# *ELECTRONIC SURVEILLANCE IN CALIFORNIA: A STUDY IN STATE LEGISLATIVE CONTROL*

One of the more dubious achievements of the twentieth century scientific and technological revolution is the unprecedented capability it has given man to intrude into the private lives of his brethren. This capability and his increasing propensity to make use of it have left few aspects of individual privacy intact.[1] Computers store, correlate, and retrieve vast amounts of information about every facet of an individual's life;[2] modern psychological testing can probe the very depths of a man's mind;[3] and devices for aural and visual surveillance have dissolved the physical barriers which have previously enabled man to shut out the outside world.[4] As scientific advances have rendered traditional protective devices inadequate, it has become necessary to replace them with legal restraints to preserve the privacy so valued in our society. This Comment is concerned with the legal response to what is certainly the most publicized,[5] if not the most important, aspect of this assault on personal privacy—the monitoring of oral communications by means of electronic devices. In particular, it will critically

---

1. *See generally* A. WESTIN, PRIVACY AND FREEDOM (1967) [hereinafter cited as PRIVACY AND FREEDOM]. Professor Westin also discusses some of the factors which have accelerated the use of technological advances for information gathering purposes. *Id.* at 90-103, 158-63. *See also* M. BRENTON, THE PRIVACY INVADERS (1964).

2. *See, e.g.*, PRIVACY AND FREEDOM, *supra* note 1, at 158-68; Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in the Information-Oriented Society*, 67 MICH. L. REV. 1089 (1969).

3. *See, e.g.*, PRIVACY AND FREEDOM, *supra* note 1, at 135.

4. A few examples of the sophisticated devices available for physical surveillance include miniature closed-circuit television cameras small enough to be hidden in a light fixture; infrared photography equipment which can take pictures in the dark; microphones the size of sugar cubes; transmitters small enough to conceal in a shirt pocket; parabolic or "shotgun" microphones which can pick up conversations hundreds of feet away; bugs which can be concealed in a telephone receiver and activated by a phone call from anywhere in the world; and various types of induction devices which will pick up telephone conversations without making physical contact with the line. These are but a small fraction of the myriad of devices available, and continuing developments in such fields as laser technology promise even more startling innovations. *See, e.g.*, E. LONG, THE INTRUDERS 5-11, 64-78 (1967) [hereinafter cited as THE INTRUDERS]; PRIVACY AND FREEDOM, *supra* note 1, at 73-78; Westin, *Science, Privacy, and Freedom*, 66 COLUM. L. REV. 1003, 1004-10 (1966). For more technical information on the design and operation of surveillance devices see S. DASH, R. SCHWARTZ, & R. KNOWLTON, THE EAVESDROPPERS 305-81 (1959) [hereinafter cited as THE EAVESDROPPERS].

5. The writings on the subject are legion in both lay publications and legal literature. For a bibliography of some of the more important recent writings in the field see ABA PROJECT ON MINIMUM STANDARDS FOR CRIMINAL JUSTICE, STANDARDS RELATING TO ELECTRONIC SURVEILLANCE app. E at 237-50 (Tent. Draft 1968) [hereinafter cited as ABA STANDARDS].

examine California's solution to the electronic surveillance[6] problem.

In 1967, the California Legislature, recognizing the threat to privacy posed by the unrestricted use of electronic snooping devices, enacted a comprehensive scheme designed to protect the confidentiality of oral communications.[7] This legislation, though flawed, effected important changes in California surveillance law and gave California one of the most comprehensive of state regulatory schemes. The year 1967 also saw the first of a number of significant developments in federal and constitutional surveillance law;[8] developments which have had a significant impact on state regulation of electronic surveillance. This Comment will analyze the California Privacy Act in light of these developments and attempt to answer the questions: What is the law of California today? How can it be improved?

In addition to explicating the law of California, the discussion will illustrate the impact of the recent federal and constitutional developments on state regulation of surveillance and will suggest some practical guidelines for other states considering legislative reform of their surveillance laws. The spate of recent activity on the federal level portends an upswing in state legislative action in the surveillance field, if only to take advantage of the new federal provisions for authorization of surveillance by state law enforcement officials.[9] As more states contemplate reform, they naturally will look to existing legislation for guidance. Hopefully, this analysis of California's comprehensive

6. The term electronic surveillance is used herein to denote all forms of aural surveillance involving electronic equipment. It includes not only all acoustical monitoring accomplished by means of electronic devices, but also the overhearing of any communication transmitted via an electronic medium. Electronic surveillance comprises the practices commonly known as wiretapping and electronic eavesdropping or "bugging." Wiretapping refers to the interception by any method of telegraphic or telephonic communications; the term electronic eavesdropping encompasses all other forms of electronic surveillance.

Participant monitoring refers to electronic surveillance performed by or with the consent of one or more parties to a communication. The term consensual surveillance will be used interchangeably with participant monitoring. All surveillance accomplished without the consent or participation of any party to the communication is denominated third-party monitoring.

7. Ch. 1509, [1967] Cal. Stats. 3584, *enacting* CAL. PENAL CODE §§ 630-37.2 (West Supp. 1968) [hereinafter referred to as the California Privacy Act].

8. The first of these developments was the United States Supreme Court decision in Berger v. New York, 388 U.S. 41 (1967). That case was soon followed by Katz v. United States, 389 U.S. 347 (1967), and the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 [hereinafter referred to as the Crime Control Act]. These developments are discussed at length in Part I, section B *infra*.

9. Title III of the Crime Control Act permits electronic surveillance by state law enforcement officials under a court order issued pursuant to a state enabling statute drawn in conformity with the provisions of title III. 18 U.S.C. § 2516 (Supp. IV, 1965-68).

scheme, with its deficiencies and oversights, will provide some insights into the traps and pitfalls which await the draftsmen of surveillance legislation. While the focal point of the discussion will be the California Privacy Act, title III of the federal Crime Control Act[10] will also receive considerable attention because of its pervasive influence, by both precept and example, on state law.[11]

The five parts of this Comment are to a large extent self-contained and independent of one another. With the exception of Part I, each deals with a particular aspect of surveillance regulation: analyzing the problem, examining the California response, and making suggestions for change. Part I will provide some basic definitional and historical background for the discussion of current law. It will briefly review the growth of surveillance law up to 1967 and examine, in somewhat more detail, the major developments since that time. Part II is devoted to an examination of the general proscriptive provisions of the California Privacy Act. Part III considers the use of electronic surveillance for law enforcement purposes. California practice is summarized, but the discussion is devoted primarily to the development of workable restraints for controlling police surveillance when it is permitted. Part IV deals with a specialized type of electronic surveillance—that performed by or with the consent of one of the communicating parties. Although this type of monitoring traditionally has been exempted from the controls imposed on third-party surveillance, this section argues that police use of participant monitoring should be circumscribed by a warrant system such as that now required for nonconsensual surveillance. Part V surveys and evaluates the sanctions and remedies available to enforce the surveillance laws and to compensate the victims of unlawful surveillance.

## I

### SETTING THE STAGE

At the outset it will be helpful to identify briefly some of the competing interests involved in the surveillance problem.[12] Electronic surveillance impinges on a number of interests which are generally subsumed under the rubric "privacy."[13] Surveillance by private parties

10. Title III of the Act deals with wiretapping and electronic eavesdropping. Its operative provisions are codified in 18 U.S.C. §§ 2510-20 (Supp. IV, 1965-68).

11. See text at notes 107-09 *infra*.

12. What follows is a truncated treatment of an obviously complex subject. It is by no means intended as an in-depth analysis of all the interests involved in the surveillance question. Rather, the discussion merely attempts to point out some of the major considerations and to illustrate that the interests affected are not the same in all contexts even though they may be referred to by the catchall "privacy."

13. *Cf.* Beaney, *The Right to Privacy and American Law*, 31 LAW & CONTEMP.

invades the broadest of the privacy interests—the general right of the individual to be free from unsolicited intrusions into his personal affairs. This is the classical right to privacy—the "right to be let alone."[14] In addition, electronic surveillance threatens liberty of communication by destroying the aura of privacy necessary for the free interchange of ideas; the fear of being monitored will chill uninhibited communication.[15] Both of these reasons militate against the use of electronic surveillance.

On the other side of the question, the interests in permitting private parties to engage in surveillance activities are insubstantial. The purposes for which individuals employ electronic surveillance—*e.g.*, to satisfy curiosity, to purloin industrial secrets, to gather evidence in domestic relations cases[16]—generally are of insufficient social utility to justify its use. Even where the goal may be more laudable—as in scientific research—it normally can be accomplished by obtaining the consent of the parties involved.[17] Thus there is general agreement that nonconsensual private surveillance should be outlawed completely;[18] and the problem in this area reduces to determining how surveillance can most effectively be controlled.

When the government enters the picture, however, the stakes in-

---

PROB. 253, 255 (1966). This Comment will follow the traditional pattern and use privacy as a convenient shorthand to refer to all the interests.

14. T. COOLEY, TORTS 29 (2d ed. 1888); *see* Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). The nature of the right to privacy is a much debated question. *See, e.g.*, Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U.L. REV. 962 (1964); Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960); *Symposium*, 31 LAW & CONTEMP. PROB. 251 (1966); Josephson, Book Review, 15 U.C.L.A.L. REV. 1586 (1968). But whatever the nature and basis of the right it is well established that a common law cause of action for invasion of privacy will lie for electronic eavesdropping and wiretapping. *See, e.g.*, McDaniel v. Atlanta Coca-Cola Bottling Co., 60 Ga. App. 92, 2 S.E.2d 810 (1939) (electronic eavesdropping); Rhodes v. Graham, 238 Ky. 225, 37 S.W.2d 46 (1931) (wiretapping). Electronic surveillance also invades privacy in the broader sociological sense of denying the individual control over access to information about himself. *See generally* Fried, *Privacy*, 77 YALE L.J. 475 (1968).

15. *See generally* King, *Wire Tapping and Electronic Surveillance: A Neglected Constitutional Consideration*, 66 DICK. L. REV. 17, 27-30 (1961). Although particular instances of surveillance may inhibit communication if the victims suspect they are being monitored, the greatest danger lies in the general adverse impact that widespread—and well-publicized—surveillance would have on communication habits.

16. Some of the many private uses of electronic surveillance are catalogued in PRIVACY AND FREEDOM, *supra* note 1, at 104-18.

17. *See id.* at 117.

18. *See, e.g.*, ABA STANDARDS, *supra* note 5, at 99, 101. The lone dissent appears in Lipset, *The Wiretapping-Eavesdropping Problem: A Private Investigator's View*, 44 MINN. L. REV. 873 (1960).

Exceptions could be made for scientific research which requires secrecy if the legislature determines that the benefits of the research outweigh the invasions of privacy involved.

crease drastically and the problem becomes more complex. The right of privacy assumes a new dimension when the government is the privacy invader. Because of the power of the government and the ultimate sanctions it possesses—deprivation of life or liberty—the government is a far more dangerous intruder than the individual. The ability of the government to monitor conversations has implications far beyond the intrusion upon the "inviolate personality"[19] of the individual; for governmental access to information is but one step removed from governmental control over the source of the information.[20] The dangers of an all-powerful government were well recognized by the founders of this country; the bill of rights is replete with measures to limit the power of the government vis-à-vis the individual.[21] Most important of these in the surveillance context is the fourth amendment which protects the individual from unreasonable searches and seizures,[22] including those conducted with electronic listening devices.[23] The threat to freedom of communication also is enhanced when it is the government who is performing the surveillance. The same factors which make the government the most dangerous snooper magnify the chilling effect of governmental surveillance.

---

19. Warren & Brandeis, *supra* note 14, at 205.

20. *Cf.* G. ORWELL, 1984 (1949).

21. *See* U.S. CONST. amends. I-VIII.

22. *Id.* amend. IV: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

23. See text at notes 71-78 *infra*. While the right of privacy against the government is far broader than the fourth amendment, *see, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965), the fourth amendment has provided the only concrete constitutional protection against electronic surveillance per se. That is not to say that it is the only constitutional interest which is invaded by governmental surveillance, however. One of the principles underlying the fifth amendment's privilege against self-incrimination is the notion that an accused should not be required to convict himself out of his own mouth—that the government must do so by independent evidence. *See* 8 J. WIGMORE, EVIDENCE § 2251, at 317-18 (McNaughton ed. 1961). Since electronic surveillance involves deceit rather than technical compulsion, the fifth amendment has not been held to preclude its use. *See* Olmstead v. United States, 277 U.S. 438, 462 (1928); Berger v. New York, 388 U.S. 41, 107 (1967) (White, J., dissenting). But to the extent that it is a method of extracting testimony from a person without his consent, electronic surveillance is repugnant to the underlying fairness norm of the fifth amendment. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 478-79 (1928) (Brandeis, J., dissenting). The notion that the government should not require the accused to aid in his own conviction is violated when testimony is elicited by stealth as well as when it is coerced.

Furthermore, there are situations where electronic surveillance may run afoul of the constitution because it is used in a particular way. For example, eavesdropping upon the conversations of an accused and his attorney violates the sixth amendment right to counsel. *See* Coplon v. United States, 191 F.2d 749 (D.C. Cir. 1951).

However, the interests served by allowing governmental surveillance also increase correspondingly. Electronic surveillance is an effective technique for the detection and investigation of crime, especially in an age when the criminal has the tools of modern technology at his disposal.[24] As social conditions deteriorate and crime rates continue to rise, the clamor for the use of police surveillance to maintain law and order is bound to increase apace. The tension between the demands of privacy and the demands of law enforcement makes the formulation of rules governing police surveillance difficult, both theoretically and politically. Within the narrow confines of fourth amendment protection delineated by the Supreme Court, state legislative experimentation in the electronic surveillance field is foreclosed. But there remain large areas where the states and the federal government are still free to formulate rules on a policy basis. The solutions have been, for the most part, a series of uneasy truces, and the controversy is still going on.

### *A. The Background*

The constitutional history of electronic surveillance law has centered around the efforts of criminal defendants to have evidence obtained by electronic surveillance excluded from their trials. The constitutional objection was based on the proposition that the seizure of a conversation without the consent of the speaker constitutes an unreasonable search and seizure under the fourth amendment.[25] As such, it would be excludable under the rule of *Weeks v. United States*.[26] Unfortunately, the United States Supreme Court, in the first surveillance case it considered, decided that the interception of a telephone conversation accomplished without trespassing on the premises of the victim was not a "search and seizure" and was therefore not subject to the restrictions of the fourth amendment.[27] The same result was later

24. *See* ABA STANDARDS, *supra* note 5, at 22-78. The question of the need for electronic surveillance will be explored at greater length in the text at notes 197-200 *infra*.

25. *See, e.g.*, On Lee v. United States, 343 U.S. 747 (1952); Goldman v. United States, 316 U.S. 129 (1942); Olmstead v. United States, 277 U.S. 438 (1928).

26. 232 U.S. 383 (1914) (evidence obtained by the government in violation of the fourth amendment is inadmissible in federal criminal trials).

27. Olmstead v. United States, 277 U.S. 438 (1928). The Court in *Olmstead* held that the wiretap involved did not violate the defendant's right to be free from unreasonable searches and seizures because it did not involve a "seizure of his papers or his tangible material effects, or an actual physical invasion of his house or 'curtilage' for the purpose of making a seizure." *Id.* at 466. The Court also seemed to rest its holding in part on an assumption of risk theory—that the defendant surrendered his fourth amendment protection when he projected his voice outside the house along the telephone wires. *Id.* However, in Goldman v. United States, 316 U.S. 129 (1942),

reached with respect to electronic eavesdropping.[28] Although the Court softened this stance in subsequent cases,[29] it was almost 40 years until electronic searches were brought fully within the purview of the fourth amendment.[30] Throughout that period the Court limited the operation of the fourth amendment to surveillance which involved a physical invasion of an area traditionally protected against searches and seizures.[31] Thus, the constitutionality of an electronic search turned not on whether a confidential communication had been intercepted, but whether a "constitutionally protected area"[32] had been invaded in the process.[33]

The history of federal statutory law was notable chiefly for congressional inaction. Electronic eavesdropping[34] was completely free from regulation. The only federal law which dealt with electronic surveillance at all was section 605 of the Communications Act of

---

an electronic eavesdropping case, the Court indicated that this language was not essential to the *Olmstead* holding. There, the Court rejected an argument that *Olmstead* did not apply because the defendant had not projected his voice outside of a closed room. *Id.* at 135-36.

28. Goldman v. United States, 316 U.S. 129 (1942).

29. In Silverman v. United States, 365 U.S. 505 (1961), the Court indicated that a *technical* trespass was not required to bring the fourth amendment into play. However it was still necessary that the surveillance be accomplished by "an actual intrusion into a constitutionally protected area." *Id.* at 512.

In Wong Sun v. United States, 371 U.S. 471 (1963), the Court found that the fourth amendment could protect against the overhearing of conversations, *id.* at 485, thus implicitly overruling one of the basic tenets of *Olmstead*: that the fourth amendment protected only tangible effects. See note 27 *supra*. In so doing, the Court laid the foundation for later decisions which held that the interception of conversations was a fourth amendment search and seizure with or without a physical invasion of the premises. See Part I, section B *infra*.

30. *See* Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967). Both cases are discussed in Part I, section B *infra*.

31. Lopez v. United States, 373 U.S. 427, 439-40 (1963); *see, e.g.*, Clinton v. Virginia, 377 U.S. 158, *rev'g per curiam* 204 Va. 275, 130 S.E.2d 437 (1963); Silverman v. United States, 365 U.S. 505 (1961); Goldman v. United States, 316 U.S. 129 (1942).

32. This term was first used to define the scope of fourth amendment protection against eavesdropping in Silverman v. United States, 365 U.S. 505, 510, 512 (1961). The term referred to those areas which, under conventional search and seizure law, have been held to be protected by the fourth amendment. The areas include, *e.g.*, a private home or apartment, Silverman v. United States, *supra*; a hotel room, United States v. Jeffers, 342 U.S. 48 (1951); or a business office, Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920). *See generally* Hendricks, *Eavesdropping, Wiretapping, and the Law of Search and Seizure—Some Implications of the Katz Decision*, 9 ARIZ. L. REV. 428, 432-35 (1968).

