Indiana Law Journal

Volume 43 | Issue 1 Article 7

Fall 1967

A Proposal for Legislative Control of Electronic Surveillance

Hugh C. Kirtland Jr.
Indiana University School of Law

A PROPOSAL FOR LEGISLATIVE CONTROL OF ELECTRONIC SURVEILLANCE

The Right Of Privacy of 1967,[1] now pending before the Cong-

---

1. Right of Privacy Act of 1967, S. 928 (H.R. 5386) 90th Cong., 1st Sess. §3 (1967).

SEC. 3. Title 18, United States Code is amended by inserting immediately following section 2424 a new chapter, to be composed of sections 2510 through 2515. . . .

SEC. 2510. Wire Interception.

(a) Any person who, whether acting under color of law or otherwise,

(1) willfully intercepts or attempts to intercept any wire communication without the consent of at least one sender or receiver of such communication; or

(2) willfully discloses or attempts to disclose, or uses or attempts to use, any information, knowing or having reason to know that such information was obtained in violation of paragraph (1) of this subsection—

Shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(b) It shall not be unlawful under this section (1) for an operator of a switchboard, or an officer, employee or agent of any communications common carrier whose facilities are used in the transmission of wire communications, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident of the rendition of service; or (2) for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of the Federal Communications Act, to intercept a wire communication while it is being transmitted by radio, or to disclose or use the information thereby obtained.

SEC. 2511. Eavesdropping.

(a) Any person who, whether acting under color of law or otherwise, willfully uses or attempts to use any electronic, mechanical or other device for the purpose of eavesdropping without the consent of at least one party to the conversation when

(1) Such device is affixed to any wire, cable, or other connection used in wire communications; or

(2) Such device transmits communications by radio; or

(3) Such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(4) Such use or attempted use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(5) Such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States; or

(b) Any person who, whether acting under color of law or otherwise, willfully discloses or attempts to disclose, or uses or attempts to use, any information, knowing or having reason to know that such information was obtained in violation of subsection (a) of this section—

Shall be fined not more than $10,000 or imprisoned not more than five years, or both.

SEC. 2512. Manufacture and Distribution of Wire Interception and Eaves-

ress, is intended to halt almost all electronic surveillance.[2] The bill al-

---

dropping Devices.

Any person who

(a) Except as a common carrier in the usual course of its business, sends through the mail or sends or carries in interstate or foreign commerce any electronic, mechanical or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of wire interception or eavesdropping; or

(b) Manufactures or assembles any electronic, mechanical, or other device, the design of which renders it primarily useful for the purpose of wire interception or eavesdropping, knowing or having reason to know that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) Places in any newspaper, magazine, handbill or other publication any advertisement of

(1) Any electronic, mechanical or other device, the design of which renders it primarily useful for the purpose of wire interception or eavesdropping; or

(2) Any other electronic, mechanical or other device, where such advertisement promotes the use of such device for the purpose of wire interception or eavesdropping,

knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce—

Shall be fined not more than $25,000 or imprisoned not more than one year, or both.

SEC. 2513. Confiscation of Wire Interception and Eavesdropping Devices.

Any electronic, mechanical or other device used, sent, carried, manufactured or assembled in violation of section 2510, 2511 or 2512 shall be seized and forfeited to the United States. . . .

SEC. 2514. National Security.

Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1103; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power or any other serious threat to the security of the United States, or to protect national security information against foreign intelligence activities. No information obtained directly or indirectly, in the exercise of such power, by wire interception or eavesdropping otherwise prohibited by this chapter shall be received in evidence in any judicial or administrative proceeding. Neither shall such information be otherwise used or divulged except as necessary to implement such power.

SEC. 2515. Definitions.

In this chapter—

(a) The term 'wire communication' means any communciation made in whole or part by aid of wire, cable, or other connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

(b) The term 'intercept' means the act of acquiring all or any part of any wire communication from the facility transmitting the communication through the use of any electronic, mechanical or other device.

