U.S., at 478.

4. 316 U.S. 129 (1942).

5. 365 U.S. 505 (1961).

6. 377 U.S. 158 (1964).

7. *Katz v. United States*, 87 Sup. Ct. 1021 (1967).

—is also open to question. The Court has not yet decided whether a court order based on probable cause can validate what would otherwise be unconstitutional eavesdropping. *People* v. *Berger,* a New York case argued this term, raises that problem. Bugging, opponents of the practice claim, is by its nature a general exploratory search, it is a search for "mere evidence,"[8] and it takes place without notice to the owner of the searched premises. Under traditional search and seizure rules any one of these factors *might* be enough to damn the practice, once it is granted that the fourth amendment is at all relevant.

To some extent, federal and state statutes have filled in the gap left open by *Olmstead.* Section 605 of the Federal Communication Act provides that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents . . . or meaning of such intercepted communication. . . ." Doubts as to whether the language of this 1934 statute was intended to apply to telephones at all, to intrastate as well as interstate calls, and to the activities of law enforcement officers, have all been resolved by an expansive reading of the statutory prohibition. Since divulgence of a wiretap is prohibited, wiretap evidence is inadmissible in federal courts. The Court has also excluded the fruits of such evidence.

The opinion in *Benanti* v. *United States*[9] in 1957 indicated with crystal clarity that the federal legislation preempts state laws legalizing wiretapping. Nonetheless, despite the fact that the policeman who introduces wiretap evidence in state proceedings commits a federal crime, the Court in 1952 held that the statute did not require suppression of such evidence[10] and has denied certiorari in more recent cases raising the same issue.[11]

A 1941 memorandum sent by Attorney General Jackson to the House Judiciary Committee outlined an interpretation of § 605 on which federal law enforcement agencies have since relied. The only offense, this theory goes, is interception *and* divulgence; thus tapping itself is permissible, and since interdepartmental communication is not divulgence, that is all right too. That this ingenious reading has not been repudiated by the Court is probably the result of lack of opportunity, rather than approval. What relevant language is to be found in the Court's opinions certainly points to a different interpretation.

Wide variation exists among states, but there has been a trend since 1955 toward tightening up wiretapping and eavesdropping laws. Some forbid all wiretapping. Others permit wiretapping only by law enforcement officers under ex parte court orders. One state, Illinois, prohibits both police and private eavesdropping by any device. Four other states make electronic eavesdropping subject to the same court order requirements as wiretapping, and forbid private eavesdropping.

Under the Supreme Court's interpretation of § 605, if a party consents, law enforcement officers can listen to a telephone conversation, at least so long as they listen on a regularly-used telephone extension.[12] The state statutes that prohibit eavesdropping, with two exceptions, allow a party to a conversation to record it or consent to eavesdropping by someone else.

Assessing the effect of any criminal legisla-

8. The Court is now reconsidering the "mere evidence" rule in Warden v. Hayden, cert, granted. 87 Sup. Ct. 290, argued April 12, 1967.

9. 355 U.S. 96 (1957).

10. Schwartz v. Texas, 344 U.S. 199.

11. People v. Dinan, 11 N.Y.2d 350, 229 N.Y.S.2d 406, cert. denied, 371 U.S. 877 (1962).

12. Ratbun v. United States, 355 U.S. 107 (1957).

tion is difficult since we cannot be sure what would have happened in its absence. The problem is magnified with regard to wiretapping and bugging, because there is so little hard knowledge about their extent. We do know, however, that § 605 has not stopped wiretapping. The Justice Department's interpretation of the law has allowed limited federal wiretapping. According to the best evidence we have, tapping of public and private phones occurs in states with permissive laws, restrictive laws, and no laws. It is done by law enforcement agents for law enforcement purposes when it is authorized, and (here the estimates of incidence vary widely) when it is not authorized. It is occasionally done by law enforcement agents for their own purposes, such as shakedowns. It is done by private individuals.