33. *See* Irvine v. California, 347 U.S. 128 (1954); Silverman v. United States, 365 U.S. 505 (1961).

34. See note 6 *supra* for the distinction between electronic eavesdropping and wiretapping.

1934,[35] which the Supreme Court interpreted to outlaw wiretapping.[36] Although the statute's proscription on divulgence of intercepted communications rendered wiretap evidence inadmissible in federal courts,[37] wiretapping for investigative purposes continued because of the singular interpretation which the Justice Department placed on the statute.[38] That agency reasoned that the statute was violated only where both an interception and a divulgence took place; and further, that dissemination within the government was not a divulgence.[39] Under that interpretation, wiretapping for internal governmental use was not prohibited.[40]

California law, in contrast, was comprehensive but confused. California was the first state to deal with the problem of electronic surveillance[41] when, in 1862, it outlawed the tapping of telegraph lines.[42] The first California Penal Code, in 1872, contained fairly detailed provisions to protect the security of telegraph facilities.[43] With the advent of more modern communications systems and more sophisticated interception techniques, these statutes were amended and reamended[44] until, by 1967, the entire scheme was badly in need of overhaul. Wiretapping was outlawed completely by statute,[45] and, since California excludes evidence secured in violation of statute as well as that obtained by un-

35. 47 U.S.C. § 605 (1964), *as amended* (Supp. IV, 1965-68). The statute at that time read: "[N]o 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 . . . ." *Id.*

36. Nardone v. United States, 302 U.S. 379 (1937). This prohibition was interpreted to apply to intrastate as well as interstate telephone communications, Weiss v. United States, 308 U.S. 321 (1939), and to government agents as well as private parties, Nardone v. United States, *supra.*

37. Nardone v. United States, 302 U.S. 379 (1937). State courts were free to adopt their own rule of admissibility. Schwartz v. Texas, 344 U.S. 199 (1952). *Schwartz* was recently overruled by Lee v. Florida, 392 U.S. 378 (1968), which made the exclusionary provisions of section 605 applicable to the states. However, the point has been largely mooted since section 605 has been amended to delete its provisions on wiretapping. See note 94 *infra.*

38. *See* Katzenbach, *An Approach to the Problems of Wire-Tapping*, 32 F.R.D. 107, 107-08 (1963); Rogers, *The Case for Wiretapping*, 63 YALE L.J. 792, 793-96 (1954).

39. *See* Donnelly, *Comments and Caveats on the Wiretapping Controversy*, 63 YALE L.J. 799, 800-01 (1954); Brownell, *The Public Security and Wiretapping*, 39 CORNELL L.Q. 195, 198-99 (1954).

40. *See* authorities cited notes 38 & 39 *supra.*

41. THE EAVESDROPPERS, *supra* note 4, at 8.

42. Ch. CCLXII, § 6, [1862] Cal. Stats. 289, *as codified*, CAL. PENAL CODE § 640 (1872), *as amended*, ch. DXXVIII, § 6, [1905] Cal. Stats. 691; ch. 117, [1915] Cal. Stats. 210; ch. 571, [1955] Cal. Stats. 1070; ch. 956, § 3, [1965] Cal. Stats. 2575 (former Penal Code § 640, repealed and replaced by Penal Code § 631 in 1967).

43. CAL. PENAL CODE §§ 638-41 (1872).

44. For example, the wiretapping statute was amended four times. See note 42 *supra.*

45. Ch. 956, § 3, [1965] Cal. Stats. 2575 (former Penal Code § 640).

constitutional seizure,[46] all wiretap evidence was inadmissible in California criminal trials.[47] Electronic eavesdropping was also prohibited by statute,[48] but the eavesdropping statutes, with one exception, did not apply to law enforcement officials.[49] Hence evidence obtained by police eavesdropping was admissible, unless its procurement involved a physical trespass which would render it constitutionally excludable.[50]

The California laws, while fairly comprehensive in scope, were basically a series of ad hoc reactions to the technological advances of the past few decades, and suffered from the absence of a clear-cut policy on the regulation of electronic devices. The resulting hodgepodge of statutes was characterized by redundant statutory provisions,[51] disparate penalties for morally indistinguishable offenses,[52] and a complete lack of standards to govern police conduct.[53]

Such was the background from which the California Privacy Act originated.[54] The new statute, although ambiguous and deficient in

46. California apparently proceeds on the theory that a search or seizure which violates a statute is per se unreasonable, and hence unconstitutional. *See* Wirin v. Horrall, 85 Cal. App. 2d 497, 193 P.2d 470 (1948); *cf.* People v. Cahan, 44 Cal. 2d 434, 440, 282 P.2d 905, 908 (1955).

47. The admissibility of evidence obtained in violation of the wiretap statute (then Penal Code § 640) was never squarely decided. The Supreme Court of California adopted the exclusionary rule for evidence obtained by unconstitutional search and seizure in People v. Cahan, 44 Cal. 2d 434, 282 P.2d 905 (1955), but nontrespassory wiretapping was not then considered to be unconstitutional. However, in numerous cases involving alleged nontrespassory violations of the wiretap statute, the court, while not finding a violation, apparently proceeded on the assumption that the evidence would have been excludable if there had been. *See, e.g.*, People v. Malotte, 46 Cal. 2d 59, 292 P.2d 517 (1956).

48. Former Penal Code section 653j prohibited eavesdropping on or recording of confidential communications. Ch. 1886, [1963] Cal. Stats. 3871 (repealed 1967). Section 653i proscribed the eavesdropping on or recording of privileged communications of persons in custody. Ch. 1879, [1957] Cal. Stats. 3285 (repealed 1967). Section 653h dealt with the installation of dictographs. Ch. 525, [1941] Cal. Stats. 1833 (repealed 1967).

49. The exception was former Penal Code section 653i which dealt with surveillance of persons in police custody. *See* statutes cited note 48 *supra.*

50. *Compare, e.g.*, People v. Chandler, 262 Cal. App. 2d 350, 355, 68 Cal. Rptr. 645, 648 (1968), *with* People v. Tarantino, 45 Cal. 2d 590, 594-95, 290 P.2d 505, 508-09 (1955).

51. *Compare* ch. 1886, [1963] Cal. Stats. 3871 (former Penal Code § 653j) (prohibiting electronic eavesdropping), *with* ch. 525, [1941] Cal. Stats. 1833 (former Penal Code § 653h) (prohibiting the installation of dictographs).

52. *Compare* ch. 956, § 3, [1965] Cal. Stats. 2575 (former Penal Code § 640) (providing up to five years imprisonment and/or $5,000 fine for wiretapping), *with* ch. 1886, [1963] Cal. Stats. 3871 (former Penal Code § 653j) (providing up to one year imprisonment and/or $1,000 fine for electronic eavesdropping).

53. *See* statutes cited note 48 *supra.*

54. For a survey of the federal and constitutional law in the field at that time see Sullivan, *Wiretapping and Eavesdropping: A Review of Current Law*, 18 HASTINGS L.J. 59 (1966).

some respects, made several significant and beneficial changes in the California law. It provided strong civil as well as criminal sanctions for unauthorized surveillance;[55] it outlawed the manufacture and sale of electronic surveillance equipment;[56] and, most importantly, it proscribed all private wiretapping and eavesdropping performed without the consent of *all* the parties to the communication.[57] California was only the third state to require all-party consent for all types of surveillance,[58] and that provision was by far the most significant change effected by the 1967 legislation.

In other respects the law was disappointing. Rather than starting afresh, the draftsmen for the most part merely collected and amended existing Penal Code sections dealing with the subject.[59] This resulted in the perpetuation of antiquated statutory provisions more suitable for the protection of telegraph systems than of modern communications facilities.[60]

---

55. *See* CAL. PENAL CODE §§ 631, 632, 634, 636, 637.2 (West Supp. 1968). These remedies are discussed in Part V *infra*.

56. *Id.* § 635.

57. *Id.* §§ 631-32. Previously both California and federal courts had permitted all forms of participant monitoring. *See, e.g.*, Lopez v. United States, 373 U.S. 427 (1963) (recording of bribery attempt by federal agent); Rathbun v. United States, 355 U.S. 107 (1957) (police monitoring of threatening call on an extension phone); On Lee v. United States, 343 U.S. 747 (1952) (transmission of conversation with suspect by informer to federal narcotic agent); People v. Dement, 48 Cal. 2d 600, 311 P.2d 505 (1957) (police listening in on extension phone); People v. Malotte, 46 Cal. 2d 59, 292 P.2d 517 (1956) (police undercover agents recording telephone conversations by means of an induction coil); People v. Fisher, 208 Cal. App. 2d 78, 25 Cal. Rptr. 242 (1962) (informer transmitting conversations with suspect to police); People v. Albert, 182 Cal. App. 2d 729, 6 Cal. Rptr. 473 (1960) (informer recording conversation with suspect).

58. Illinois and Pennsylvania had reached the same result by judicial interpretation of their surveillance statutes. *See* People v. Kurth, 34 Ill. 2d 387, 216 N.E.2d 154 (1966); Commonwealth v. Murray, 423 Pa. 37, 223 A.2d 102 (1966). Nevada requires the consent of all parties for wiretapping, NEV. REV. STAT. § 200.620(1) (1967), but not for electronic eavesdropping. *Id.* § 200.650. Michigan requires all-party consent for electronic eavesdropping, MICH. COMP. LAWS ANN. § 750.539c (1968), but its wiretapping statute speaks only in terms of unauthorized tapping. *Id.* § 750.540. *See generally* Greenawalt, *The Consent Problem in Wiretapping and Eavesdropping*, 68 COLUM. L. REV. 189, 207-11 (1968).

59. Present Penal Code sections 631, 632, 636, 637, and 637.1 had their origin in former Code sections 640, 653j, 653i, 619, and 621 respectively. *Compare* CAL. PENAL CODE § 631(a) (West Supp. 1968), *with* ch. 956, § 3, [1965] Cal. Stats. 2575 (former Penal Code § 640); CAL. PENAL CODE § 632 (West Supp. 1968), *with* ch. 1886, [1963] Cal. Stats. 3871 (former Penal Code § 653j); CAL. PENAL CODE § 636 (West Supp. 1968), *with* ch. 1879, [1957] Cal. Stats. 3285 (former Penal Code § 653i); CAL. PENAL CODE § 637 (West Supp. 1968), *with* ch. DXXVIII, § 1, [1905] Cal. Stats. 689 (former Penal Code § 619); CAL. PENAL CODE § 637.1 (West Supp. 1968), *with* ch. DXXVIII, § 3, [1905] Cal. Stats. 690 (former Penal Code § 621).

60. For example, the wiretapping statute was originally drafted to protect telegraph facilities and it retains much of the original language today. *Compare* CAL. PENAL CODE § 640 (1872), *with* CAL. PENAL CODE § 631 (West Supp. 1968).

It is also unfortunate that the law did not deal more concretely with the problem of law enforcement surveillance. The bill as originally drafted applied the proscriptions on surveillance to law enforcement officials as well as private parties.[61] During the course of legislative consideration, the law enforcement lobby succeeded in having provisions inserted which nullified the effect of the legislation for most law enforcement officers.[62] But this exemption for police surveillance was not accompanied by any standards to circumscribe its use.[63]

All in all, however, the Privacy Act was an improvement over the existing law. Even though it left much to be desired, it gave California one of the most comprehensive of state regulatory systems.

### *B. The Developments*

At the same time the California Legislature was considering the Privacy Act, the United States Supreme Court had before it a case which was to spark a revolution in the law of electronic surveillance. The case was *Berger v. New York*,[64] and in it the Court sounded the death knell of the trespass doctrine. Berger had been convicted of conspiracy to bribe a public official solely on the basis of evidence secured by bugging the business offices of his co-conspirators. The eavesdropping device was planted pursuant to an order issued under section 813-a of the New York Code of Criminal Procedure.[65] That statute permitted state judges to authorize electronic eavesdropping upon a showing of probable cause to believe that evidence of crime would be obtained thereby.[66]

The Supreme Court overturned Berger's conviction. It found the

---

61. A.B. 860, 1967 Sess. California Legislature (Author's Draft, March 1, 1967).

62. *See* Letter from then Speaker of the California Assembly Jesse M. Unruh (author of A.B. 860), Nov. 22, 1968, on file with the *California Law Review* [hereinafter cited as Unruh Letter]. The results of the lobbying process can be observed in the successive amendments to the bill as it proceeded through the Legislature. *See* A.B. 860, 1967 Sess. California Legislature (Author's Draft, March 1, 1967); *id., as amended* April 20, 1967; *id., as amended* June 5, 1967; *id., as amended* June 13, 1967; *id., as amended* June 16, 1967.

63. The exemption allowed the designated law enforcement officers to overhear or record any communication which they could lawfully have overheard or recorded prior to the statute. CAL. PENAL CODE § 633 (West Supp. 1968). This merely perpetuated the previous system which was totally devoid of any standards. *See* statutes cited note 48 *supra*.

64. 388 U.S. 41 (1967). Although *Berger* was decided shortly before the final passage of the California Privacy Act, it is treated herein as a subsequent, or at least contemporaneous development. The Privacy Act was drafted before the *Berger* opinion was handed down, and the opinion apparently had no effect on either its content or passage.

65. Ch. 676, [1958] N.Y. Laws 1513, *as amended*, ch. 681, § 86, [1967] N.Y. Laws 1623, *repealed*, ch. 546, § 1, [1968] N.Y. Laws 1948.

66. *Id.*

statute under which the eavesdrop order was issued to be unconstitutional on its face because it authorized overly broad searches. After specifically holding—for the first time—that electronic eavesdrops were searches within the meaning of the fourth amendment,[67] the Court struck down the statute because it did not contain the requisite fourth amendment safeguards for authorization of governmental searches. The Court found the New York statute lacking in several respects: First, the statute did not require a description of the conversations sought to be seized, or even a showing of belief that a specific crime had been or was being committed. These omissions violated the requirement of the fourth amendment that warrants describe with particularity the place to be searched and the things to be seized. Second, the 60-day listening period authorized by the statute was the equivalent of a series of searches and seizures pursuant to a single showing of probable cause. Third, there was no requirement for prompt execution. Fourth, renewal of the authorization could be obtained without a new showing of probable cause. Fifth, no provision was made for termination of the surveillance once the conversation sought had been obtained. Sixth, the statute contained no provision for a return on the warrant. Seventh, there was no requirement that notice be given to the subject of the surveillance or a showing of exigent circumstances be made in lieu thereof.[68] The absence of these safeguards rendered the warrants suspect; the Court felt they were too reminiscent of the general warrants which the fourth amendment was intended to eliminate.[69]

Although at the time it appeared the *Berger* decision was heralded as signalling the demise of the trespass requirement,[70] its primary sig-

67. 388 U.S. at 51. Although passages in Silverman v. United States, 365 U.S. 505, 509-12 (1961) had indicated that conversations could be the subject of electronic searches and seizures, the *Berger* opinion was the first to hold explicitly that the capture of conversations by electronic means was a search within the meaning of the fourth amendment.

68. 388 U.S. at 58-60.

69. *Id.* at 58.

70. At the time it appeared, the *Berger* decision was hailed by many as bringing all electronic surveillance, both trespassory and nontrespassory, within the purview of the fourth amendment. *E.g.*, Berger v. New York, 388 U.S. 41, 64 (Douglas, J., concurring); Note, *Electronic Surveillance After Berger*, 5 SAN DIEGO L. REV. 107, 122-23 (1968); 17 DE PAUL L. REV. 219, 226-27 (1967). Although the placement of the recording device in *Berger* involved a trespass, Justice Clark's majority opinion mentioned the trespassory aspect of the eavesdrop only once. 388 U.S. at 44. The Court's holding that the use of electronic devices to capture conversations was a search within the meaning of the fourth amendment apparently was not conditioned on an accompanying trespass, *id.* at 51, and the general tenor of the opinion appeared to cover all eavesdrops whether accompanied by physical intrusion or not. However, later cases have made it clear that the *Berger* decision was predicated on a trespass, and that the trespassory distinction retained its vitality until it was finally interred in Katz v. United States, 389 U.S. 347 (1967). *See* Kaiser v. New York, 394 U.S 280 (1969); Desist v. United States, 394 U.S. 244 (1969).

nificance today lies in the Court's detailed criticism of the New York statute. In enumerating the deficiencies of that statute, the Court apparently set out the criteria which must now be met in order to legitimize electronic searches.

The following term, in *Katz v. United States*,[71] the Supreme Court fulfilled the promise of *Berger* by finally laying to rest the trespass doctrine and bringing all nonconsensual electronic surveillance within the purview of the fourth amendment.[72] In *Katz*, FBI agents had procured evidence of petitioner's bookmaking activities by installing electronic monitoring devices on the outside of a public telephone booth from which he transacted his business. Katz' conversations were recorded and the recordings were admitted at his trial, resulting in a conviction for transmitting wagering information by telephone.

The Supreme Court reversed the conviction, holding that the monitoring of Katz' conversations was violative of the fourth amendment,[73] and explicitly overruling the decisions on which the trespass doctrine was based.[74] This was not particularly startling in light of *Berger*, but the method by which the Court reached its conclusion is of great significance. Whereas previous decisions had been couched in terms of physical invasion of a "constitutionally protected area,"[75] the Court here not only rejected the contention that physical trespass was a requirement, but also abandoned the idea that the fourth amendment's protection applies only in certain constitutionally protected areas. Rather, noting that the fourth amendment protects people rather than places, Justice Stewart found that the constitutional protection applies to all those conversations which a person seeks to preserve as private.[76] The area in which the conversation or seizure takes place is still important, but only as evidence of a person's expectation of privacy; it is no longer dispositive.