(c) The term 'eavesdropping' means surreptitiously listening to, monitoring, transmitting, amplifying or recording a private conversation.

(d) The term 'electronic, mechanical or other device' does not include

(1) an extension telephone instrument furnished to the subscriber or user by a communications common carrier in the ordinary course of its business; or

(2) a hearing aid or similar device used by a person with impaired hearing, for the purpose of overcoming the impairment and permitting the hearing of sounds ordinarily audible to the human ear.

2. Electronic surveillance may take one of two forms: wiretapping or eavesdropping. Wiretapping is the surreptitious interception of telephone or telegraph com-

though it represents a great improvement over the existing patchwork of law, has serious deficiencies. This note will discuss the strengths and weaknesses of this legislation.

The bill makes it illegal to intercept or disclose any wire communication without the consent of at least one party. Eavesdropping, which is defined as "surreptitiously listening to, monitoring, transmitting, amplifying or recording a private conversation," or disclosing information so obtained is also made illegal. The penalty for eavesdropping or wiretapping is a 10,000 dollar fine, or imprisonment for five years, or both. Manufacturing, mailing, or shipping in interstate or foreign commerce, or advertising a device which is "primarily useful" for wiretapping or eavesdropping is subject to a fine of 25,000 dollars, one year of imprisonment, or both. Possession is, in effect, prohibited by a seizure and forfeiture section. This bill contains no provision for electronic surveillance by law enforcement agencies although it does not limit the powers of the President with respect to national security matters. But even in this area, evidence obtained by surveillance techniques may not be introduced in any judicial or administrative proceeding.

One of the strongest features[3] of this proposed legislation is that it represents the first national, comprehensive effort toward attacking the problem of surveillance. There is, of course, much law on the subject but at present it is limited in scope and efficacy. There is a federal statute[4] which perhaps was intended to prevent wiretapping but it has been so construed by the courts and the Department of Justice that it is practically useless; the only meaningful federal restriction on surveillance is that its products usually may not be introduced as evidence.[5] Several

---

munications by gaining access to the electrical signal at some point along the wire through which it travels. Eavesdropping is the surreptitious overhearing of conversations by intercepting the sound waves thus generated.

3. Although only three features of S. 928 will be discussed, the rest of the bill is also well designed. Prohibiting the actual surveillance is obviously crucial, as is prohibiting the possession of certain devices, which is the effect of the forefeiture provision. The exclusionary evidence section removes much of the incentive to eavesdrop or wiretap. The prohibition against advertising is especially good. The billions of dollars spent annually for advertising attest to its important role in product distribution. This prohibition should significantly disrupt the distribution system of surveillance equipment.

4. Federal Communications Act of 1934 § 605, 47 U.S.C.§ 605 (1964). "[A]nd no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. . . ."

5. Although there are numerous decisions concerning what acts of surveillance are illegal under the fourth amendment or section 605 [Some decisions rely on both the fourth amendment and section 605. *See, e.g.*, Goldman v. United States, 316 U.S. 129 (1942)], most of them consider the illegality only for purposes of determining the admissibility of evidence so gathered rather than for purposes of imposing criminal sanctions under section 605. Since 1953 when the Department of Justice assumed sole responsibility for enforcing section 605, there has been a disposition of only thirty

states have enacted statutes which prohibit various facets of surveillance[6]

---

cases involving violations. There have been nineteen convictions, eight acquittals, and three dismissals. Three cases are presently awaiting trial. Letter from Fred M. Vinson, Jr., Assistant Attorney General, Criminal Division, Department of Justice (by Harold P. Shapiro) to *Indiana Law Journal*, March 23, 1967.