Relatively few private persons have been successfully prosecuted for illegal wiretap activities. Prosecutions of law enforcement officers are even rarer. The Department of Justice, in part because the F.B.I. has been tapping and in part because of permissive state laws, has not attacked state officers who tap and testify about the evidence obtained. State officials have been understandably hesitant to prosecute police who disobey local laws forbidding tapping or requiring court orders. They are also deterred from bringing private prosecutions by the questionable legality of their own activities, a desire not to create a public outcry against all tapping, and perhaps by the wishes of the telephone company. The police may depend on the assistance of company officials to tap, and the company does not want the public to lose faith in the privacy of the telephone. Since there is no federal law concerning electronic eavesdropping and few states yet have applicable statutes, it proceeds for the most part undeterred except by the laws of criminal trespass and breaking and entering and, insofar as the police are concerned, the exclusionary rule of constitutional law.

If our present legal situation with regard to electronic surveillance is not intolerable, it is at least highly illogical. Some defense of it can be made. Federal officers can tap when they deem it essential, though the evidence is inadmissible. The states, despite appearances, are left wide flexibility to deal with the problem as they choose.

At the very least, however, some adjustments in existing law are called for, and I believe more fundamental changes are needed. Plainly we need more effective prohibition of private wiretapping and eavesdropping. The notion that divulgence is a part of the crime under § 605 excludes private parties who have no need to divulge what they intercept. Since virtually no one argues that the social benefits of private wiretapping outweigh its harmful effects, all private wiretapping without the consent of one party should be prohibited by federal statute, and private damage actions, as well as criminal sanctions, should be provided for.

Another obvious change is that eavesdropping law must be brought into parity with wiretapping law. Electronic bugging poses a greater long-run threat to privacy than wiretapping. Tapping creates insecurity only about the use of one's phone, and the very nature of our telephone system precludes absolute certainty of privacy. Bugging, on the other hand, may reach any conversation, at one's office, at one's home, in one's bed, even on a boat in the middle of a lake. To the extent of its power,[13] the federal government should conform its eavesdropping law to its wiretap law, and

13. I believe that the Administration's view of the limits of federal power is too conservative in light of Katzenbach v. Morgan, 384 U.S. 641 (1966). See letter of Acting Attorney General Clark to Sen. Earl Long, reprinted Cong. Rec. 70th Cong. V. 113, No. 19, Feb. 8, 1967.

if there are gaps left, these should be filled in by the states.

Insofar as constitutional principles are concerned, the distinction between overhearing with a physical intrusion and overhearing without such intrusion is not now tenable, if it ever has been. As Mr. Justice Douglas said, concurring in *Silverman,* comparing the spiked mike in that case with the detectophone in *Goldman:*

> Was not the wrong in both cases done when the intimacies of the home were tapped, recorded, or revealed? The depth of the penetration of the electronic device—even the degree of its remoteness from the inside of the house—is not the measure of the injury.[14]

We now come to the more difficult questions. Should law enforcement tapping and bugging be permitted? If so, in what sorts of circumstances and by what sorts of officials.

Although eavesdropping may be effective in gathering evidence in some cases, the possibilities of abuses and the social damage that would occur even without abuse are too significant to allow tapping and bugging whenever law enforcement officers think it would be helpful. Many officials are willing to forego authority to tap in all cases, if their right to tap in certain circumstances is assured.[15] Unfortunately there is disagreement among those who favor limited wiretapping as to just what sorts of crimes should give rise to tapping.