The result in *Katz* was a logical outgrowth of the Court's implicit recognition in *Berger* that the aspect of electronic surveillance which is repugnant to the principle of the fourth amendment is the government's seizure of a man's private conversations, not the incidental trespass which might occur in the process.[77] The boundaries of the new "ex-

71. 389 U.S. 347 (1967).

72. While *Katz* involved electronic eavesdropping, there is no doubt that the constitutional principles it enunciates apply equally to wiretapping. *See, e.g.*, Hendricks, *supra* note 32, at 438.

73. 389 U.S. at 353.

74. *Id.* (overruling Olmstead v. United States, 277 U.S. 438 (1928), and Goldman v. United States, 316 U.S. 129 (1942)).

75. *E.g.*, Lopez v. United States, 373 U.S. 427, 438-39 (1963); Silverman v. United States, 365 U.S. 505, 510-12 (1961).

76. 389 U.S. at 349-51, 359.

77. *Cf.* Desist v. United States, 394 U.S. 244, 248 (1969).

pectation of privacy" test are yet to be delineated, but at a minimum it greatly expands the scope of protection afforded by the fourth amendment and provides a more realistic approach than technologically outmoded property concepts.[78]

The classification of electronic interceptions as fourth amendment searches and seizures carried with it important consequences. Antecedent judicial authorization, long a cornerstone of conventional search law, is now mandatory for electronic searches.[79] Surveillance without such authorization is an unreasonable search and seizure per se,[80] and evidence procured thereby is inadmissible in both federal and state courts.[81] In addition to the exclusionary rule, the whole body of law which has been built up around the fourth amendment, governing such questions as probable cause, standing to suppress evidence, and validity of consent, is now applicable to electronic searches.

*Berger* and *Katz* left two unsettled controversies in their wake. The Supreme Court's condemnation of the New York statute in *Berger* for failing to meet the particularity requirement of the fourth amendment has created speculation that no warrant can be devised which could authorize the type of nonselective surveillance used in *Berger* and still meet fourth amendment particularity standards.[82] If this is true,

78. *Cf.* Silverman v. United States, 365 U.S. 505, 512-13 (1961) (Douglas, J., dissenting).

79. Katz v. United States, 389 U.S. 347, 356-57 (1967).

80. *Id.*

81. Bringing electronic surveillance under the fourth amendment made the exclusionary rule, see note 26 *supra*, binding on the states through Mapp v. Ohio, 367 U.S. 643 (1961).

82. *See, e.g.*, Berger v. New York, 388 U.S. 41, 71 (1967) (Black, J., dissenting); *id.* at 113 (White, J., dissenting); Schwartz, *Electronic Eavesdropping—What The Supreme Court Did Not Do*, 4 CRIM. L. BULL. 83 (1968); 52 MINN. L. REV. 541, 552-53 (1967).

The *Katz* Court indicated that the particularity requirement could have been met in that case had the agents attempted to obtain a warrant. 389 U.S. at 354. However, *Katz* involved a situation where the interception could be limited to the criminal conversations sought. According to the government's account of the surveillance, the agents, aware of Katz' habits, knew at what times he would use the telephone booth and limited their monitoring to those periods. Six conversations averaging three minutes each were recorded, and on the only occasion where the conversation of another party was inadvertently intercepted they did not listen. 389 U.S. at 354 & nn.14, 15. The same particularity was possible in the cases cited approvingly in *Berger*. In *Berger* the Court cited Goldman v. United States, 316 U.S. 129 (1942), Lopez v. United States, 373 U.S. 427 (1963), and Osborn v. United States, 385 U.S. 323 (1966), to refute the charge that no warrant could be drawn to meet the fourth amendment requirements laid down therein. 388 U.S. at 63. *Goldman* was overruled in *Katz*, see note 74 *supra* and accompanying text, but both *Lopez* and *Osborn* were participant monitoring cases where the interceptor was in a position to limit the eavesdropping to particular conversations.

At the time of the decision there was also some concern that the apparent requirement that the victim be given notice, 388 U.S. at 60, created another insuperable

that type of surveillance is now completely proscribed. The requirement that a warrant describe with particularity "the place to be searched and the persons or things to be seized"[83] was intended to prevent general searches by limiting the scope of the search to the items specified in the warrant.[84] The problem encountered in applying this standard to electronic surveillance is obvious. Although some types of surveillance, such as that involving a participant or that which is accompanied by visual observation, are sufficiently selective to meet the requirement,[85] most electronic surveillance is inherently indiscriminate. Such practices as tapping a private telephone line or bugging a home for an extended period of time result in the interception of innocent as well as criminal conversations, and the conversations to be seized are impossible to describe in advance.[86] Whether a warrant can be drawn to authorize that type of surveillance is a question which the Supreme Court has not yet answered. Congress has answered the question in the affirmative, however, in title III of the Crime Control Act,[87] and the ultimate resolution awaits a test of the constitutionality of that Act.

*Berger* and *Katz* also left unanswered the question of whether judicial authorization is now required for participant monitoring. In both decisions the Court extolled *Osborn v. United States*,[88] a case involving judicially authorized participant recording, as a model of constitutionally permissible surveillance.[89] This has led to speculation that a warrant might now be a sine qua non for participant monitoring as well as

---

obstacle to legalized surveillance. *See, e.g.*, 388 U.S. at 86 (Black, J., dissenting). This fear was allayed in *Katz*, where the Court indicated that notice could be dispensed with on a destruction of evidence rationale. 389 U.S. at 355 n.16.

83. U.S. CONST. amend. IV.

84. Marron v. United States, 275 U.S. 192, 195-96 (1927).

85. See note 82 *supra*.

86. This type of surveillance will intercept not only conversations of the suspect which are not related to the offense under investigation, but also conversations of wholly innocent parties.

87. *See* 18 U.S.C. §§ 2516, 2518 (Supp. IV, 1965-68). These provisions are discussed in Part III *infra*.

88. 385 U.S. 323 (1966). In *Osborn*, two federal judges authorized an FBI informer to record conversations with James Hoffa's attorney for the purpose of determining whether an attempt was being made to tamper with the jury in Hoffa's so-called *Test Fleet Trial*. *Id.* at 328-29.

89. *See* Berger v. New York, 388 U.S. 41, 56-57, 63 (1967); Katz v. United States, 389 U.S. 347, 355-56 (1967). In the *Berger* opinion, Justice Clark's characterization of the eavesdrop in *Osborn* as "[A]n invasion of privacy protected by the Fourth Amendment, [which] was admissible because of the authorization of the judges . . . ." implies that the recording would not have been valid without the warrant. 388 U.S. at 56-57. *See The Supreme Court, 1966 Term*, 81 HARV. L. REV. 69, 187 (1967).

The *Berger* Court placed itself in a rather anomalous position. It struck down the New York statute which contained many fourth amendment safeguards, *see* 388

third-party interceptions.[90] The federal courts of appeals are divided on the question[91] and the Supreme Court has granted certiorari to resolve it.[92]

The most recent development in surveillance law was the enactment of the Omnibus Crime Control and Safe Streets Act of 1968.[93] Title III of this Act brings almost the full range of surveillance activities under federal control. It purports to regulate all nonconsensual wiretapping and eavesdropping, both public and private,[94] although it is not altogether clear that Congress has the power to regulate intrastate eavesdropping.[95] Nonconsensual private surveillance is prohib-

---

U.S. at 84-85 (Black, J., dissenting), without considering if the statute as applied to the petitioner denied him his fourth amendment rights. *Id.* at 55. At the same time they held up *Osborn*, where the eavesdrop order was issued without any statutory authorization, as the shining example of fourth amendment compliance. *Id.* at 56-57, 63.

90. *See, e.g.*, Pitler, *Eavesdropping and Wiretapping—The Aftermath of Katz and Kaiser: A Comment*, 34 BROOKLYN L. REV. 223, 224-26 (1968); Schwartz, *supra* note 82, at 87.

91. *Compare* United States v. White, 405 F.2d 838 (7th Cir.) (en banc), *cert. granted*, 394 U.S. 957 (1969), *with, e.g.*, United States v. Kaufer, 406 F.2d 550 (2d Cir.), *aff'd on other grounds per curiam*, 394 U.S. 458 (1969); Holt v. United States, 404 F.2d 914 (10th Cir. 1968), *cert. denied*, 393 U.S. 1086 (1969); Dancy v. United States, 390 F.2d 370 (5th Cir. 1968).

92. United States v. White, 405 F.2d 838 (7th Cir.), *cert. granted*, 394 U.S. 957 (1969) (No. 1024, 1968 Term; renumbered No. 46, 1969 Term).

93. Pub. L. No. 90-351, 82 Stat. 197 (1968).

94. *See* 18 U.S.C. §§ 2510-11 (Supp. IV, 1965-68). The Act also amended section 605 of the Communications Act of 1934 to remove wiretapping from its coverage. *See* 47 U.S.C. § 605 (Supp. IV, 1965-68).

95. *See* S. REP. No. 1097, 90th Cong., 2d Sess. 92 (1968) [hereinafter cited as SENATE REPORT]. Congressional power to prohibit both private and governmental interception of intra- as well as inter-state wire communications is well established under the commerce clause. *See* Weiss v. United States, 308 U.S. 321 (1939). However, the power of Congress to legislate against the interception of totally intrastate oral communications—particularly interceptions by private parties—is open to serious question, although the recent cases of Katzenbach v. Morgan, 384 U.S. 641 (1966) and United States v. Guest, 383 U.S. 745 (1966) have indicated that Congress may possess such power under section five of the fourteenth amendment. *See generally* Cox, *Constitutional Adjudication and the Promotion of Human Rights*, 80 HARV. L. REV. 91 (1966).

Congress recognized that the blanket proscription on the interception of oral communications might be held unconstitutional and provided a series of backup provisions to extend federal regulation to its permissible limit should that in fact occur:

> [A]ny person who—
>
> . . .
>
> (b) willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—
>
> (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
>
> (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
>
> (iii) such person knows, or has reason to know, that such device

ited; a warrant system is set up for law enforcement surveillance; and a broad array of remedial provisions is established to aid in enforcement.[96] Although the Act has been criticized for its permissive treatment of law enforcement surveillance,[97] even its critics would agree that in other respects it constitutes an important advance. It has clarified the law and provided much-needed national legislation in an area in which state laws are notoriously inadequate.[98]

Title III permits surveillance by law enforcement officials under a warrant system which attempts to meet the requirements of *Berger* and *Katz*.[99] It provides for judicial issuance of warrants based on probable cause and describing the person whose conversations are to be seized, the location where the surveillance is to take place, and the nature of the offense for which evidence is sought.[100] The warrants can be issued for a period of 30 days, with renewals available for additional 30-day periods, and expire upon obtaining the desired conversations.[101] There are also numerous ancillary provisions dealing with emergency authorization, notice to the suspect, and authentication of

---

> or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or
>
> (iv) such use or endeavor to 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 relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
>
> (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States; . . .

18 U.S.C. § 2511(1) (Supp. IV, 1965-68).

These measures, with the exception of subsection (v), are based on the commerce power and attempt to reach all activities to which that power can legitimately be extended. *See* SENATE REPORT, *supra* at 92-93. As a practical matter, the most important of these provisions will probably be those in subsections (iii) and (iv).

If the backup provisions are called into play, the area of federal control will depend to a large extent on how expansively the courts interpret them, particularly subsection (iii). If "component" is interpreted to mean every constituent part of a piece of electronic gear, *i.e.*, every resistor, capacitor, or other element, the scope of this section will be large indeed, and virtually every electronic surveillance device will fall under federal control. If, on the other hand, components are considered to be major elements of a total surveillance system, *i.e.*, microphone, recorder, or transmitter, federal control will not be so pervasive, and a significant amount of electronic surveillance will remain exclusively under state control.

96. 18 U.S.C. §§ 2510-20 (Supp. IV, 1965-68).

97. *See, e.g.*, SENATE REPORT, *supra* note 95, at 166-76 (additional views of Mr. Hart); Schwartz, *The Legitimation of Electronic Eavesdropping: The Politics of "Law and Order"*, 67 MICH. L. REV. 455 (1969).

98. *See* Berger v. New York, 388 U.S. 41, 112 (1967) (White, J., dissenting); SENATE REPORT, *supra* note 95, at 69.

99. *See* SENATE REPORT, *supra* note 95, at 74-75, 96, 101-05.

100. 18 U.S.C. §§ 2518(1)-(4) (Supp. IV, 1965-68).

101. *Id.* § 2518(5).

the recordings.[102] Because of the complexity of the statute these will be discussed later only as they affect state law.

The constitutionality of various aspects of the scheme has been questioned by some commentators.[103] Most of the criticisms, such as the length of the 30-day authorization period, could easily be remedied by amendment and provide no obstacle to states who wish to set up similar systems.[104] However, the overriding question of whether any warrant authorizing nonselective surveillance can meet the fourth amendment's particularity requirement remains. It seems clear that if this system will not pass constitutional muster, none will; there is little that can be done to particularize a conversation beyond describing the suspect, the location, and the general nature of the conversations to be seized. Despite these difficulties, however, this Comment is premised on the assumption that the major provisions of the Act will be held constitutional. Even though it is difficult to square the dragnet nature of electronic surveillance with the language of the fourth amendment, the Supreme Court in the past has shown itself not averse to liberally construing the fourth amendment to accommodate compelling governmental needs.[105] Four members of the Court have given indications in past opinions that warrant requirements such as those contained in the Act would meet their definition of what is demanded by the fourth amendment,[106] and with the current hue and cry for law and order, it seems highly unlikely that the Court would completely invalidate such a highly touted investigative tool.

Because title III applies to both inter- and intra-state surveillance[107] it has necessarily created minimum standards which state legislation must now meet. In some areas, such as law enforcement surveillance, it establishes explicit standards for state legislation;[108] in others it establishes implicit standards by virtue of the supremacy

102. *Id.* §§ 2518(7)-(9).

103. *E.g.*, Clark, *Wiretapping and the Constitution*, 5 CAL. WESTERN L. REV. 1 (1968); Linzer, *Federal Procedure for Court Ordered Electronic Surveillance: Does it Meet the Standards of Berger and Katz?*, 60 J. CRIM. L.C. & P.S. 203 (1969); Schwartz, *supra* note 97; 1968 DUKE L.J. 1008.

104. Other criticisms include the lack of a mandatory requirement for notice to the victim and the authorization of surveillance without a warrant in emergency situations. *See* authorities cited note 103 *supra*.

105. *See* Terry v. Ohio, 392 U.S. 1 (1968); Camara v. Municipal Court, 387 U.S. 523 (1967); Berger v. New York, 388 U.S. 41, 114 (1967) (White, J., dissenting).

106. In the *Berger* case, three Justices indicated that they felt the New York statute—which was considerably less stringent than title III—was constitutional on its face. *See* 388 U.S. at 68 (Stewart, J., concurring); *id.* at 94-101 (Harlan, J., dissenting); *id.* at 118 (White, J., dissenting). Justice Black believes that the fourth amendment does not apply to electronic surveillance at all. *See id.* at 78-81; Katz v. United States, 389 U.S. 347, 364-74 (1967) (Black, J., dissenting).

107. See text at note 94 *supra*.

108. 18 U.S.C. §§ 2516, 2518 (Supp. IV, 1965-68).

clause. The states are free to enact more restrictive controls, or none at all, but they cannot adopt more permissive regulations.[109] The Crime Control Act provides a benchmark against which all existing and proposed state legislation must now be measured.

## II

### CALIFORNIA LAW TODAY—THE SUBSTANTIVE PROHIBITIONS

The 1967 Privacy Act was California's answer to the growing surveillance problem. It attempted to outlaw, with a few exceptions, all forms of private surveillance, including those involving the consent of one party. This Part will analyze the major provisions of the Act in light of the developments outlined in the preceding discussion and will briefly compare it with the federal scheme. It should be recalled that although the statutes speak in terms of all persons, most of California's proscriptions on wiretapping and eavesdropping do not apply to law enforcement officers.[110] Hence, the ensuing discussion, except where otherwise noted, applies only to surveillance by private parties.

### *A. The California Statutes*

#### *1. Wiretapping*

The problems created by repeated amendment in lieu of original drafting are nowhere more apparent than in Penal Code section 631,[111] the basic statute governing wiretapping. The antecedents of this complex statute date back to 1862 and, as a result of numerous previous amendments, it is badly in need of simplification.[112] Its basic problems stem from its ancient origins and its attempt to protect two different interests—the physical integrity of communications facilities and the privacy of communications—simultaneously.

The statute actually contains two separate clauses dealing with wiretapping activities. The first prohibits the making of unauthorized connections with telephone facilities;[113] the second forbids attempts to learn the contents of telephonic communications without the consent of all

109. *See* SENATE REPORT, *supra* note 95, at 98.

110. See text at note 49 *supra.*

111. CAL. PENAL CODE § 631 (West Supp. 1968).

112. See note 42 *supra.*

113. CAL. PENAL CODE § 631(a) (West Supp. 1968): "Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system . . . is punishable by a fine . . . or by imprisonment . . . ."

parties to the communication.[114] While these provisions overlap to a large degree, each also has an independent significance.

The first provision, since it forbids all unauthorized connections whether made for the purpose of intercepting communications or not,[115] protects utility companies[116] against individuals who attempt to connect their own equipment to the company's system.[117] Prior case law makes it clear that the authorization required to legitimize a connection is not just that of the subscriber, but includes the permission of the utility as well.[118]

The ban on connections also serves a privacy interest, however. By prohibiting all types of connections it prevents the surreptitious interception of telephone conversations. It is bolstered in this effort by the second clause which proscribes any attempt to learn the contents of such a communication without the consent of the conversing parties. Thus it requires the consent of the utility company, all the parties to the conversation, and possibly the subscriber, to legitimately intercept a telephone conversation by means of a connection to the communication facilities.

The second clause also serves a purpose which has generally been overlooked. By its terms the statute forbids the interception of messages in transit or during transmission and reception without the consent of all parties.[119] This proscription applies whether or not there is

114. *Id.* § 631(a): "Any person who . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any such wire, line, or cable, or is being sent from, or received at any place within this state . . . is punishable by a fine . . . or by imprisonment . . . ."