The Department of Justice has construed section 605, since it states "intercept *and* divulge," (emphasis added) as no bar to wiretapping so long as the conversation is not divulged outside the Department. Kamisar, *The Big Ear, the Private Eye, and the Lawman*, 36 WIS. B. BULL. 33 (June 1963). According to the courts, section 605 protects the communications system not the conversation. Goldman v. United States, *supra*. Thus, placing a microphone on the opposite side of the wall of a room in which the defendant conducted a telephone conversation so that the defendant's part of the conversation was overheard was not a violation because the telephone system was not touched. Nor is there a violation of section 605 by broadcasting a conversation by a transmitter because there are no wires, On Lee v. United States, 343 U.S. 747 (1952), or by listening to a conversation on an extension telephone, at least with the consent of one party, beccause there is no "interception." Rathbun v. United States, 355 U.S. 107 (1957). Under the fourth amendment, it has been held that there is no violation by a wiretap performed without a physical trespass, Olmstead v. United States, 277 U.S. 438 (1928), by eavesdropping with a microphone, again without a physical trespass, Goldman v. United States, *supra*, by transmitting a conversation by a radio, On Lee v. United States, *supra*, or by recording a conversation on a concealed wire recorder. Lopez v. United States, 373 U.S. 427 (1963). However, in Silverman v. United States, 365 U.S. 505 (1961), a spike microphone had been driven into a party wall so that it made contact with the heating ducts in the defendant's apartment. The Court stated that it was not concerned with the law of party walls—the police had usurped an integral part of the defendant's house without his knowledge or consent. This was an actual intrusion into a "constitutionally protected area." The most recent case concerning what conduct constitutes a violation of the fourth amendment is Berger v. State of New York, 388 U.S. 41 (1967). *Berger* held that New York's statute, note 6 *infra*, permitting judicial *ex parte* orders for eavesdropping did not meet the fourth amendment requirements for a showing of probable cause and particular description of the things (conversations in this case) to be seized. It cannot be said, however, that *Berger* puts an end to all permissible uses of surveillance equipment. In Osborn v. United States, 385 U.S. 542 (1966), a federal district judge authorized a person, who was a secret agent for the federal government, to carry a concealed tape recorder into a conversation during which a bribery attempt was anticipated. The Court did not believe that this conduct represented a violation of fourth amendment rights. In *Berger, Osborn* was cited to show that not necessarily all eavesdropping was prevented. Berger v. State of New York, *supra* at 63.

Once it has been determined that evidence was obtained illegally, the question turns to whether or not the evidence is admissible. In Nardone v. United States, 302 U.S. 379 (1937), it was held that federal agents could not testify in federal court as to the substance of certain of defendant's telephone conversations which the agents had overhead by means of an illegal wiretap. In the second *Nardone* case, Nardone v. United States, 308 U.S. 338 (1939) (*semble*), the Court reversed a holding by the Court of Appeals for the Second Circuit that, although the introduction into evidence of the exact words of a conversation overheard in violation of section 605 is prohibited, all other uses of what is learned through the wiretap are permissible. Benanti v. United States, 355 U.S. 96 (1957), held that state agents may not testify in federal court on wiretap evidence secured in violation of section 605. Similarly, evidence obtained in violation of the federal constitution may not be introduced in a state court. Mapp v. Ohio, 367 U.S. 643 (1961) ; Berger v. State of New York, *supra*.

The admissibility in a state court of evidence obtained in violation of section 605 is not, however, entirely clear. Although it would seem that *Mapp* could easily be interpreted as forbidding the introduction of such evidence, the Court of Appeals for the Second Circuit chose not to do so in Williams v. Ball, 294 F.2d 94 (2d Cir. 1961), *cert. denied*, 368 U.S. 990 (1962). The court noted that Schwartz v. Texas, 344 U.S. 199 (1952), had held that evidence obtained in violation of section 605 *is* admissible in a state court. The reasoning continued that, since Congress has not expressly suspended

but because most of them only make it illegal "to eavesdrop" or "to wiretap," the difficulty of enforcement has overcome whatever value the statutes might have.