Legislation proposed in 1962 would have allowed tapping by federal officers for crimes affecting national security, the transmission of gambling information, and travel or transportation in aid of racketeering enterprises, and by both federal and state authorities in cases of murder, kidnapping, extortion, bribery, narcotics offenses, and conspiracies to commit all these offenses. Let us look at each of these categories. If we assume that electronic surveillance is really an essential tool for combatting foreign subversion and intelligence activities—and that cause has not been publicly proved—we should be ready to sanction the necessary invasion of privacy; and if we don't sanction it we should expect that it will take place anyway. It is not at all obvious, however, that national security requires criminal convictions based on the evidence obtained or leads from the evidence. Though it seems illogical to permit a tap but not the introduction of its evidence, this may be a necessary compromise between the need to tap and the possibilities of abuse. Little showing has been made to indicate that wiretapping and eavesdropping are particularly effective techniques for solving murders, and even less that murders would be deterred by whatever minimal law enforcement gains are achieved. The costs are too great to justify tapping in murder cases. I have already suggested that the kidnapping and extortion cases may be handled by allowing overhearing with the consent of one of the parties. Taps and bugs may well be effective tools in bribery cases, but they would often be directed at public officials. The inhibition on open discussion by public servants and the particularly pernicious possibility of abuse of these techniques for political reasons suggest that the price is too great here.

Insofar as gambling, narcotic offenses, and racketeering offenses are concerned, we need ask three questions. Are electronic devices effective? Are these crimes serious enough to justify their use? If not, are these offenses so connected to organized crime that authority to tap is needed to bring our country's criminal warlords to justice? Some opponents of

14. 365 U.S. 505, at 513.

15. Some proponents of limited wiretapping and bugging suggest very strict procedural safeguards in lieu of, or in addition to, limits on the classes of offenses for which electronic devices can be used. Although space precludes discussion of these possibilities here, they deserve the most serious consideration.

tapping have argued that only lazy law enforcement officials need to tap, that it accomplishes little that cannot be done by ordinary means. It is true that the use of informers and police in disguise is instrumental in enforcement of the narcotics and gambling laws, but particularly in regard to the higher-ups, I find rather persuasive the contention that eavesdropping is often more effective and sometimes indispensable. But the cost is considerable. General authorization would allow the police to tap the phones of a great number of low level suspected criminals and their clients to solve crimes which do not elicit a high degree of moral condemnation, crimes, it might be added, which involve a particular danger of police shakedowns. For me, the assertion that wiretapping is necessary for effective enforcement of the gambling laws is a more persuasive argument for legalizing gambling than for permitting wiretapping.

Can the price be justified as one we must pay if our society is not to be undermined by organized crime? Perhaps widespread tapping of underlings really is necessary to catch the big fish, but we should, in my view, exhaust every other avenue before we accept that judgment. We should also examine what the effect on organized crime would be if we altered the substantive criminal law to eliminate some of the offenses, such as gambling, that provide much of its revenue. Another suggestion made is that we allow wiretapping and bugging only against the higher-ups in organized crime. This would permit intensive "intelligence" efforts leading to proof of criminality of those already known to be heavily involved in criminal activities. Perhaps this is more acceptable, but the problem of definition is a difficult one, and there is something unsavory about laws directed at types of persons rather than offenses.

A few general observations seem relevant to me to the decisions whether to allow any electronic surveillance and, if so, in which cases. The more officers who make legitimate use of electronic devices, the wider will be their availability for unsanctioned use, and the more complex the job of keeping them out of private hands. The more circumstances in which use is allowed, the more difficult it becomes to draw a meaningful moral line between permitted and prohibited use, and the harder it is to expect officers to eschew unauthorized uses.

On the basis of what we now know, I believe wiretapping and electronic eavesdropping without the consent of any party to the conversation[16] should be outlawed in all cases not involving national security.[17] In these circumstances use should be limited to federal officers. Though such a rule would involve some sacrifice of law enforcement capacity, it should lead to better enforcement against private and unauthorized public surveillance, it should minimize abuse of the terrifying potential of eavesdropping devices, and thus make a significant contribution to privacy.

---

16. Except for the summary description of existing law, I have not considered the problem of overhearing with the consent of one party, or recording or transmittal by one party without the consent of the other. My own view is that these should be prohibited when no law enforcement interest is involved, and that even in the law enforcement context, such use of electronic devices should be circumscribed by a requirement of probable cause and a court order system.

17. This is the position taken by the President and in the Administration bill, S. 928, introduced by Senator Edward Long on February 8. Though I am in disagreement with some parts of the bill, most particularly its treatment of consent, its central provisions seem to me sound.