115. The statute is violated by a connection to any of the designated facilities whether or not there is an intent to intercept communications. *See* People v. Trieber, 28 Cal. 2d 657, 171 P.2d 1 (1946) (construing identical language in former Penal Code section 640).

116. The term "utility company" is used for convenience although the statute applies to private telephone systems as well. See note 113 *supra.*

117. Although the entire scheme is purportedly aimed at the protection of privacy, *see* CAL. PENAL CODE § 630 (West Supp. 1968), the property protection role of the anti-connection clause of section 631 was emphasized by the concurrent deletion of a similar provision from section 591 of the Penal Code. Section 591, which deals with injury to telegraph, telephone, or electric lines or facilities, formerly prohibited, *inter alia*, the making of unauthorized connections with telephone or telegraph facilities. *See id.* § 591 (West 1957), *as amended*, (West Supp. 1968). However, simultaneously with the enactment of section 631, section 591 was amended to delete the proscriptions on making connections. Ch. 1509, § 2, [1967] Cal. Stats. 3589. This left the burden of protecting communication facilities on section 631.

118. *See* People v. Trieber, 28 Cal. 2d 657, 171 P.2d 1 (1946); People v. Snowdy, 237 Cal. App. 2d 677, 680-82, 47 Cal. Rptr. 83, 85-86 (1965) (construing identical language in former Penal Code section 640).

119. See note 114 *supra.*

a connection of any kind involved. Not all telephone surveillance involves a connection to the facilities; a call can be surreptitiously monitored by listening on an extension phone or by sharing the receiver with one of the parties. It was the intent of the drafters, and apparently the Legislature, to outlaw just such forms of consensual overhearing, unless all parties are apprised of the existence of the listener.[120] That intent might not be effectuated, however. California courts, in construing identical language in a previous statute, completely ignored the language pertaining to interception during transmission and reception—probably because of the archaic terminology which appears to be primarily applicable to telegraph messages.[121] Similarly, commentators have assumed that section 631 applies only to messages in transit.[122] In light of this history there is a strong possibility that the courts may apply the all-party-consent requirement only to interceptions involving some type of connection with communication facilities.

Redrafting of this statute might be necessary to accomplish the intention of the Legislature, and in any case would be desirable in the interests of simplification. A simple ban on the interception or overhearing of all telephone communications without the consent of all parties would effectively protect the privacy of communications and avoid the ambiguities in the present statute. The property interests of the utility companies would be better relegated to a simple trespass-type statute.[123]

One important advance made in section 631 was the inclusion of internal telephonic communication systems in its coverage.[124] The sur-

120. "This legislation would require that all parties to a telephone conversation must give their consent before an outsider may legally overhear it. This would protect a person placing or receiving a call from a situation where the person on the other end of the line permits an outsider to tap his telephone or listen in on the call." Digest of A.B. 860, 1967 Sess. California Legislature, on file with the *California Law Review*. This legislative digest was used by the author of the bill in explaining its purposes during legislative debate on the proposal. Unruh Letter, *supra* note 62.

121. *See, e.g.*, People v. Fontaine, 237 Cal. App. 2d 320, 332, 46 Cal. Rptr. 855, 864 (1965); People v. Carella, 191 Cal. App. 2d 115, 138, 12 Cal. Rptr. 446, 460 (1961) (construing identical language in former Penal Code section 640).

122. *See* CALIFORNIA CONTINUING EDUCATION OF THE BAR, REVIEW OF SELECTED 1967 CODE LEGISLATION 162 (1967); Degnan, *Evidence*, in CAL. LAW—TRENDS AND DEVELOPMENTS 1967, at 259, 261 (N. Levy ed. 1968).

123. Interference with communications facilities is a trespass to property, not a violation of privacy, and it should be treated as such. The logical course for the Legislature to have pursued in 1967 would have been to leave the proscription on unauthorized connections in the malicious injury statute, see note 117 *supra*, and limit section 631 to the protection of communications. This would have freed the wiretapping statute from ambiguity and placed each offense in its proper context with appropriate penalties for that type of offense.

124. CAL. PENAL CODE § 631(a) (West Supp. 1968), quoted in note 113 *supra*. The prior statute only applied to facilities under the control of telegraph or telephone companies. *See* ch. 956, § 3 [1965] Cal. Stats. 2575 (former Penal Code section 640).

veillance of employees by business organizations is a major threat to privacy in this state,[125] and the prior surveillance statutes did not apply to internal telephone systems.[126] This statute provided the first complete control over the internal monitoring practices of large organizations.[127]

### 2. *Electronic Eavesdropping*

Electronic eavesdropping is governed by sections 632 and 636 of the Penal Code.[128] These provisions are much more straightforward than section 631, probably because they are of later origin.[129] Section 632 prohibits the eavesdropping on or recording of any confidential communication without the consent of all parties to the communication.[130] The confidential communication protected is defined as "any communication carried on in such circumstances as may reasonably indicate that any party to such communication desires it to be confined to such parties."[131] By making the parties' expectation of privacy the basis of the protection accorded oral communications, the California Legislature presaged the Supreme Court's ruling in *Katz*, and the protection afforded by section 632 appears to be virtually coincident with the constitutional limits outlined in that case.[132] However, there are as yet no

125. An official of the San Francisco Telephone Company has estimated that 10,000 firms in Northern California alone monitor their executives' calls. Whitman, *Is Big Brother Taping You?*, TAPE RECORDING, Feb. 17, 1965, reprinted in *Hearings on Invasion of Privacy Before the Subcomm. on Administrative Practice of the Senate Comm. on the Judiciary*, 89th Cong., 1st Sess., pt. 1, at 17 (1965) [hereinafter cited as *1965 Hearings*]. *See also* CAL. SENATE JUDICIARY COMM., CAL. LEGISLATURE, 1957 REG. SESS., REPORT ON THE INTERCEPTION OF MESSAGES BY THE USE OF ELECTRONIC AND OTHER DEVICES 12 (1957) [hereinafter cited as REGAN COMM. REPORT]. For other examples of the use of electronic surveillance for internal security or employee monitoring purposes, see THE EAVESDROPPERS, *supra* note 4, at 269-72; THE INTRUDERS, *supra* note 4, at 206-08; PRIVACY AND FREEDOM, *supra* note 1, at 105-07.

126. The prior statutes applied to internal electronic eavesdropping, *see* ch. 1886, [1963] Cal. Stats. 3871 (former Penal Code section 653j), but internal wiretapping was not regulated. *See* statutes cited note 48 *supra*.

127. The Crime Control Act now places such activity under federal control as well. While its definition of "wire communication" does not include internal telephone systems, *see* 18 U.S.C. § 2510(1) (Supp. IV, 1965-68), all forms of internal surveillance apparently are covered by the ban on interception of oral communications. *See id.* § 2510(2).

128. CAL. PENAL CODE §§ 632, 636 (West Supp. 1968).

129. See note 59 *supra*.

130. CAL. PENAL CODE § 632(a) (West Supp. 1968): "Every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records such confidential communication, whether such communication is carried on among such parties in the presence of one another or by means of a telegraph, telephone or other device, except a radio, shall be punishable by fine . . . or by imprisonment . . . ."

131. *Id.* § 632(c).

132. See text at note 76 *supra*. While the statute refers only to eavesdropping by means of electronic devices, it might be noted that the rationale of *Katz* is equally

decisions construing this section, and it remains to be seen how expansively the courts interpret the definition of confidential communications.

Section 636 of the Penal Code prohibits eavesdropping on certain privileged communications of persons in legal custody.[133] Unlike section 632, this section is also applicable to law enforcement officers, but its protection is limited to persons in the custody or on the premises of law enforcement agencies.[134] This is in part mandated by the sixth amendment's right to counsel which is infringed when attorney-client conversations are subjected to electronic surveillance.[135] This provision could be eliminated if the general surveillance proscriptions were applied to law enforcement officers.

### 3. *Exceptions*

Sections 631 and 632 each contain subsections with identical exceptions to their general proscriptions.[136] The first exempts public utilities and their employees when conducting surveillance necessary for the operation and maintenance of their facilities.[137] The wisdom of such a carte blanche exemption might be questioned in light of the past excesses performed under the guise of so-called service checks.[138] At a very minimum a clause, such as the one found in the Crime Con-

---

applicable to aural snooping accomplished without electronic augmentation. The essence of *Katz* was that a person who conducts himself in such a way that he has an expectation of privacy is protected against the uninvited ear. If the conversing parties have a legitimate expectation of privacy, the uninvited ear intrudes just as much when it is pressed against the keyhole as when it is on the receiving end of a radio transmission. The same rationale could also be extended to cover visual surveillance. *Cf.* MICH. COMP. LAWS ANN. §§ 750.539a, b, d (1968).

133. CAL. PENAL CODE § 636 (West Supp. 1968): "Every person, who, without permission from all parties to the conversation, eavesdrops on or records by means of an electronic or other device, a conversation, or any portion thereof, between a person who is in the physical custody of a law enforcement officer or other public officer, or who is on the property of a law enforcement agency or other public agency, and such person's attorney, religious advisor, or licensed physician, is guilty of a felony . . . ."

The privileged communications protected in this statute differ from those given a privileged status by the Evidence Code. The evidentiary privileges also include a psychotherapist-patient privilege, CAL. EVID. CODE §§ 1010-26 (West 1966), but the physician-patient privilege is not available in criminal proceedings. *Id.* § 998.

134. *See* CAL. PENAL CODE §§ 632, 633, 636 (West Supp. 1968).

135. *See* Coplon v. United States, 191 F.2d 749 (D.C. Cir. 1951).

136. *Compare* CAL. PENAL CODE § 631(b) (West Supp. 1968), *with id.* § 632(e).

137. *Id.* §§ 631(b)(1), 632(e)(1).

138. Senator Edward V. Long of Missouri, chairman of the Senate subcommittee which conducted the *1965 Hearings*, *supra* note 125, reports that testimony before his committee established that A.T. & T. had greatly exceeded the bounds of monitoring for quality control purposes. In 1965 alone, 39 million calls were monitored. *See* THE INTRUDERS, *supra* note 4, at 18.

trol Act,[139] admonishing the utilities to restrict their monitoring to bona fide service checks should be inserted.

Also exempted is the use of "[E]quipment . . . furnished and used pursuant to the tariffs of . . . a public utility."[140] This clause permits the use of the various types of auxiliary recording and monitoring equipment available from utility companies. Common examples of such equipment are speakerphones, which broadcast conversations throughout a room, and recording couplers, devices by which tape recorders are connected to telephones. This equipment is exempted because compliance with the company tariff regulations[141] which govern its use will normally preclude any surreptitious monitoring. These regulations require the use of tone warning devices[142] on recording equipment and generally provide that other types of equipment not be used in such a way as to allow unauthorized persons to overhear conversations.[143] Such an exception requires a close policing of the tariff regulations to ensure that they accurately reflect the current law. At

139. 18 U.S.C. § 2511(2)(a) (Supp. IV, 1965-68): "It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication: *Provided*, That said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks."

140. CAL. PENAL CODE §§ 631(b)(2), 632(e)(2) (West Supp. 1968).

141. Tariffs are regulations promulgated by the utility company which have the force of law when filed with and accepted by the Public Utilities Commission. They contain rate schedules and rules governing the use and operation of equipment furnished by the utility. *See* CAL. PUB. UTIL. CODE § 489 (West 1956); Solomon v. Southern Cal. Tel. Co., 45 Cal. R.R.C. 775 (1945). Although they have the force of law, they are not backed by criminal sanctions; noncompliance results in removal of the equipment.

142. Both the California Public Utilities Commission and the Federal Communications Commission require that all equipment furnished by utilities for recording telephone conversations be equipped with an automatic warning device which will produce a distinctive tone at regular intervals during the course of the conversation. Use of Recording Devices in Connection with Telephone Service, 12 F.C.C. 1005, 1006-07 (1947); *In re* Beep Tones on Telephone Monitoring Equipment, 64 Cal. P.U.C. 526 (1965).

143. For example, the tariffs of the Pacific Telephone and Telegraph Company provide that customer-owned recording equipment can be connected with company facilities only through company-furnished recorder connector equipment which contains an automatic tone warning device. Tariffs of the Pacific Telephone and Telegraph Co., Schedule Cal. P.U.C. No. 135-T, Original Sheet 21 (Apr. 28, 1969). The tariffs governing loudspeaker sets and speakerphones require the subscriber to obtain the consent of the speaker to let others listen in. The equipment cannot be used to permit overhearing of messages by persons not entitled to hear them. *Id.* Schedule Cal. P.U.C. No. 32-T, 6th Rev. Sheet 25 (Apr. 28, 1969); *id.* 3d Rev. Sheet 38-A (Dec. 10, 1963).

present, the tariffs of the Pacific Telephone and Telegraph Company place no restrictions on the use of ordinary extension telephones.[144] Thus, under this exception one party seemingly can permit a third person to listen in on a conversation on an extension, a clear contradiction of the intent of section 631(a).[145]

Finally, neither statute applies to internal telephonic communications systems within correctional facilities.[146] This exception reflects the case law which existed at the time of the statute's enactment.[147] The California courts had previously held that there was "no right of privacy in a jail,"[148] and there was dictum in a United States Supreme Court opinion to the same effect.[149] However, inasmuch as the constitutionality of prison surveillance was predicated on the assumption that a jail was not a "constitutionally protected area,"[150] the abandonment in *Katz* of the constitutionally protected area concept[151] leaves the status of this type of surveillance in some doubt. It is at least arguable that a prisoner who seeks to preserve the confidentiality of his communications may have a reasonable expectation of privacy and

144. There is no tariff which regulates the use of extension telephones as such; nor does the tariff which sets forth the general rules of the company place any restrictions on the use of extensions for eavesdropping purposes. *See* Rule No. 15—Rules Under Which Service Will Be Rendered by the Company, Tariffs of the Pacific Telephone and Telegraph Co., Schedule Cal. P.U.C. No. 36-T, 3d Rev. Sheet 58 (April 28, 1969). *See also* Rule 2—Description of Service, *id.* 2d Rev. Sheet 18 (May 25, 1956); *id.* 5th Rev. Sheet 27 (Jan. 26, 1967).

145. See note 120 *supra* and accompanying text.

146. CAL. PENAL CODE §§ 631(b)(3), 632(e)(3) (West Supp. 1968): "This section shall not apply . . . (3); to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility."

147. *See, e.g.*, People v. Apodaca, 252 Cal. App. 2d 656, 60 Cal. Rptr. 782 (1967); People v. Morgan, 197 Cal. App. 2d 90, 16 Cal. Rptr. 838 (1961), *cert. denied*, 370 U.S. 965 (1962).

148. People v. Lopez, 60 Cal. 2d 223, 248, 384 P.2d 16, 30, 32 Cal. Rptr. 424, 438 (1963); *see* cases cited note 147 *supra*.

149. Lanza v. New York, 370 U.S. 139, 142-44 (1962). Justice Stewart, writing for a majority of four (Justices Frankfurter and White abstained) announced, in a totally superfluous dictum, that a jail was not a constitutionally protected area. *Id.* Chief Justice Warren and Justice Brennan, with the concurrence of Justice Douglas, added special memoranda decrying the insertion of this unnecessary dictum into the opinion. *Id.* at 147-53. Justice Brennan went on to say that "[o]f the abbreviated Court of seven who participate in the decision, fewer than five will even intimate views that the constitutional protections against invasion of privacy do not operate for the benefit of persons—whether inmates or visitors—inside a jail . . . ." *Id.* at 150. Thus *Lanza* does not provide the strong support claimed for the assertion in some California cases that it is well settled that there is no privacy in a jail or that there are no fourth amendment barriers to surveillance of inmates by prison authorities. *See* People v. Chandler 262 Cal. App. 2d 350, 355-56, 68 Cal. Rptr. 645, 648-49 (1968); People v. Miller, 252 Cal. App. 2d 877, 881 n.2, 60 Cal. Rptr. 791, 793 n.2 (1967).

150. *See* Lanza v. New York, 370 U.S. 139, 142-44 (1962).

151. See text at notes 75-76 *supra*.

hence be entitled to fourth amendment protection notwithstanding his location.[152] The fact that surveillance "has traditionally been the order of the day"[153] in prisons should not bear on the expectation of privacy; for that merely means that in the past the law has defeated the reasonable expectation which arises from an effort to guard against overhearing. Where there are alternate places or methods of communication available, it might make sense to say that a person should not expect privacy when he voluntarily converses in a place or through a medium known by him to be subject to surveillance. But in the controlled environment of a prison, the prisoner has nowhere to go to avoid the uninvited ear.[154] Moreover, denying the prisoner any right of privacy strips him of one of the major aspects of human dignity,[155] a result seemingly inconsistent with the rehabilitative goals of modern penology.

Even if prison inmates, by virtue of their conviction, do not enjoy all the constitutional rights of the unincarcerated[156] and can be subjected to otherwise unconstitutional surveillance, it is by no means clear that such surveillance can be imposed on their visitors.[157] This provision allows prison authorities to monitor the face-to-face intercom systems which are commonly found in prison visiting rooms.[158] Furthermore, the sweep of this exception is so broad that it would even countenance monitoring the conversations of prison guards or other employees who are communicating via an internal telephone system. That type of surveillance would clearly require judicial authorization to be constitutional.[159]

---

152. *See* Schwartz, *supra* note 82, at 84; Note, *From Private Places to Personal Privacy: A Post-Katz Study of Fourth Amendment Protection*, 43 N.Y.U.L. REV. 968, 984 n.92 (1968).

153. Lanza v. New York, 370 U.S. 139, 143 (1962).

154. This is particularly true in visiting rooms where the prisoner must use the facilities available or forego any contact with the outside world.

155. *See generally* Bloustein, *supra* note 14.