The proposed bill similarly makes the act of surveillance a crime and there is no reason to believe that enforcement of this part of the bill would be any easier simply because the legislation were federal. However,

---

state power with respect to this rule of evidence, the illegality of the gathering of the evidence is but one factor for the state to consider in formulating its evidence law. Thus the Second Circuit does not read *Mapp* as overruling *Schwartz*. *Mapp* is distinguished on the basis that the Court there stated that the exclusionary evidence rule was necessary to enforce the fourth amendment and that it is section 605, not the fourth amendment, that is being violated in *Williams*.

6. Only a few states have addressed the total problem of electronic surveillance and have devised comprehensive legislation; nearly all states have enacted statutes which relate to the subject in some degree. These statutes are generally of three types. The first type of statute makes it a crime, usually a misdemeanor, to injure, harm, tamper with, etc. a telephone or telegraph wire. In almost all cases these statutes are quite old and were intended to prevent malicious mischief to property. It is only by accident that they may also apply to wiretapping. *E.g.*, MICH. COMP. LAWS §§ 484,157, .6 (1948), MICH. STAT. ANN. §§ 22.1367, .1415 (1935). Another type of statute makes it a crime to wiretap. These statutes usually have been enacted within the last fifteen years but they address themselves only to wiretapping. *E.g.*, PA. STAT. ANN. tit. 15, § 2443 (1958). The third type deals with both eavesdropping and wiretapping. Illinois and New York both have statutes of this type and the two statutes are noteworthy because of the different philosophies they reflect. The Illinois statute makes it a crime to eavesdrop or wiretap upon any conversation unless at least one party consents. The prohibition applies equally to law enforcement officials. Any victim of eavesdropping or wiretapping is given the civil remedies of an injunction or damages, both actual and punitive. ILL. ANN. STAT. ch. 38, §§ 14-1, -2, -6 (Smith-Hurd 1964). Any evidence obtained illegally is excluded from criminal and civil trials, administrative or legislative proceedings, or grand jury hearings. ILL. ANN. STAT. ch. 38 § 14-3 (Smith-Hurd 1966). It has been held that, although the crime of eavesdropping or wiretapping is not committed so long as one party consents to the surveillance, evidence so obtained may not be admitted against any party to the conversation who did not consent. The court emphasized that the statute is intended to protect privacy. People v. Kurth, 34 Ill. 2d 387, 216 N.E.2d 154 (1966). The New York statute similarly prohibits eavesdropping and wiretapping and also makes it a crime to possess surveillance equipment in a situation that shows an intent to use it unlawfully. N.Y. PEN. §§ 738, 741, 742 (McKinney 1967). No civil remedies are provided, however. The significant difference is that law enforcement officers may eavesdrop or wiretap pursuant to an *ex parte* court order which is issued upon a showing that there is reasonable ground to believe that evidence of a crime may be obtained. N.Y. CODE CRIM. PROC. § 813-a (McKinney 1967 Supp.). This provision, however, was litigated in Berger v. State of New York, 388 U.S. 41 (1967), and it is doubtful that it will be of further use, at least in its present form. Prior to *Berger*, section 813-a had been construed to mean that eivdence so obtained could be introduced in the state courts even though there had been a violation of section 605 of the Federal Communications Act of 1934. United States *ex rel.* Graziano v. McMann, 275 F.2d 284 (2d Cir.), *cert. denied*, 365 U.S. 854 (1960); People v. Dinan, 11 N.Y.2d 350, 183 N.E.2d 689, 229 N.Y.S.2d 406, *cert. denied* 371 U.S. 877 (1962). It had also been held, however, that a wiretap order could not be executed by a physical trespass into a constitutionally protected area. People v. Grossman, 45 Misc. 2d 577, 257 N.Y.S.2d 266 (Sup. Ct. Kings Co. 1965). The same procedure also authorizes eavesdropping by a law enforcement officer. N.Y. CODE CRIM. PROC. § 813-a (McKinney 1967 Supp.). However, eavesdropping, unlike wiretapping, is permitted for twenty four hours without an *ex parte* order if the delay to obtain the order would result in a loss of the evidence. N.Y. CODE CRIM. PROC. § 813-b (McKinney 1967 Supp.).