156. It is not clear to what extent those convicted of a crime can be stripped of their constitutional rights, but some infringement is allowed. *See, e.g.*, Price v. Johnston, 334 U.S. 266, 285 (1948) (right to be present at trial); Davis v. Superior Court, 175 Cal. App. 2d 8, 20, 345 P.2d 513, 521 (1959) (freedom of speech—limitations on correspondence).

157. Court-ordered wiretaps, if they can be authorized legally under *Berger* and *Katz*, see text accompanying notes 82-87 *supra*, will intercept the conversations of innocent parties as well as those of the person against whom the tap is directed. It does not necessarily follow, however, that when the authority for the wiretap derives not from a judicial order, but from the disability of one of the parties, the innocent party's end of the conversation can be monitored at will.

158. Most of the California cases have involved just such a practice. *See, e.g.*, cases cited note 147 *supra*. The exemption is limited to telephonic communications and it may well have been aimed at this very situation, since surveillance outside visiting rooms presumably would be done by electronic eavesdropping which is not exempted from the general proscriptions.

159. See text at notes 79-80 *supra*.

As it appears in the electronic eavesdropping statute this exception is not only constitutionally questionable, it is illogical. Because it is merely a repetition of the exclusion in the wiretapping statute,[160] it is limited to the interception of telephone conversations. Surely, if surveillance is to be permitted at all, there is no reason to differentiate between telephonic and other communications. It is anomalous to allow the interception of a conversation when a prisoner is conversing with his visitors through an intercom system but not when they are talking face to face.[161] This exception would best be deleted altogether. If retained, however, it should be drafted more narrowly to permit only that surveillance which is constitutional, and the disparity in treatment between oral and wire communications should be eliminated.

*4. Other Discrepancies*

The exception for correctional facilities is not the only anomaly in the statutory scheme. While section 631 forbids the use or divulgence of information procured by wiretapping, section 632 contains no similar provision for the products of electronic eavesdropping.[162] Thus one who obtains eavesdrop information secondhand can use it with impunity so long as the use itself is not illegal.[163] While situations where the user is not involved in the procurement may be relatively

160. *Compare* CAL. PENAL CODE § 632(e)(3) (West Supp. 1968), *with id.* § 631 (b)(3), quoted in note 146 *supra.*

161. Even if the prisoner might expect that telephone communications are less secure than face-to-face conversations, he has no alternative but to use the intercom system.

162. *Compare* CAL. PENAL CODE § 631(a) (West Supp. 1968) ("Any person . . . who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained . . . is punishable by a fine . . . or by imprisonment . . . ."), *with id.* § 632(a) (no reference to use). Section 637 also deals with the disclosure of telegraphic or telephonic communications: "Every person not a party to a telegraphic or telephonic communication who willfully discloses the contents of a telegraphic or telephonic message, or any part thereof, addressed to another person, without the permission of such person, unless directed so to do by the lawful order of a court, is punishable by imprisonment . . . or by fine . . . ." *Id.* § 637.

In People v. Earl, 19 Cal. App. 69, 124 P. 887 (1912), section 619 of the Penal Code, ch. DXXVIII, § 1, [1905] Cal. Stats. 689 (the predecessor of section 637), was interpreted to apply only to those engaged in the dispatch, transmission, or delivery of telegraphic messages. The interpretation was required because a literal construction of the statute as it then read would have rendered the sender of a message liable to felony sanctions if he disclosed the contents of his own message to another person. 19 Cal. App. at 73, 124 P. at 888. Section 637 retained the basic provisions of section 619, but the Legislature responded to the criticism in *Earl* by limiting the application of the section to persons not parties to the communication. It would appear, however, that the prohibition is still aimed at those entrusted with the handling of communications—the employees of the carrier.

163. Aside from the surveillance laws, the use of the information for improper purposes may subject the user to criminal or tort liability. An example would be blackmail.

rare, the problem is not unimportant. When it does arise, the victim is deprived of his only effective remedy—recourse against the user.[164] To remedy this defect and make the law uniform a single code provision should prohibit the use or divulgence of any communication known to have been obtained in violation of any of the surveillance statutes.[165]

Section 631 also applies to solicitations, attempts, and conspiracies to engage in wiretapping activities, while section 632 makes no mention of inchoate violations of the electronic eavesdropping laws.[166] The inclusion of attempts and conspiracies in either section is unnecessary; California has specific statutes to cover those offenses.[167] Solicitations might merit separate treatment, however.[168] There is no separate statute to sanction those who attempt to employ snoopers,[169] and private surveillance usually involves a solicitation; matrimonial and industrial espionage—two of the most prevalent uses of surveillance—are seldom performed directly by the party seeking the information. Thus it might be desirable to create some criminal liability for solicitations in order to lessen the potential market for the eavesdropper's skills. In any event, the wiretapping and eavesdropping statutes should be standardized.

---

164. The problem would probably arise most often in an industrial espionage context where an enterprising snooper might have a ready market for information about competitors. For example, *X*, by means of an illegal electronic eavesdrop, procures confidential information belonging to corporation *Y* which would be of value to its competitors. He later sells this information to *Y*'s competitor *Z*. *Z*, even though he may know of the illegal origin of the information, is free to use it to his advantage so long as he does not contravene any other law or tort principle in so doing. Section 632 does not prohibit such use and he is not an accessory if he was not involved in the procurement. Although *Y* may be able to proceed against *X* in either a criminal prosecution or an action for damages, chances are *X* will be judgment proof. Meanwhile *Y* is deprived of any remedy against *Z*, including, most importantly, injunctive relief to prevent further use. None of the remedies of the Privacy Act, see Part V, section C *infra*, are available because the surveillance laws have not been violated.

165. Such a provision should include a requirement that the user have knowledge of the illicit source of the information. Section 631 does not have scienter requirement, but the courts would probably read in a requirement of knowledge on general criminal law principles. *See* CAL. PENAL CODE § 20 (West 1957); 1 B. WITKIN, CALIFORNIA CRIMES § 52 (1963).

166. *Compare* CAL. PENAL CODE § 631(a) (West Supp. 1968) ("Any person . . . who . . . aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine . . . or by imprisonment . . . ."), *with id.* § 632 (no reference).

167. *Id.* § 664 (attempts); *id.* § 182 (conspiracies).

168. *Cf.* MICH. COMP. LAWS ANN. § 750.539c (1968).

169. California has a solicitation statute, but it applies only to specific offenses. Violations of the surveillance laws are not included. CAL. PENAL CODE § 653f (West 1957).

### B. The Federal Law

The Crime Control Act, although cast in different terms, prohibits most of the same activities as does the California Privacy Act, but it applies to all persons, law enforcement personnel included. The federal law does not classify on the basis of the type of surveillance (wiretapping or eavesdropping) but rather on the type of communication (wire or oral), and prohibits all interception of those communications.[170] The ban on the interception of wire communications in effect outlaws the same forms of wiretapping as does section 631,[171] and the "oral" communications protected in the federal statute are substantially the same as the "confidential" communications of section 632.[172] The federal law, however, provides that interceptions can be legitimized by the consent of one party unless they are attempted for illicit purposes.[173] This creates the only major conflict between the two statutes. Since California requires the consent of all parties to legally intercept a communication,[174] a federal investigative officer acting within the scope of the federal law in monitoring a conversation with the consent of one of the parties would theoretically be liable to prosecution under the California Penal Code.[175] However, it is questionable whether California could constitutionally prosecute a federal agent for such activities.[176] The liability of federal officers not acting under warrant for violations of state law is unclear,[177] but even if they were subject to prosecution,

170. *See* 18 U.S.C. §§ 2510-11 (Supp. IV, 1965-68).

171. Both statutes prohibit the interception of telephonic communications by any method. *Compare* 18 U.S.C. §§ 2510-11 (Supp. IV, 1965-68), *with* CAL. PENAL CODE § 631 (West Supp. 1968).

172. *Compare* CAL. PENAL CODE § 632(c) (West Supp. 1968) (quoted in text at note 131 *supra*), *with* 18 U.S.C. § 2510(2) (Supp. IV, 1965-68) ("'[O]ral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation . . . .").

173. *See* 18 U.S.C. §§ 2511(2)(c)-(d) (Supp. IV, 1965-68).

174. See note 57 *supra* and accompanying text.

175. CAL. PENAL CODE § 633 (West Supp. 1968) exempts most state law enforcement officials from the operation of sections 631 and 632 and hence from the all-party-consent rule. However, there is no such exemption for federal officers.

176. *See Hearings on Wiretapping, Eavesdropping, and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 85th Cong., 2d Sess., pt. 1, at 204 (1958) [hereinafter cited as *1958 Hearings*] (testimony of Prof. Alan Westin).

177. An officer acting under specific authorization apparently is immune from state suit and can be freed from state custody by writ of habeas corpus under 28 U.S.C. § 2241 (1964). *See In re* Neagle, 135 U.S. 1 (1889). And an officer who violates a state law in the line of duty can have the state prosecution removed to a federal district court under 28 U.S.C. § 1442 (1964). However, the question of liability for acts not performed under specific authorization has never been authoritatively determined. *Compare In re* Neagle, *supra*, *with* Colorado v. Symes, 286 U.S. 510, 517-18 (1932). It would seem that in the instant situation, even though the federal statute does not

such action would be highly unlikely for obvious political and practical reasons.

The federal scheme seems clearly superior to California's cumbersome and poorly organized system as a structural model for state surveillance laws. A statute patterned on the federal law would first define the types of communication to be protected and then prohibit their interception by any means. After laying down a comprehensive proscription on surveillance, the statute could enumerate any desired exceptions such as an exemption for utility service checks or a warrant system for police surveillance. This approach disregards unnecessary distinctions between wiretapping and electronic eavesdropping and errs on the side of privacy if oversights should occur.

## III

## ELECTRONIC SURVEILLANCE FOR LAW ENFORCEMENT PURPOSES

### *A. California Law Today*

After laying down blanket prohibitions on virtually all wiretapping and eavesdropping in sections 631 and 632, the California Penal Code proceeds to carve out a very large exception for the police. Section 633 allows certain enumerated law enforcement officers to overhear or record "any communication which they could lawfully overhear or record prior to the effective date of this chapter."[178] Although originally intended to perpetuate California's then permissive rules on police surveillance,[179] section 633's exception was severely limited by *Berger* and *Katz*.[180] Those decisions restricted nonconsensual police surveillance

specifically authorize one-party-consent monitoring, it evidences a congressional intent to permit federal officers to use this technique in the performance of their duties, and they would be immune.

178. CAL. PENAL CODE § 633 (West Supp. 1968). The list of exempted officers is quite comprehensive. It includes "the Attorney General, any district attorney, or any assistant, deputy, or investigator of the Attorney General or any district attorney, or any officer of the California Highway Patrol, or any chief of police, assistant chief of police, or policeman of a city or city and county, or any sheriff, undersheriff, or deputy sheriff regularly employed and paid as such of a county, or any person acting pnrsuant to the direction of one of the above-named law enforcement officers acting within the scope of his authority." *Id.* There are, however, a few types of state investigative officers, such as agents of the Alcoholic Beverage Control Board, who do not come under section 633, and it does not apply to any federal officials.

179. *Id.* § 630: "[I]t is not the intent of the Legislature to place greater restraints on the use of listening devices and techniques by law enforcement agencies than existed prior to the effective date of this chapter." See text at notes 45-46 *supra* for the pre-existing rules.

180. Since *Berger* was decided prior to passage of the Privacy Act, its requirements were embodied in the statute when it took effect.

to that performed with prior judicial authorization.[181] Even the possibility of court-ordered surveillance was short-lived, however, for the Crime Control Act has indirectly outlawed all nonconsensual police surveillance in California. The federal Act not only requires a warrant, but also requires a state enabling statute before such electronic search warrants can be issued.[182] Since California as yet has no enabling statute, even court-ordered nonconsensual surveillance is at present a violation of federal law.

In the area of consensual surveillance, however, section 633 is significant, for it exempts law enforcement officers from the all-party-consent requirement of sections 631 and 632. "Prior to the effective date of"[183] section 633, California permitted all forms of electronic surveillance performed by, or with the consent of, one of the communicating parties.[184] Section 633 has, for the time being at least, perpetuated that policy for the police.[185] *Berger* and *Katz* cast some doubt on the constitutionality of such practices,[186] but until there is a clear mandate from the Supreme Court that judicial approval is required it is doubtful that California's policy will change. Since the Crime Control Act also requires the consent of only one party,[187] the police are free to employ all types of participant monitoring under both state and federal law.

### B. *Prospects for the Future*

Debate on the general question of whether police surveillance

181. See text at note 79.

182. *See* 18 U.S.C. § 2516(2) (Supp. IV, 1965-68); SENATE REPORT, *supra* note 95, at 98.

183. CAL. PENAL CODE § 633 (West Supp. 1968).

184. See note 57 *supra.*

185. It is interesting to note that while the Privacy Act perpetuated the single-party-consent rule for the police, it undermined the rationale on which that rule had been based. The rule had its origin in People v. Malotte, 46 Cal. 2d 59, 292 P.2d 517 (1956), where the California supreme court held that there was no unauthorized learning of the contents of a telephone conversation within the meaning of Penal Code section 640 (the precedessor to section 631) when one party consented to the acquisition. 46 Cal. 2d at 64, 292 P.2d at 520. Since section 631 now explicitly requires the consent of all parties to authorize the learning of the contents of a message, see note 114 *supra*, that premise is no longer valid. Even though the rationale of *Malotte* has been vitiated, however, section 633 validates the practices to which it gave birth. *See* Degnan, *supra* note 122, at 264.

186. Although there are intimations in *Berger* and *Katz* that court orders might be required for consensual surveillance, see text at notes 88-92 *supra*, the states are free to pursue their own policies until a more definitive rule is laid down by the Supreme Court.

187. 18 U.S.C. § 2511(2)(c) (Supp. IV, 1965-68): "It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."

should be permitted at all has raged for 40 years.[188] Its partisans claim that it is an indispensable law enforcement tool, especially in combatting organized crime; that the attendant invasions of privacy are the price that must be paid for effective law enforcement; and that judicial supervision will eliminate most abuses.[189] Opponents, on the other hand, charge that it is a "dirty business"[190] which intrudes intolerably on personal privacy; that its effectiveness is questionable at best; and that warrant systems are notoriously unsuccessful in controlling police misconduct.[191] There is substance to each of these arguments, but the opposing factions tend to exaggerate both the value and the dangers of electronic surveillance. If subjected to stringent controls, police surveillance is probably neither the calamity which its critics prophesy nor the boon which its proponents anticipate.

In the first place, electronic surveillance has inherent characteristics which curtail its effectiveness as an investigative device as well as lessen the incentive for abuse. Electronic surveillance is normally a time-consuming investigative technique—especially when it involves procuring a warrant—and it is not feasible to use for a large number of minor offenses.[192] The expenditure of time and effort required is not justified by the seriousness of the offense. Furthermore, the number of crimes which are susceptible of solution by electronic surveillance is limited. Crimes of passion or violence and crimes characteristically involving a single person do not normally yield to surveillance techniques.[193]

It is clear that innocent conversations will be intercepted and the privacy of innocent parties violated even under the most discriminating controls. If electronic surveillance is as effective a tool as its proponents claim,[194] however, a limited number of such intrusions might not be

188. Since the Supreme Court first dealt with the question in Olmstead v. United States, 277 U.S. 438 (1928), the outpouring of commentary on the subject has been voluminous. *See, e.g.*, bibliography cited note 5 *supra*; bibliography in *1958 Hearings*, *supra* note 176, at 187-91.

189. *See* J. LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT 220-27 (1966). *See also* ABA STANDARDS, *supra* note 5, at 96-97; Parker, *Surveillance by Wiretap or Dictograph: Threat or Protection?*, 42 CALIF. L. REV. 727 (1954); Rogers, *supra* note 38; Scott, *Wiretapping and Organized Crime*, 14 HOWARD L.J. 1 (1968).

190. Olmstead v. United States, 277 U.S. 438, 470 (1928) (Holmes, J., dissenting).

191. *See* J. LANDYNSKI, *supra* note 189, at 220-27. *See also* W. DOUGLAS, THE RIGHT OF THE PEOPLE (1958); Solomon, *Wiretapping & Bugging—A Counter Proposal*, 40 N.Y.S.B.J. 94 (1968). Two of the more eloquent judicial attacks on electronic surveillance will be found in the dissenting opinions of Justice Brandeis in Olmstead v. United States, 277 U.S. 438, 471-85 (1928), and Justice Frankfurter in On Lee v. United States, 343 U.S. 747, 758-62 (1952).

192. *See* ABA STANDARDS, *supra* note 5, at 45-46.

193. *See* Brown & Peer, *The Wiretapping Entanglement: How to Strengthen Law Enforcement and Preserve Privacy*, 44 CORNELL L.Q. 175, 183-84 (1959).

194. New York County District Attorney Frank Hogan has claimed that wire-

too high a price to pay. A point may be reached where the invasions of privacy perpetrated by criminal activity outweigh those occasioned by limited police surveillance.[195] Furthermore, a properly designed warrant system, while not eliminating abuses, should keep them to a minimum. Although there have been serious abuses of police surveillance under previous court order systems, they can in large part be attributed to a lack of adequate controls or to a poorly designed system.[196]

On the other hand, there is surprisingly little data on the effectiveness of electronic surveillance; most of the current information consists of conclusory statements by law enforcement officials.[197] There is little to support proponents' claims that it is indispensable,[198] although there

---

tapping "is the single most valuable weapon in law enforcement's fight against organized crime." *Hearings on S. 2813 and S. 1495 Before the Senate Comm. on the Judiciary*, 87th Cong., 2d Sess. 173 (1962).

195. *Cf.* ABA STANDARDS, *supra* note 5, at 96-97.