S. 928 goes much farther in that it attempts to control surveillance by controlling the source of surveillance equipment.

The prohibition on manufacturing, distribution, and importation of certain devices is the second great strength of the bill. Because of the extreme difficulty of apprehending anyone "in the act" of using surveillance equipment, any approach to the problem of controlling electronic surveillance must make some attempt to restrict the availability of the equipment with which it is performed.

It is the nature of the equipment used that makes it extremely difficult to detect someone engaged in electronic surveillance. Although electronic surveillance devices are frequently used in combination, there are basically three types of devices. One group of devices is microphones—microphones disguised as jewelry, spike microphones, parabolic microphones, and devices which turn an ordinary telephone into a microphone.[7] Microphones will often be attached to transmitters, which comprise the second group. There is the infamous martini olive which acts as a microphone and transmitter[8] and other less novel transmitters small enough to be carried in a pocket, purse, or briefcase or sewn into the lining of a man's suit. The third group, tape recorders, is used when it is not practical to have a human operator monitoring the intercepted conversations.[9] In addition to this affirmative surveillance equipment, there have been developed a large number of defensive devices designed to detect the presence of surveillance equipment.[10]

---

7. Microphones have been built into cuff links, tie clasps, and wristwatches. The spike microphone, when driven into a wall of a room from the opposite side, turns the entire wall into a sounding board for every sound uttered in that room. The parabolic microphone is so sensitive that it can pick up a conversation over 500 feet distant. The telephone devices include a piece of equipment which need only be placed near a telephone. When that telephone number is dialed and a note sounded on a harmonica, the telephone does not ring but instead picks up every sound in the room. Some of the less spectacular devices are the three-wire tap, which is connected to a telephone line, and the induction coil which need only touch the line. Both of these devices are designed so that they do not weaken the electrical signal and betray their presence. *Hearings on Invasions of Privacy (Government Agencies) Before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary*, 89th Cong., 1st Sess. 14-32 (1965) [hereinafter cited as *Hearings*].

8. The olive will transmit approximately two blocks even when submerged in the martini. The toothpick is the antenna. *Hearings* 14-32.

9. Most tape recorders designed for these purposes are equipped with long-life batteries so that they may be left unattended for long periods of time. When it is convenient, the operator will return to the tape recorder, pick up the used tapes, and install fresh ones. *Hearings* 14-32.

10. The Mosler Research Products Corporation manufactures a "Soun-D-Tect" kit, which contains both affirmative and detective equipment. There are few wiretapping or eavesdropping operations that could not be performed with the equipment in this kit, which consists of seventeen items: a hearing aid phone kit, a crystal microphone, a spike microphone, a shielded cable, high and low impedence test leads, a radio frequency test probe, a metal detector, an induction coil, a special microphone and cable pair, a tone

The essence of electronic surveillance is that it must be conducted in secret. The need has been so effectively met by the suppliers of the equipment that even the victim is seldom aware that he has been a victim unless he notices that other people possess information that they could not otherwise have obtained. In fact, an expert, armed with defensive equipment, can do no more than render an opinion that a particular room is not subject to surveillance.[11]

Although it may seem paradoxical, the prohibitions against manufacturing, a great strength of the bill, are also a great weakness. The effort to restrict manufacturing, while a step in the right direction, does not go far enough; as it is drafted, the bill will affect only a few devices. The reason is that the bill does not reflect an adequate analysis of the nature of electronic surveillance equipment.[12]