196. Most of the available information comes from New York which has had a court order system since 1942. In the 1940's and early 1950's the New York system was consistently and flagrantly abused, particularly by the police. Much surveillance was performed without a court order, and there were many instances of police officers using surveillance for personal gain. *See generally* THE EAVESDROPPERS, *supra* note 4, at 37-119. However, the New York scheme contained neither an exclusionary rule nor criminal penalties for extra-legal police surveillance. *See* ch. 924 [1942] N.Y. Laws 2030, *as amended* ch. 879, § 1, [1957] N.Y. Laws 1915 (repealed 1968). Furthermore, the statute allowed any police officer above the rank of sergeant to obtain surveillance orders. *Id.* In 1951, as a result of a grand jury investigation, administrative procedures within the New York City Police Department were tightened up, *see* THE EAVESDROPPERS, *supra* note 4, at 62-63, and in 1957, illegal police surveillance was made a crime. *See* ch. 879, § 2, [1957] N.Y. Laws 1916 (repealed 1968). Even these rather mild improvements apparently were effective in curtailing abuse. *See* PRESIDENT'S COMM'N ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 202 (1967).

197. *E.g.*, "All the district attorneys of New York State, and all district attorneys that I have come in contact with in the national association, feel most strongly that wiretapping is absolutely necessary if they are to cope with the modern criminal," Silver, *Legalized Wiretapping Necessary to Combat Streamlined Efficiency of Organized Crime*, HARV. L. RECORD, Feb. 27, 1958, reprinted in *Hearings on Wiretapping, Eavesdropping, and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 86th Cong., 1st Sess., pt. 3, at 544, 547 (1959) [hereinafter cited as *1959 Hearings*]; "[w]iretapping—whether by private individuals or public officials—should be generally prohibited. The needs of law enforcement can be met without reliance on such large-scale intrusions on personal privacy," *Hearings on S. 675 Before the Subcomm. on Criminal Law and Procedures of the Senate Comm. on the Judiciary*, 90th Cong., 1st Sess., at 358 (1967) (statement of former Attorney General Ramsey Clark) [hereinafter cited as *1967 Senate Hearings*]. *See* Hennings, *The Wiretapping-Eavesdropping Problem: A Legislator's View*, 44 MINN. L. REV. 813, 829, 833-34 (1960). Senator Hennings was chairman of the Senate subcommittee which conducted the 1958 and 1959 hearings cited *supra* and note 176 *supra*.

198. The most comprehensive argument for the need for legalized police surveillance is found in the ABA STANDARDS, *supra* note 5, at 48-97, but even the ABA committee admitted that there is little empirical evidence to support its position. *Id.* at 50-52.

is no doubt that it is useful in certain situations.[199] The Crime Control Act contains detailed reporting procedures which should, in time, generate data on which to evaluate objectively the effectiveness of electronic surveillance.[200] Until such time as it is proven vital, however, it would seem that a heavy burden of justification should fall on those who advocate the use of such a potentially dangerous investigative tool.[201]

The foregoing summary has attempted to point out some of the major arguments for and against the legalization of law enforcement surveillance, but it is not the purpose of this Comment to become embroiled in that controversy. Reams have been written on the subject, and it seems a futile exercise to reiterate arguments which have not changed substantially in 40 years. Congress has resolved the question in favor of allowing law enforcement surveillance under a court order system,[202] and, unless title III is held unconstitutional, it appears that police surveillance is here to stay. Furthermore, it seems likely that many states, possibly including California,[203] will follow the congressional lead and establish warrant systems of their own.[204] For that reason, this Comment will accept the existence of law enforcement surveillance and concentrate on the problem of controlling it. The remainder of Part III will be devoted to a discussion of restrictions which can be placed on police surveillance, when it is permitted, to prevent abuses and minimize invasions of privacy. Title III of the Crime Control Act will serve as the focal point of the discussion because, in addition to being the most logical model for state schemes, it imposes a number of mandatory requirements on the states. However, title III should not be considered the final word. In some areas it is so

199. *See id.* at 52-70. Even law enforcement officials who feel that electronic surveillance should be outlawed admit that it is effective. *See, e.g., 1958 Hearings, supra* note 176, pt. 1, at 25 (statement of Attorney General Thomas McBride of Pennsylvania).

200. *See* 18 U.S.C. § 2519 (Supp. IV, 1965-68).

201. Much of the following discussion is premised on the thesis that where a practice is so potentially destructive of civil liberties it should be employed only when its benefits clearly outweigh the dangers it poses.

202. See text at notes 99-102 *supra.*

203. Bills to set up a court order system have been introduced at the last two sessions of the California Legislature. A.B. 253, 1969 Sess. California Legislature (modeled on the federal statute); S.B. 1090, 1968 Sess. California Legislature; A.B. 598, 1968 Sess. California Legislature.

204. Minnesota and New Jersey have already enacted court order schemes closely patterned on the federal Act. Ch. 953, [1969] Minn. Laws 1856; N.J. STAT. ANN. §§ 2A:156A-1 to -26 (Supp. 1969). In addition several other states have either established or revised their court order systems since the *Katz* decision. *See* ARIZ. REV. STAT. ANN. §§ 13-1051 to -1059 (Supp. 1968); MASS. GEN. LAWS ANN. ch. 272, § 99 (Supp. 1968); N.Y. CODE CRIM. PROC. §§ 814-25 (McKinney Supp. 1969).

permissive as to be constitutionally suspect,[205] and it permits practices whose utility is far outweighed by their potential for abuse. There is considerable room for improvement in the federal scheme both with respect to the rules governing the interception of communications and those dealing with the use of legally intercepted communications.

### *1. Control of Interception*

#### *a. General Limitations Imposed by the Crime Control Act*

The Crime Control Act places certain general restrictions on the use of electronic surveillance by state law enforcement officials.[206] The first limits the use of electronic surveillance to the investigation of specified crimes:[207] purportedly those offenses which are characteristic of organized crime or which are violent in nature.[208] However, the list is drawn very broadly; it includes any "crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year."[209] Since "property" is to be liberally construed,[210] this leaves the states free to include a very broad range of offenses.[211]

State enabling legislation should carefully limit the offenses for which surveillance may be used to those deemed serious enough to warrant the attendant invasions of privacy.[212] The legislature should evaluate each offense in terms of its seriousness and its susceptibility to solution by surveillance techniques in determining whether it should

205. See notes 103-04 *supra* and accompanying text.

206. 18 U.S.C. § 2516(2) (Supp. IV, 1965-68): "The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire or oral communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire or oral communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses."

207. *Id.*

208. *See* SENATE REPORT, *supra* note 95, at 97-99.

209. 18 U.S.C. § 2516(2) (Supp. IV, 1965-68).

210. SENATE REPORT, *supra* note 95, at 99.

211. *See* Schwartz, *supra* note 97, at 481-82.

212. Under New York's court order system, the preponderance of wiretapping in New York City was performed for minor gambling offenses. *See* PRIVACY AND FREEDOM, *supra* note 1, at 128. *See also* Note, *Wiretapping—Analysis of the Law and Practice Under New York Constitutional and Statutory Provisions*, 31 N.Y.U.L. REV. 197, 213 (1956) (80 percent of wiretap applications received by one court were for bookmaking).

be included. Political offenses and crimes which may involve first amendment freedoms should be excluded.[213] Furthermore, the statute should specifically enumerate the offenses rather than employing a catchall phrase which can be construed too broadly. Such precautions will minimize the opportunities for engaging in fishing expeditions and will ensure that electronic surveillance is used only where the legislature has made a concrete determination that it is warranted.

Additional limitations in the Crime Control Act centralize the administration of the warrant system. The authority to apply for court orders is given only to the state attorney general and to district attorneys,[214] and surveillance orders can be issued only by judges of courts of general criminal jurisdiction.[215] These requirements might prove to be among the most effective checks on police abuse. Previous court order systems for electronic surveillance—as well as search warrant practice in general—have frequently been assailed by critics for not working in practice.[216] In New York, surveillance at the police department level was at one time rife with abuse,[217] and magistrates too often issued orders as a matter of course.[218] District attorneys, however, appear to have been more circumspect in their use of electronic surveillance.[219] By centralizing the policymaking power in the chief prosecuting officer of the county and limiting the authority to issue warrants to higher levels of the judiciary, these provisions hopefully will avoid some of the past abuses.

In addition, state enabling legislation should contain provisions explicitly restricting the actual performance of surveillance work to full-

213. *See* PRIVACY AND FREEDOM, *supra* note 1, at 394. The dangers of abuse in these areas are too great, and the chilling effect of even limited governmental surveillance of such activities would be intolerable. See text at notes 19-20 *supra.*

214. *See* 18 U.S.C. § 2516(2) (Supp. IV, 1965-68), quoted in note 206 *supra*; SENATE REPORT, *supra* note 95, at 98.

215. *See* 18 U.S.C. §§ 2510(9), 2516(2) (Supp. IV, 1965-68). In California this would limit issuance to superior court judges.

216. *See, e.g.*, AMERICAN CIVIL LIBERTIES UNION, THE WIRETAPPING PROBLEM TODAY, *reprinted in Hearings on H.R. 5037, H.R. 5038, H.R. 5384, H.R. 5385, & H.R. 5386 Before Subcomm. No. 5 of the House Comm. on the Judiciary*, 90th Cong., 1st Sess., ser. 3, at 976, 978-80 (1967) [hereinafter cited as *1967 House Hearings*]; Schwartz, *supra* note 97, at 477-80.

217. See note 196 *supra. See generally* THE EAVESDROPPERS, *supra* note 4, at 35-119. It was estimated that plainclothesmen in New York city were making from 13,000 to 26,000 wiretaps in a year when police records indicated that only 338 wiretap orders had been obtained. *Id.* at 68. *See also* PRIVACY AND FREEDOM, *supra* note 1, at 127-28.

218. *See* THE EAVESDROPPERS, *supra* note 4, at 45. During the House hearings on the Crime Control Act, committee chairman Celler reported that one New York judge would sign blank wiretap orders, leaving the actual authorization to his clerk. *1967 House Hearings, supra* note 216, at 407.

219. *See 1958 Hearings, supra* note 176, pt. 2, at 207 (testimony of Prof. Alan Westin).

time law enforcement officers.[220] Although title III indicates that authorized surveillance is to be performed by "investigative or law enforcement officers having responsibility for the investigation of the offense,"[221] this limitation, when read in conjunction with California law, would still permit the use of deputized civilian technicans to perform the actual work.[222] The utilization of civilians to perform law enforcement surveillance is undesirable. It creates a market for their skills, thereby encouraging the proliferation of professional snoopers who are available for extra-legal spying as well as legitimate police work. In addition, the district attorney or other prosecuting officials might tend to be less zealous in the investigation and prosecution of the illicit activities of those who are in their employ.[223] As a matter of administrative procedure each district attorney should have a small, carefully selected group of investigators under his control to perform all of the electronic surveillance in his jurisdiction. This centralization of operation would further tend to inhibit abuse[224] and would enable the district attorney to exert stricter control over the use of intercepted communications.[225]

*b. Warrant Requirements*

The heart of the federal scheme is the section which sets out the detailed procedures and criteria to be followed in the issuance and

220. The need for precise standards governing the authority to perform electronic surveillance is pointed up by the experience under a previous section of the California Penal Code which permitted the installation of dictographs by "regularly salaried peace officers." *See* ch. 525, [1941] Cal. Stats. 1833 (repealed 1967). This definition of authority appears sufficiently precise, but, in practice, the statute was frequently circumvented by delegating the installation to private parties under various deputizing practices and other subterfuges. *See* REGAN COMM. REPORT, *supra* note 125, at 18.

221. 18 U.S.C. § 2516(2) (Supp. IV, 1965-68).

222. An "investigative or law enforcement officer" is defined in title III as "[A]ny officer of . . . a State or political subdivision thereof, who is empowered by law to conduct investigations of or make arrests for offenses enumerated in this chapter . . . ." 18 U.S.C. § 2510(7) (Supp. IV, 1965-68). Under California law, officers authorized to make arrests for such offenses are called peace officers and can include "any qualified person, when deputized or appointed by the proper authority as a reserve or auxiliary sheriff or city policeman while performing police functions assigned to him by the appointing authority." CAL. PENAL CODE § 817 (West Supp. 1968).

223. In his study for the Pennsylvania Bar Association which culminated in the publication of *The Eavesdroppers*, Samuel Dash found that some police departments in California had granted an informal immunity to private investigators who performed surveillance work for them. THE EAVESDROPPERS, *supra* note 4, at 164.

224. While a warrant requirement can never stop a policeman from snooping for private gain, taking him out of the surveillance business should remove some of the temptation for extra-legal spying and particularly for misusing the fruits of lawful surveillance.

225. See text at notes 277-78 *infra*.

execution of surveillance orders.[226] These procedures were designed to

226. 18 U.S.C. § 2518 (Supp. IV, 1965-68):

(1) Each application for an order authorizing or approving the interception of a wire or oral communication shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigations is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire or oral communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire or oral communications within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) there is probable cause for belief that the facilities from which, or the place where, the wire or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire or oral communication shall specify—

meet the requirements of *Katz* and *Berger*.[227] For the most part they seem to represent a bona fide attempt to do so,[228] at least insofar as that is possible when authorizing nonselective surveillance.[229] However, they do contain some objectionable features which should be avoided in state legislation.

First, the Act fails to provide for a return on the warrant. While it requires any recording to be promptly turned over to the judge issuing the order,[230] it is not clear that this would meet the requirement of a return laid down in *Berger*.[231] To ensure compliance with the

---

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communications sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

(5) No order entered under this section may authorize or approve the interception of any wire or oral communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Extensions of au order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be exccuted as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

. . .

227. *See* SENATE REPORT, *supra* note 95, at 97.

228. The author of the *Berger* opinion apparently feels that, with the possible exception of the time limit, see text at notes 233-35 *infra*, and the emergency authorization, see text at notes 237-38 *infra*, the system meets the requirements of *Berger* and *Katz*. *See* Clark, *supra* note 103, at 5.

229. See text at notes 82-86 *supra*.

230. 18 U.S.C. § 2518(8)(a) (Supp. IV, 1965-68). Although section 2518 recommends that all conversations be recorded, recording is not an absolute requirement. Where no recording has been made section 2518 requires no return of any kind. *Id.*

231. The *Berger* Court criticized the New York statute because it failed to "provide for a return on the warrant thereby leaving full discretion in the officer as to the use of

*Berger* standard, explicit provision should be made for a return on the warrant, including all recordings, notes and records pertaining to the execution of the order.[232] A full and complete return will enable the issuing judge to determine whether the conditions of the surveillance order have been complied with.

The maximum duration of surveillance orders should be shorter than that allowed by the federal statute. The 30-day limit (with opportunity for additional 30-day extensions) authorized by the Crime Control Act[233] approaches the 60-day period decried by the Court in *Berger*.[234] Although the federal scheme calls for termination upon the acquisition of the desired communications, where the objective is not a single conversation the surveillance can continue until the time limit expires in hope of obtaining further evidence.[235] It is difficult to say just what constitutes an appropriate time limit, but something in the order of ten days seems reasonable. This would allow a certain amount of flexibility, while greatly increasing the demand for particularity and probable cause. The more clearly the desired conversations can be temporally delimited the higher the degree of particularity and the less the opportunity for engaging in fishing expeditions.[236]

The Crime Control Act also permits emergency surveillance without a warrant under certain circumstances, provided authorization is subsequently obtained.[237] Even if such a provision is constitutional—

---

seized conversations of innocent as well as guilty parties." 388 U.S. at 60. Similarly, in *Katz*, the absence of a warrant was scored because, *inter alia*, the officers were not required, "after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized." 389 U.S. at 356.

232. The new Minnesota statute, for example, requires that the return include a description of each surveillance installation and a designation of any telephone or telegraph lines involved in the interception. The return must also include the dates the surveillance took place and an identification of the parties whose conversations were intercepted. Ch. 953, § 7, [1969] Minn. Laws 1866.

233. 18 U.S.C. § 2518(5) (Supp. IV, 1965-68), quoted in note 226 *supra*.

234. 388 U.S. at 59. *See, e.g.*, Clark, *supra* note 103, at 5.

235. *See* Schwartz, *supra* note 97, at 462-63.

236. A legislature might well decide that an even shorter time limit is desirable in order further to increase particularity. The time limit could be reduced to the point where only known, preplanned calls or conversations could be monitored. This would maximize particularity, but would, of course, greatly impair the usefulness of surveillance as an investigative tool. Within constitutional limits the legislature will have to strike an appropriate balance between particularity and utility.

237. 18 U.S.C. § 2518(7) (Supp. IV, 1965-68):

> Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—
>
> (a) an emergency situation exists with respect to conspiratorial activities threatening the national security interest or to conspiratorial activities characteristic of organized crime that requires a wire or oral communication to be intercepted before an order authorizing such inter-

and its constitutionality has been challenged by a number of commentators[238]—it is inadvisable. It creates a virtual license to engage in exploratory searches.[239] If no evidence is uncovered, nothing has been lost. However, if the surveillance is productive, subsequent ratification, with the advantages of post facto determination of probable cause,[240] can legitimize the entire operation. The necessity for such emergency surveillance does not seem to counterbalance this potential for abuse. The installation of surveillance equipment is a time consuming process, normally allowing ample time for the procurement of a warrant.[241] Situations where the need for surveillance arises and the equipment can be put into operation before a judge can be found will be rare.[242] This limited usefulness is far outweighed by the danger of abuse.

---

ception can with due diligence be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire or oral communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire or oral communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

Another curious provision of the federal law exempts law enforcement officers from all controls when eavesdropping on equipment furnished by a communications common carrier. *Id.* § 2510(5). The possibilities for abuse are self-evident and there is no discernible reason for exempting the police from even the requirement of single-party consent when using such equipment.

238. *See* authorities cited note 103 *supra.*

239. Samuel Dash found that under New York's former court order system, police would often tap telephones to sample the conversations before attempting to get an order. THE EAVESDROPPERS, *supra* note 4, at 66.

240. *Cf.* Beck v. Ohio, 379 U.S. 89, 96 (1964).

241. *See* ABA STANDARDS, *supra* note 5, at 45-48. A leading proponent of law enforcement surveillance, former King's County, New York District Attorney Edward Silver, has testified that the need for surveillance orders does not ordinarily arise quickly, and that law enforcement agencies in New York had ample time to get warrants if grounds for issuance existed. *Hearings on Wiretapping Before Subcomm. No. 5 of the House Comm. on the Judiciary*, 84th Cong., 1st Sess. 98 (1955). In THE INTRUDERS, *supra* note 4, at 113, Senator Long quotes a statement by former government wiretapper William Mellin in which he expressed a belief that in none of the over 60,000 wiretaps he had performed would a requirement to obtain a court order have hampered him, providing a warrant could have been obtained within 48 hours.

242. *Cf.* Katz v. United States, 389 U.S. 347, 358 n.21 (1967): "Although '[t]he Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others,' [citation omitted] there seems little likelihood that electronic surveillance would be a realistic possibility in a situation so fraught with urgency." See also note 241 *supra.*

*c. Other Controls*

Two additional controls proposed by the Advisory Committee on the Police Function of the American Bar Association merit attention because they will probably be considered by any legislative body working in the field.[243] They concern the interception of privileged communications and the surveillance of public telephone facilities. Although it would appear desirable to prohibit the interception of privileged communications, there seems to be no practical way of doing so.[244] The ABA solution is to require an additional showing when surveillance is to take place on premises or facilities normally utilized for the exchange of privileged communications. The showing consists of establishing probable cause to believe that there is a special need for the overhearing of the communications and that the surveillance will be performed in such a manner as to minimize the interception of privileged communications.[245] As Professor Herman Schwartz has pointed

243. The ABA STANDARDS, *supra* note 5, in which these proposals are found includes comprehensive findings and recommendations on all aspects of electronic surveillance law and will no doubt have a significant influence on legislatures considering new surveillance laws. These proposals are incorporated in the new New Jersey court order system. N.J. STAT. ANN. § 2A:156A-11 (Supp. 1969).

244. The basic rationale behind the concept of privileged communications demands that they not be used in criminal investigations at all. See discussion of this point in text at notes 271-76 *infra*. Moreover, where the privileged communications are between a defendant and his attorney, the sixth amendment demands that they be free from electronic surveillance. *See* Coplon v. United States, 191 F.2d 749 (D.C. Cir. 1951) (interception of conversations betwcen defendant and counsel before and during trial violates fifth and sixth amendments and constitutes reversible error whether or not any evidence derived therefrom is presented at trial). Obviously, the surest way to avoid the use of privileged communications would be to prohibit their interception, and certainly no warrants should issue to intercept known privileged communications. However, it is virtually impossible in most instances to predict in advance when communications will be privileged.

245. ABA STANDARDS, *supra* note 5, §§ 5.10, 5.11:

5.10 Public facilities.

No order should be permitted authorizing or approving the overhearing or recording of communications over public facilities unless an additional showing is made establishing probable cause for belief that—

(i) the overhearing or recording will be or was made in such a manner so as to eliminate or minimize insofar as practicable the overhearing or recording of other communications whose overhearing or recording are not or would not be authorized, and

(ii) there is or was a special need for the overhearing or recording of communications over the facilities.

5.11 Privileged communications.

(a) Facilities and places.

No order should be permitted authorizing or approving the overhearing or recording of communications over a facility or in a place primarily used by licensed physicians, licensed lawyers, or practicing clergymen or in a place used primarily for habitation by a husband and wife unless an additional showing as provided in 5.10 is made.

(b) Communications.

out, such a showing is a hollow formality; it adds nothing to the requirements for the interception of any communication.[246] Short of the equally impractical solution of outlawing surveillance on those facilities and premises entirely,[247] there seems to be no feasible method of avoiding the interception of privileged communications. Rather than placing unworkable restraints on their interception, privileged communications might best be protected by attempting to prevent their use after acquisition. This approach will be explored in the next section.[248]

The ABA standards require the same additional showing to be made when surveillance involves public telephone facilities.[249] But the monitoring of public telephones involves such numerous and indiscriminate invasions of privacy that it should be disallowed completely unless a better control device than the ABA's additional showing can be found.[250] One possibility would be to permit the surveillance of such facilities only if the suspect named in the warrant is under visual observation and the monitoring can be limited to his calls.[251] The construction and location of most telephone booths would seem to make this solution feasible.

### 2. *Limitations on Use of Intercepted Communications*

In addition to placing restraints on the interception of communica-

---

No privileged communication however overheard or recorded should be disclosed or used unless it is necessary in the disclosure or use of other communications whose overhearing or recording was authorized or approved.

246. Schwartz, *supra* note 97, at 481-82. It is difficult to see how the "additional showing" would have a significant effect on the issuance of orders. The showings which must be made presumably would be required for the issuance of any surveillance order. *Compare* ABA STANDARDS, *supra* note 5, § 5.10(i) (quoted in note 245 *supra*), *with* 18 U.S.C. § 2518(5) (Supp. IV, 1965-68) (quoted in note 226 *supra*); *compare* ABA STANDARDS, *supra* note 5, § 5.10(ii), *with* 18 U.S.C. § 2518(1)(c) (Supp. IV, 1965-68).

247. As the commentary on section 5.11 of the *ABA Standards* points out, complete immunity would soon turn homes and lawyers' offices into communications centers for criminal operations. *See* ABA STANDARDS, *supra* note 5, at 154.

248. See text at notes 268-76 *infra*.

249. See note 245 *supra*.

250. An oft-cited example is the tapping of a public telephone in New York City which resulted in the recording of conversations involving the Julliard School of Music, Brooklyn Law School, Consolidated Radio Artists, Western Union, Mercantile Commercial Bank, several restaurants, a drug store, a real estate company, an importer, many lawyers, a stationery store, a dry cleaner, numerous bars, a garage, the Prudential Insurance Company, a health club, the Medical Bureau to Aid Spanish Democracy, dentists, brokers, engineers, and a New York police station. *See Hearings Before a Subcomm. of the Senate Comm. on Interstate Commerce Pursuant to S. Res. 224*, 76th Cong., 3d Sess., at 833-959 (1940).

251. Surveillance of public telephones could be most discriminating if subjected to a strict visual observation requirement. Given the open nature of most of these facilities, it should not be too onerous to require that surveillance be limited to the time the police actually observe the suspect using the facilities. That was apparently the procedure used in *Katz*. See note 82 *supra*.

tions, the Crime Control Act also restricts the use which can be made of lawfully intercepted communications.[252] In general these restrictions allow a law enforcement officer who obtains information procured by means of an authorized interception[253] to use it in the performance of his official duties,[254] communicate it to other law enforcement officials,[255] and disclose it in testimony at a trial or grand jury proceeding.[256] Any other divulgence of the information subjects him to the full criminal and civil sanctions of title III.[257] While this limitation

252. 18 U.S.C. § 2517 (Supp. IV, 1965-68):

> (1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.
>
> (2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.
>
> (3) Any person who has received, by any means authorized by this chapter, any information concerning a wire or oral communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any criminal proceeding in any court of the United States or of any State or in any Federal or State grand jury proceeding.
>
> (4) No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.
>
> (5) When an investigative or law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized herein, intercepts wire or oral communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

The California Privacy Act does not even mention the subject of police use of lawfully intercepted communications.

253. The nontestimonial uses are not strictly limited to information lawfully intercepted. In limited situations, such as the prosecution of an eavesdropper, disclosure of an illegally seized communication would be appropriate to the proper performance of the officer's duties. *See* SENATE REPORT, *supra* note 95, at 99-100.

254. Uses permitted in the performance of official duties would include establishing probable cause for arrest or search and developing witnesses. *Id.*

255. The disclosure must also be appropriate to the proper performance of the duties of the officer receiving the information. *Id.*

256. This disclosure is not limited to law enforcement officers. Any person who has legally received lawfully intercepted information can testify to it. *See* 18 U.S.C. § 2517(3) (Supp. IV, 1965-68), quoted in note 252 *supra.*

257. *See id.* §§ 2511(1), 2520.

on the use of intercepted communications is directly applicable to state officials,[258] any state enabling legislation should carry a similar provision to cover situations where the state authorization procedures might be more stringent than the federal rules.[259]

Additional controls are necessary to deal with situations where the surveillance does not follow the normal pattern, as when an authorized eavesdrop or wiretap produces evidence of a crime other than that specified in the order. The use of such evidence poses a difficult problem. The objection to allowing its use is, of course, the danger that the authorities will use electronic search warrants as a pretext for making general exploratory searches.[260] Where, however, the original order is obtained and executed in good faith, the interception is incidental to such execution, and the scope of the search is limited to that specified in the authorizing order, there is no reason to disallow the use of such evidence. The privacy of the victim has already been invaded by the authorized search, and no societal interest is served by suppressing the evidence.[261]

In conventional search and seizure cases this dilemma can be solved, if necessary, by requiring the procurement of another warrant to authorize the seizure of the unexpected evidence.[262] Due to the very

258. *See id.* §§ 2510(7), 2511(2)(c), 2516(2), 2517. Section 2517 applies to any investigative or law enforcement officer, defined in section 2510 to include state officials, who obtains the information by any means authorized in the chapter. Since any authorization for surveillance at the state level comes from section 2516 (or in the case of consensual surveillance from section 2511), state officials acting pursuant to their own enabling act would come under the restrictions of section 2517.

259. For example, if California passed an enabling statute which required a warrant for participant monitoring as well as third-party surveillance, see text at notes 302-09 *infra*, an officer eavesdropping with the consent of only one party would run afoul of the state law without violating the federal statute. See text at notes 173-75 *supra*.

260. *Cf.* Marron v. United States, 275 U.S. 192 (1927).

261. *See generally* ABA STANDARDS, *supra* note 5, at 144-45.

262. *See* Aron v. United States, 382 F.2d 965, 973 (8th Cir. 1967) (dictum); People v. Roberts, 47 Cal. 2d 374, 303 P.2d 721 (1956). At present it is not totally clear under what circumstances another warrant would have to be obtained in order to seize the evidence. In Marron v. United States, 275 U.S. 192 (1927), the Supreme Court held that evidence not described in a search warrant could not be seized pursuant to the warrant even though relating to the same offense and discovered in the course of the search pursuant to the warrant. *Id.* at 195-98. At the same time, however, the Court approved the seizure of the same evidence on the grounds that the officers could seize the instrumentalities of a crime being committed in their presence during a search incident to an arrest for that crime. *Id.* at 198-99. Since that time, the lower federal courts have allowed the seizure of instrumentalities of a crime being committed in the presence of officers performing a search for other evidence pursuant to a warrant. *See, e.g.*, Aron v. United States, *supra*, at 973-74; United States v. Eisner, 297 F.2d 595 (6th Cir. 1962); Johnson v. United States, 293 F.2d 539 (D.C. Cir. 1961), *cert. denied*, 375 U.S. 888 (1963). Until recently, however, no court had permitted the seizure of evidence not described in the warrant which did not consist of the instrumentalities of a crime. But the repudiation of the "mere evi-

nature of electronic searches this solution is impossible in the electronic surveillance context. But the same result theoretically can be reached by requiring judicial approval before the evidence can be used.[263] Although this again involves the possibility of justifying the methods in light of the results, the dangers are probably less than in the emergency authorization situation.[264] Here, the incidence of abuse would be less because the police must obtain a warrant and establish probable cause concerning the commission of some offense in order to initiate the surveillance in the first place. In addition, the validating court will be able to reexamine the probable cause for the original warrant in light of the differing results obtained.

The Crime Control Act permits evidence of unexpected crimes to be used in the same manner as evidence whose seizure has been authorized, with the proviso that it cannot be used at trial without prior judicial approval.[265] If the use of such evidence is to be permitted at all, however, the requirement of judicial validation should be extended to all uses. The evidence can be just as damaging if used for investigative purposes. If evidence is intercepted in a subterfuge search, it should not only be inadmissible in court, it should not be used at all.[266]

A similar problem arises when legal surveillance produces evidence incriminating a person not named in the authorizing order. The Crime Control Act is silent on this problem, but the same considerations are present here as in the unexpected offense problem. There might be a greater incentive to attempt to fabricate probable cause in order to en-

---

dence rule" in Warden v. Hayden, 387 U.S. 294 (1967), has led one district court to admit such evidence. United States v. Robinson, 287 F. Supp. 245 (N.D. Ind. 1968). Whether this further liberalization will be condoned by the Supreme Court remains to be seen.

263. Since the search and seizure involved in an electronic interception constitute one indivisible operation there is no possibility of obtaining an additional warrant. The evidence has already been seized and the only question is whether its use will be allowed. Given the impossibility of prior authorization the only alternatives are subsequent validation or a complete prohibition on the use of the evidence. The purpose of the particularity requirement in the warrant is to prevent general searches. *See, e.g.*, Berger v. New York, 388 U.S. 41, 58 (1967); Marron v. United States, 275 U.S. 192, 196 (1927). Therefore if it is shown on subsequent application that the evidence was necessarily intercepted during the proper execution of a lawful surveillance order, the purposes of the fourth amendment are satisfied and the evidence should be available for use.

264. See text at notes 237-42 *supra*.

265. *See* 18 U.S.C. § 2517(5) (Supp. IV, 1965-68), quoted in note 252 *supra*. The evidence need not be of one of the offenses for which interception can be authorized under section 2516. *See* SENATE REPORT, *supra* note 95, at 100.

In order to use the evidence at trial it must be shown upon subsequent application that "the original order was lawfully obtained, that it was sought in good faith and not as a subterfuge search, and that the communication was in fact incidentally intercepted during the course of a lawfully executed order." *Id.*

266. *Cf.* Silverthorne Lumber Co. v. United States, 251 U.S. 383, 392 (1920).

gage in exploratory searches here, however, since the potential rewards are greater. The potential gain here is the opportunity to gather and use evidence against a large number of persons—all those who might be in communication with the person named in the warrant—as opposed to the possibility of gathering evidence of additional offenses against a single individual—the person designated in the order. However, this distinction is probably not significant enough to warrant different treatment of the two situations. If such evidence is to be used it should be subjected to prior judicial scrutiny to ensure that it was obtained within the scope of the authorized intrusion.[267]

Finally, it is necessary to consider the use of privileged communications. In the past such communications normally lost their privileged character when intercepted by a third party; thus the holder of the privilege was not protected against testimony by an eavesdropper.[268] Section 2517 now provides that any communication intercepted either in violation of or in accordance with the provisions of title III shall not lose its privileged nature because of the interception.[269] California had earlier reached the same result when it enacted its Evidence Code.[270] However, this extension is still inadequate, in an electronic surveillance context, to fulfill the basic policy objectives which the doctrine was created to promote.

---

267. Not only would this blanket requirement of subsequent validation provide a salutary deterrent to subterfuge searches, it would relieve the state in a subsequent prosecution from having to prove that any evidence derived from the intercepted communication was not the fruit of a poisonous tree. See text accompanying notes 361-67 *infra*.

268. The traditional privileged relationships of attorney-client, physician-patient, husband-wife, and priest-penitent afforded to the client, patient, communicating spouse, and penitent a protection from either voluntary or involuntary disclosure by the other party to the relationship of the privileged communications in legal proceedings. However, this privilege was not extended to cover disclosures by third parties, so that parties who acquired such communications by overhearing or other surreptitious methods were not barred from testifying to their contents. *See* ABA STANDARDS, *supra* note 5, at 156-57; 8 J. WIGMORE, *supra* note 23, at §§ 2325-26, 2339, 2381. *But see* UNIFORM RULES OF EVIDENCE rule 26 (extending lawyer-client privilege by preventing disclosure by eavesdroppers).

269. 18 U.S.C. § 2517(4) (Supp. IV, 1965-68): "No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character." This section is not intended to create a uniform national privilege doctrine. It adopts the nature and scope of the privileges as defined by state law but provides that these privileges will not be abrogated by electronic interception. *See* SENATE REPORT, *supra* note 95, at 100.

270. The Evidence Code provides that the holder of any privilege can prohibit an eavesdropper or other interceptor from testifying to a privileged communication. *See* CAL. EVID. CODE §§ 954 & Comment (lawyer-client), 980 & Comment (confidential marital communications), 994 & Comment (physician-patient), 1014 & Comment (psychotherapist-patient), 1033 & Comment (clergyman-penitent) (West 1968).

It should be noted that in California the physician-patient privilege is not applicable in criminal proceedings. *Id.* § 998.

The traditional lawyer-client, husband-wife, physician-patient, and priest-penitent privileges are founded on a policy judgment that the ultimate goals of society are best served by guaranteeing complete freedom of communication in these relationships.[271] This atmosphere of freedom is maintained even at the expense of suppressing relevant evidence, and is achieved only when the fear of compulsory disclosure is removed.[272] To this end California, like most states, provides that the state cannot compel either party to testify to confidential communications made in the course of such a relationship.[273] However, this rule, even when extended to cover eavesdroppers, only prevents the eavesdropper from testifying in legal proceedings; it would not prohibit use of the communication for investigative purposes.[274] The inadequacy of this protection in an electronic surveillance situation is readily apparent. Every electronic interception is in effect a compulsory disclosure which the privilege holder is powerless to prevent, and the use of the information obtained by such a disclosure for investigative purposes destroys the effectiveness of the privilege just as would compelled testimony.[275] For this reason the traditional privilege doctrine should be further modified to prohibit all uses of privileged communications whether intercepted legally or illegally.[276]

There are, of course, practical problems involved in attempting to restrict the use of any intercepted evidence for investigative purposes. Once the officer has overheard a conversation no statutory mandate or court order can wipe it from his mind. But if, as was suggested earlier,[277] the actual performance of surveillance work is restricted to a small group of technicians under the control of the district attorney, the surveillance and investigative functions could be effectively isolated from one another. All evidence obtained by surveillance personnel would be turned over to the district attorney for dissemination to the appropriate law enforcement agencies. The district attorney could be required to obtain judicial approval before releasing any information that was not obtained in strict conformity with the surveillance order.

271. *See* 8 J. WIGMORE, *supra* note 23, at §§ 2290-91 (lawyer-client), 2332 (husband-wife), 2380a (physician-patient), 2396 (priest-penitent).