The versatility of electronic equipment greatly limits the number of devices whose manufacturing can be prohibited. Electronic components, *i.e.*, capacitors, vacuum tubes, transformers, etc., have thousands of uses. Only when an electronic assembly becomes highly complex does it begin to take on characteristics peculiar to surveillance use. It is clear that only a minute fraction of all known electronic equipment is undesirable by reason of its suitability for surveillance uses. Therefore, a statute that prohibited the manufacturing of more than electronic devices that were suited to surveillance use and little else would severely damage twentieth century technology. Of necessity, then, it is only manufacturing, in the sense of putting a device in a condition so that it is immediately capable of being used for surveillance, that can safely be prohibited. Consequently, the manufacturing of very few pieces of equipment can be made illegal and the important manufacturing section of S. 928 would have a very limited effect.[13]

The piece of equipment that is actually used for surveillance is seldom any one piece of equipment at all but rather combinations of

---

generator adaptor, a recorder adaptor, and a carrying case. Sales Brochure of Mosler Products, Inc. 10, reprinted in *Hearings* 55.

11. *Hearings* 39-44.

12. The draftsmen were, however, aware that only a few devices would be restricted. *Hearings on S.* 928 *Before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary,* 90th Cong., 1st Sess. 57 (1967).

13. It is the writer's opinion that, of the items contained in the Mosler "Soun-D-Tect" kit, note 10 *supra,* only one—the spike microphone—whose cost is less than three per cent of the total cost of the kit, does not have enough legitimate uses that to outlaw entirely its manufacture would be unthinkable.

The same reasoning applies to the advertising restrictions. *See* note 3 *supra.* For example, the Mosler firm would be completely barred from advertising only the spike microphone. Although it could continue to advertise the other sixteen items in its kit, it could not advertise them in combinations which made their adaptability to surveillance uses so obvious.

electronic units; *i.e.*, a transmitter or microphone by itself is useless for eavesdropping; connect the two and eavesdropping can begin. It is manufacturing in the sense of connecting the transmitter to the microphone (with intent to eavesdrop) that must be prevented. But this act, like the act of surveillance itself, is one that the eavesdropper could perform in complete privacy without great risk of detection. The problem, then, is that manufacturing must be narrowly defined to avoid disastrous side effects and, because of the nature of the few activities prohibited by this narrow definition, illegal manufacturing will be detected with difficulty, if at all.

A more effective solution might be achieved by *regulating* as well as prohibiting the manufacturing and distribution of certain equipment. The suitability for surveillance use of a piece of electronic equipment is a matter of degree. A spike microphone is immediately ready to be used for eavesdropping and can be used for little else. A transmitter or microphone is also perfectly suited for eavesdropping but has numerous legitimate uses. A resistor not only must be assembled with other parts but has thousands of other uses. This suggests a basis for a legislative classification—prohibit the manufacturing of the class of items immediately useable for surveillance and suitable for little else, regulate the manufacturing and distribution of items immediately or quickly useable for surveillance but with numerous legitimate applications, and leave unrestricted the manufacturing of items not immediately or quickly useable for surveillance.[14]

A workable legislative scheme would prohibit all manufacturing, selling, advertising, or possessing of devices immediately useable for, and only for, surveillance, such as the spike microphone or martini olive transmitter; prohibit the manufacturing of devices immediately or quickly useable for surveillance, but which have other legitimate purposes, by any person who does not possess a license;[15] and prohibit buying in quantity of these devices by any person who does not possess a similar license.[16] All sellers of devices in the second classification would be

14. It is important to keep in mind that the ultimate goal of a legislative scheme to control electronic surveillance is to eliminate all undesirable *uses*. But a statute that merely prohibits use will be ineffective because of the difficult enforcement problem. Therefore, a viable statute must function as a realistic deterrent to the proscribed conduct by providing a means which maximizes the likelihood that a violation will be detected and prosecuted. The value of the statute must be measured by this standard.

15. All restrictions, whether total prohibitions or regulations, should apply equally to importation. Apparently foreign products suited to electronic surveillance are available in the United States. See *Hearings* 20.

16. It might be advantageous to require the buyer to possess a license for all sales but at some point in the distribution process it is likely that the number of potential buyers would be so large that this would be impractical. However, it should be possible to license all buyers except the ultimate consumer.

required to keep records of all transactions. The records should include the name and address of the buyer, the quantity, a description of the devices sold, and any serial numbers on the devices.[17] The ultimate purchaser, although he would not need a permit to buy, would be required to sign his name and address on a register and show identification. This requirement is like the present one which requires one to sign his name when purchasing certain drugs which, although they contain narcotics, do not require a prescription.[18] Periodically the retailers would send their sales records to an appropriate federal agency which, by means of data processing equipment, would examine all purchases for any suspicious buying patterns. This would uncover, for example, a person who had acquired twenty transmitters and microphones from different stores in a short period of time or someone who had similarly acquired the array of equipment presently sold as a kit by the Mosler Research Products Corporation.

There must also be some means of determing which equipment is to be prohibited, which is to be regulated, and which is to be unrestricted. It would seem that administrative determinations are ideally suited for this task. Electronic equipment is sufficiently versatile and the industry is progressing at such a rate that a statute which attempted to make the necessary detailed classification would be unduly cumbersome and quickly outdated.[19] Administrative regulations would provide the necessary flexibility.[20] These regulations could specify or describe in relatively detailed terms which devices may not be manufactured, sold, advertised, or possessed and which may be manufactured and distributed only by licensees who keep the appropriate records.[21]

The administrative agency could also serve two other functions. First, it would issue the licenses to manufacturers and sellers. This would be only a ministerial task since, with the exception of the prohibited devices, the goal is not to restrain production and distribution of electronic equipment but to aid law enforcement by keeping track of certain devices or combinations of devices. The agency could also be the instrument by which the President's orders with respect to national security surveillance are implemented. As was mentioned earlier, the bill represents a

17. It would aid enforcement to require a serial number to be placed on *all* devices in the regulated category. The small size of much of the equipment and the added cost, however, would seem to make this impractical.

18. *E.g., Wis.* STAT. ANN. §§ 161.09(3), (5) (1957).

19. Standards must be set by the statute in order to avoid an unconstitutional delegation of legislative authority. *See* Schechter Poultry Corp. v. United States, 295 U.S. 495 (1935).

20. It would seem that the Federal Communications Commission might be the proper agency for this function since it likely possesses the required expertise.

21. The description of an item in the latter category might be "a radio transmitter smaller than five inches by two inches by one inch."

policy decision that use of surveillance equipment is appropriate in situations in which the national security is threatened. But the term "national security" is very broad. It would not be unreasonable to give it a construction such that it could apply to the threat posed by organized crime, corrupt public officials, narcotics, professional gambling, and the like. It appears, however, that the draftsmen do not intend this broader meaning.[22] If this is the case, they can not be satisfied with this part of S. 928.[23]

Regardless of the final decision made by Congress concerning the meaning of "national security," it seems clear that some uses of surveillance equipment are to be allowed. If these operations require equipment that is on the prohibited list, the agency could authorize the manufacturing of a limited number of them by designated firms under carefully controlled conditions. To the extent that the necessary equipment is a combination of devices on the regulated list so that it is only the combining of the components, use, or possession that is a violation, this need could be accommodated by the agency's doing nothing; *i.e.*, forebearing to apprehend what would be law violations in the absence of the national security justification.

To summarize, if the legislation proposed here were adopted, wiretapping, eavesdropping, or the disclosing of information so obtained would be illegal except in cases of national security. Manufacturing, importation, sale, possession, or advertising of a device immeditaely or quickly useable for eavesdropping or wiretapping but with other legitimate purposes would be illegal except when licensing and record keeping requirements are followed. Records of sales to ultimate consumers would be evaluated by data processing equipment as an aid to law enforcement. The total scheme would thus touch all stages of electronic surveillance—from manufacturer to user. Certain types of devices would no longer be available. Other devices, although they could still be readily purchased, could not be obtained unless the buyer left a trail. Because any information obtained through surveillance would be inadmissible as evidence, much of the incentive to use surveillance techniques would be eliminated. Possession or use of surveillance equipment would clearly be criminal activity.

A violation of *any part* of the statute should be subject to criminal sanctions. That is, not only should it be a crime to use or possess electronic surveillance equipment but it should also be a crime to manufacture, import, advertise, sell without a permit, fail to keep records, or falsify

22. *Hearings on S. 928 Before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary*, 90th Cong., 1st Sess. 51 (1967).

23. For Mr. Justice White's discussion of the weakness of the term "national security," see People v. Berger, 388 U.S. 41, 113-17 (1967) (dissenting opinion).

records. This is necessary to protect the integrity of the system. It would also seem that the penalties for a violation should be heavy in order to maximize the deterrent effect of the criminal law.

It should be recognized, however, that this scheme, as comprehensive as it may be, contains weaknesses. The first is that many people, even if they could not obtain a transmitter or similar piece of equipment, could build one with basic electronic parts available in any electronic supply store. Obviously, there are fewer people who have the ability to assemble a transmitter or who would go to the trouble than there are people who are capable of connecting a microphone and pre-assembled transmitter. Yet there are probably hundreds of high school students who have this ability. Detection here would be as unlikely as the detection of the act of surveillance.

A second weakness is that even the record keeping will not be as effective in policing a surveillance statute as it is in other areas where this technique is used. For example, the records kept on gun sales can be used to link a gun with its owner. When a gun is found near the scene of a crime, its serial number will lead the police to its purchaser. The surveillance records, however, can do little more than alert law enforcement officers that a certain person may be preparing to violate the law.[24] Nevertheless, it would give the police a place to begin an investigation and would increase the opportunities for detecting a person in the act of illegal surveillance.

An important consideration in judging any legislation is the cost and burden of compliance. The cost to a manufacturer or seller of obtaining a license would be no more than the time involved to fill out an application, plus postage. Manufacturers and sellers, however, will also be required to keep records describing the particulars of many sales. The actual cost of this is not known but one suspects that in most cases it would not be great. First, it is generally only small, portable, assembled components that will be restricted. Because businesses already keep many detailed records for cost accounting and inventory control, income tax purposes, warranty claims, and quality control, it is likely that many firms already maintain records that would satisfy this legislation. It should be remembered that it is only the retailer who must compile information and send it to a federal agency; all others need only maintain the records so that they would be available for inspection. In the case of retailers, all they need do is keep a simple looseleaf notebook, in which buyers write their names and addresses, and periodically mail it to the enforcing

24. Serial numbers on electronic surveillance equipment could also be used to lead police to the purchaser. It is doubtful, however, that more than a few electronic devices will bear serial numbers. See text accompanying note 17 *supra*.

agency. Retailers of some types of goods are already required to do this; the requirement for narcotic-containing drugs has already been mentioned and most states have similar requirements for the sale of handguns[25] and poisons.[26] The principal cost, that of setting up and operating the data processing facilities, would be borne by the federal government. In view of the rapidly increasing use of this equipment by the federal government, even this should not be excessively costly.

For some time, the use of electronic surveillance equipment has been the subject of much talk and little action. There is now the very real possibility that Congress will enact comprehensive legislation. Unfortunately, the proposed legislation is not adequate to accomplish its apparent goal of eliminating all electronic surveillance except in national security matters. The major reason for the shortcoming in the bill is that its authors failed to demonstrate an appreciation for the nature of electronic technology. The proposal based on a functional classification of electronic devices seems much more likely to eliminate undersirable uses of electronic surveillance equipment.

Hugh C. Kirtland, Jr.

---

25. *E.g.,* IND. ANN. STAT. § 10-4742 (Burns Repl. 1956); N.J. REV. STAT. § 2A: 151-25 (1951).

26. *Cf.* IND. ANN. STAT. § 10-3527(3), (.4) (Burns Repl. 1956); *e.g.,* WIS. STAT. ANN. § 151.10(1)(c) (1957).