272. *Id.*

273. See note 270 *supra* and sources cited therein.

274. *See* CAL. EVID. CODE §§ 901, 910 (West 1968). The privileges apply in proceedings in which testimony can be compelled to be given. *Id.*

275. *Cf.* CAL. EVID. CODE § 910, Comment (West 1968). If the purpose of the privilege is to encourage free communication in these relationships the knowledge that an intercepted communication could be used to develop other evidence would exert just as much of a chilling effect on communication as would the knowledge that the message itself could be used as evidence.

276. This solution was incorporated in the ABA standards. ABA STANDARDS, *supra* note 5, at § 5.11(b), quoted in note 245 *supra.*

277. *See* text at notes 223-25 *supra.*

The ultimate check would be the right of the accused to show that evidence introduced against him was the fruit of an electronic search which was illegal to begin with or which exceeded the scope of the authorization.[278]

### 3. *Summary*

The safeguards discussed in the preceding sections by no means constitute an exhaustive list. There are numerous other measures which, because they are adequately covered in the Crime Control Act or are not controversial, have been omitted. Thus any scheme should include provisions to prevent tampering with recordings and otherwise to ensure the fidelity of reproduction of surveillance evidence.[279] Provision should be made for notice to the subject of the surveillance in time for him to challenge the evidence and to prepare adequately for trial.[280] The ultimate goal of the system should be to ensure that electronic surveillance is permitted only where it is necessary and effective, that it is only employed pursuant to proper authorization supported by probable cause, that it is performed in such a way as to minimize the interception of innocent communications, that the information obtained is used only for legitimate purposes, and that the procedures facilitate effective judicial review.

## IV

## PARTICIPANT MONITORING

Up to this point, the discussion has centered on those types of surveillance conducted without the knowledge of the communicating parties. This Part will deal with another aspect of the surveillance problem—surveillance in which one of the parties is involved, either actively, by recording the conversation himself or transmitting it to a third party, or passively, by allowing a third party to monitor the conversation electronically. These practices, collectively referred to as participant monitoring,[281] are probably far more widespread than third-party

278. See text at notes 361-65 *infra*.

279. *E.g.*, 18 U.S.C. §§ 2518(8)(a), (b) (Supp. IV, 1965-68), quoted in note 226 *supra*.

280. *E.g.*, *id.* § 2518(8)(d).

281. The term "participant monitoring" comes from Greenawalt, *supra* note 58. Although there are many different forms of participant monitoring, and distinctions can and should be drawn between them in determining what legal sanctions to apply, the subject can be treated unitarily for the purpose of discussing the desirability of imposing legal controls at all. While the purposes and methods of the monitoring may vary, all forms of participant monitoring have a common feature: the accurate, instantaneous reproduction of the speaker's words to an unknown auditor, either human or electronic. It is this characteristic, common to all forms of participant

surveillance.[282] Police use of undercover agents and informers to record incriminating conversations is common,[283] and the amount of participant recording and eavesdropping performed by private parties is beyond estimation.[284] Although participant monitoring has not received as much attention as the more exotic forms of electronic surveillance,[285] it poses a serious privacy problem in its own right, a problem which should be the subject of legislative concern.

### *A. The Problem*

Participant monitoring traditionally has been tolerated as part of the risk of listener republication inherent in conversation, under the rationale that since the listener is free to repeat a conversation to a third party he is also free to transcribe it electronically or to allow the third party to listen in.[286] It is true that a speaker always risks repetition by his listener, if only because of the inadequacy of the legal system to con-

---

monitoring, which provides the common analytical key. For example, one might argue that recording of a conversation is a more serious breach of privacy than just allowing a third person to monitor it, because the former is more permanent and is capable of being disseminated to a larger audience. However, each contains the same element of speaker loss of control over the extent of dissemination.

Distinctions should and will be made, however, in discussing what legal sanctions to apply. For that purpose it is necessary to weigh the purpose and objective of the monitoring against its social disadvantages to determine the amount of control to be applied. See Part IV, section B *infra.*

282. *See* Greenawalt, *supra* note 58, at 211-12.

283. *See* PRIVACY AND FREEDOM, *supra* note 1, at 131. The great preponderance of California appellate cases dealing with electronic surveillance involve some form of participant monitoring. *See, e.g.,* California cases cited note 57 *supra.* Testimony before Senator Long's committee in 1965, see note 125 *supra,* revealed that participant monitoring was also the most common form of electronic surveillance utilized by federal agencies such as the Food and Drug Administration and the Internal Revenue Service. *See* THE INTRUDERS, *supra* note 4, at 110-11 (FDA), 133 (IRS).

284. *See* Greenawalt, *supra* note 58, at 212. It has been common practice among lawyers in California, at least prior to the Privacy Act, to record all important incoming calls. *See* REGAN COMM. REPORT, *supra* note 125, at 11.

285. Although a great deal has been written concerning electronic surveillance in general, relatively little attention has been devoted to the special problems of participant monitoring. At present the Greenawalt article, *supra* note 58, is the definitive work on this particular aspect of the surveillance problem. *See also* Enker, *Controls on Electronic Eavesdropping—A Basic Distinction,* 2 ISRAEL L. REV. 461, 462 (1967).

286. *See, e.g.,* Lopez v. United States, 373 U.S. 427 (1963); Rathbun v. United States, 355 U.S. 107 (1957); Enker, *supra* note 285, at 462. This theory was succinctly summarized by Justice White in his concurring opinion in *Katz*: "When one man speaks to another he takes all the risks ordinarily inherent in so doing, including the risk that the man to whom he speaks will make public what he has heard. The Fourth Amendment does not protect against unreliable (or law-abiding) associates. [citation omitted] It is but a logical and reasonable extension of this principle that a man take the risk that his hearer, free to memorize what he hears for later verbatim repetitions, is instead recording it or transmitting it to another." 389 U.S. at 363 n.*.

trol every minor breach of confidence.[287] It is not so clear, however, that this normal risk of listener betrayal should include the risk of electronic monitoring. There is a qualitative as well as a quantitative difference between secondhand repetition by the listener and simultaneous dissemination to a second auditor, whether that auditor be a tape recorder or a third party.[288] In the former situation the speaker retains control over the extent of his immediate audience. Even though that audience may republish his words, it will be done secondhand, after the fact, probably not in entirety, and the impact will depend upon the credibility of the teller. Where electronic monitoring is involved, however, the speaker is deprived of the right to control the extent of his own firsthand dissemination. A new audience—either electronic or human—has been introduced: an audience whose size and very existence are outside the speaker's control; an audience which gives independent evidence of the speaker's statements.[289] In this regard participant monitoring closely resembles third-party surveillance; both practices deny the speaker a most important aspect of privacy of communication—the right to control the extent of first instance dissemination of his statements.[290]

To say that the speaker assumes the risk of participant monitoring when he chooses to indulge in confidential conversation is a fiction. An assumption of risk connotes the existence of a viable, less risky alternative; in this case the only alternative is not to speak at all.[291] The risk can be minimized to some extent by careful choice of auditors, but it can only be eliminated by refraining from conversing entirely. In fact, the risk of participant monitoring is not assumed, it is imposed upon the speaker by the legal system, or, more correctly, the system allows the listener to impose it. The real question, then, is whether that risk should be imposed. The answer, it is submitted, is no.

---

287. The primary reason that a listener is free to repeat confidential messages is not because society considers such action morally correct, but because it would be impossible for the legal system to control every such act of bad faith.

288. *See* Lopez v. United States, 373 U.S. 427, 450 (1963) (Brennan, J., dissenting). This rationale was accepted by the FCC when it proscribed the use of radio transmitting devices to overhear or record communications without the consent of *all* parties. *See* 31 Fed. Reg. 3397-98 (1966).

289. It is well established that, once properly qualified and admitted, recordings are independent evidence and are not dependent upon the credibility of the listener who made them. Lopez v. United States, 373 U.S. 427, 448 (1963) (Brennan, J., dissenting); Monroe v. United States, 234 F.2d 49, 54-55 (D.C. Cir. 1956). Testimony of a second party who was allowed to listen in would of course be independent evidence if he could identify the parties.

290. *Cf.* Lopez v. United States, 373 U.S. 427, 452 (1963) (Brennan, J., dissenting): "[T]he suggestion that the right of privacy is lost . . . by the auditor's consenting to transcripton of the speaker's words. . . . invokes a fictive sense of waiver wholly incompatible with any meaningful concept of liberty of communication."

291. *See id.* at 450 (Brennan, J., dissenting).

One argument against the unrestricted use of participant monitoring is that it is unethical; that it is unfair to record or permit another party to listen in on a person's communications without his knowledge or consent.[292] The degree to which the practice offends notions of fair play varies with the circumstances,[293] but, except for a few limited uses such as in psychotherapy or behavioral research,[294] even the most innocuous forms of participant monitoring, such as the recording of a business call for future reference, involve a deception which appears to be inconsistent with basic norms of fairness.

One stumbling block to judicial imposition of controls on law enforcement monitoring on fairness grounds has been the difficulty of distinguishing participant monitoring from other deceptive police practices.[295] Although the invasion of privacy occasioned by an informer recording a conversation is arguably more serious than if the same informer related his information secondhand,[296] the practices can hardly be differentiated on moral grounds. This difficulty need not deter a legislature from attacking the problem, however; they are free to deal with one aspect of it at a time.

The unfairness argument is not the only reason for imposing controls on participant monitoring. After all, many unethical practices, while incurring societal disapproval, are not subjected to legal sanctions. A more serious objection to participant monitoring was voiced by Justice Brennan in his dissent in *Lopez v. United States*:[297]

> If a person must always be on his guard against his auditor's having authorized a secret recording of their conversation, he will be no less reluctant to speak freely than if his risk is that a third party is doing the recording. . . . I believe that there is a grave danger of chilling all private, free, and unconstrained communication if secret recordings, turned over to law enforcement officers by one party to a conversation, are competent evidence of any self-incriminating statements the speaker may have made. In a free society, people ought not to

292. *See generally* Greenawalt, *supra* note 58, at 214-15.

293. A deceptive recording of a confidential conversation by an erstwhile friend for blackmail purposes would no doubt be viewed with more opprobrium than the recording of a bribery offer by a public official.

294. These examples are offered as "good" uses of participant monitoring, but it is by no means certain that even they would be universally viewed as being consistent with norms of fair play. *See generally* Ruebhausen & Brim, *Privacy and Behavioral Research*, 65 COLUM. L. REV. 1184 (1965).

295. The Supreme Court has not been anxious to impose constitutional controls on participant monitoring, and one of the primary reasons for the Court's inaction undoubtedly has been the fact that an assault on participant monitoring would open up a Pandora's box, with other even more odious police deceptive practices called into question. *See* Lopez v. United States, 373 U.S. 427, 465-66 (1963) (Brennan, J., dissenting).

296. See text at notes 288-90 *supra*.

297. 373 U.S. 427 (1963).

have to watch their every word so carefully.[298]

Although Justice Brennan was speaking in a criminal context, the argument is also applicable to monitoring for private purposes. It is not only the fear of having incriminating statements monitored which would tend to inhibit free communication. Everyday business and social conversation is marked by exaggeration, profanity, coarse figures of speech, and the expression of unpopular ideas or beliefs.[299] These things impart color to social discourse, as well as an ambiance conducive to the free interchange and development of ideas. Although inoffensive, the speaker would normally prefer that they not progress past his immediate audience, much less be recorded for posterity on magnetic tape. This "unedited quality of conversation"[300] contributes to the atmosphere of a free and open society and should be preserved if true freedom of communication is to be maintained.

Moreover, it is not only the unedited quality of conversation that will be lost if people fear to speak casually for fear of being monitored. Exaggeration, profanity, and other speech mannerisms, in addition to imparting a personal flavor to conversation, often serve as a vital aid to communication. By reason of personality, habit, or education, many people are virtually unable to communicate without the use of such conversational crutches. Such persons might be deterred from conversing on matters of substance because of the fear of having these indispensable but inconsequential utterances monitored. The result would be a loss of substantively important conversation because of the fear of participant monitoring.

In light of the foregoing discussion, the argument for imposing controls on participant monitoring appears persuasive if participant monitoring would, in fact, have the chilling effect which Justice Brennan ascribed to it. Justice Brennan assumed, without analysis, that participant monitoring would exert as great a chilling effect on communication as would third-party surveillance.[301] However, Professor Greenawalt of Columbia, in what is to date the most exhaustive treatment of the participant monitoring problem,[302] reached a different conclusion. After examining the effect the risk of participant monitoring would have in a variety of confidential communication situations, he concluded that the threat posed by participant monitoring, although serious, was substantially less than that created by third-party surveil-

298. *Id.* at 452. *See* Osborn v. United States, 385 U.S. 323, 353-54 (1966) (Douglas, J., dissenting); *cf.* King, *supra* note 15, at 24-30.

299. *See* Schwartz, *On Current Proposals to Legalize Wire Tapping*, 103 U. PA. L. REV. 157, 162 (1954).

300. *Id.*

301. See quotation in text at note 298 *supra*.

302. Greenawalt, *supra* note 58.

lance.[303] Whereas most people rely on their physical surroundings and a lack of interest in their conversations to protect themselves from third-party snooping, the principal protection against party monitoring is the reliance of the speaker on the character of his auditor. Most speakers have such confidence in the persons they choose to confide in that the threat of participant monitoring would not deter them from speaking.[304]

However, the fact that participant monitoring is not quite as dangerous or offensive as third-party monitoring is only half an answer. On balance, the threat posed by participant monitoring is still sufficiently great to warrant careful regulation. In some situations it might be the determinative factor in the decision to speak or not. Even more important would be the general chilling effect that pervasive monitoring would foster. Widespread use, especially if publicized, would surely make people more wary of talking freely, and this vague, general fear of being monitored would destroy the relaxed and casual atmosphere necessary for the free interchange of ideas. This effect would be particularly strong where the speaker is using an electronic medium which does not involve face-to-face confrontation with the listener.[305] Pervasive use of participant monitoring by the police would exert this chilling effect with special force on those who espouse unpopular political beliefs, whose even casual conversations might be of more than passing interest to the authorities.[306]

The preceding arguments suggest that participant monitoring be subjected to some type of legal control because of its intrinsic immorality and because of the threat it poses to freedom of communication. The next section will consider just what these controls should be. Again the discussion will take place within the framework of California law.

### *B. The Controls*

#### *1. Monitoring by Private Parties*

California is one of the few states to have outlawed participant monitoring by private parties.[307] This was the major change effected by the 1967 Privacy Act and it will have an impact on the conduct of

303. "The likelihood of social harm in the form of inhibited communication from the addition to preexisting risks in conversation seems much less than with regard to third party overhearing. But in some specific cases it might make a crucial difference, and, more generally, widespread participant monitoring would be likely to have a subtle negative effect on people's willingness to communicate." *Id.* at 221.

304. *See id.* at 217-20.

305. It would seem that the sense of security which flows from visual confrontation would make face-to-face communication less susceptible to chilling than that carried on from remote locations over a medium which is susceptible to interception.

306. The more one's communications are of interest to the state, the greater the fear of monitoring and the greater the chilling effect because of the imperfection of the protections against sanctions—both formal and informal—against unpopular speech.

307. See note 58 *supra* and accompanying text.

even everyday business and personal affairs.[308] Whereas previous surveillance laws had required the consent of only one party to legitimize an interception,[309] the new statutes forbid any recording or overhearing by a third party without the consent of all parties to the conversation.[310] Most law enforcement officers are exempted from the all-party-consent requirement,[311] however, and there is a limited exception for private parties.

The private exemption is found in Penal Code Section 633.5[312] which allows one party to a confidential communication to record it if he reasonably believes that he will thereby procure evidence related to the commission of certain enumerated crimes. This provision permits the victim of threatened criminal action who has no time to obtain police assistance to record the threats for future evidentiary use.[313] If limited to this purpose, the exemption appears to be reasonable. By threatening or engaging in criminal action during the course of communication the party has forfeited any claim to privacy he might have; he clearly could not reasonably expect his audience to remain limited. Furthermore, the chilling effect which this exception is intended to produce on narrowly defined areas of conversation should not carry over into general conversation of a noncriminal character. However, strict enforcement of the reasonable belief requirement will be required to ensure that this section will not be used as a pretext for the general recording of private communications. The limitation of the offenses for which evidence can be recorded to those involving violence or those

308. Such relatively innocuous, and heretofore permissible, activity as recording a business call or listening on an extension now subjects the party to possible felony criminal sanctions. *See* CAL. PENAL CODE §§ 631, 632 (West Supp. 1968).

309. The old electronic eavesdropping statute required the consent of "any" rather than "all" of the parties to the conversation. *See* ch. 1886, [1963] Cal. Stats. 3871 (former Penal Code section 653j). The wiretapping statute was interpreted to give the same results. *See* People v. Dement, 48 Cal. 2d 600, 311 P.2d 505 (1957); People v. Malotte, 46 Cal. 2d 59, 292 P.2d 517 (1956). The one exception was former Penal Code section 653i which prohibited eavesdropping on the privileged conversations of persons in the custody or on the premises of law enforcement ageucies without the consent of all parties. *See* ch. 1879, [1957] Cal. Stats. 3285.

310. *See* CAL. PENAL CODE §§ 631, 632, 636 (West Supp. 1968) quoted in notcs 114, 130, 133 *supra.*

311. See text at notes 183-87 *supra.*

312. CAL. PENAL CODE § 633.5 (West Supp. 1968): "Nothing in Section 631 or 632 shall be construed as prohibiting one party to a confidential communication from recording such communication for the purpose of obtaiming evidence reasonably believed to relate to the commission by another party to such communication of the crime of extortion, kidnapping, bribery, any felony involving violence against the person, or a violation of Section 653m [pertaining to harassment by telephone], and nothing in Section 631 or 632 shall be construed as rendering inadmissible in a prosecution for [these crimes] auy evidence so obtained."

313. This at least was the purpose of the exemption. *See* Digest of A.B. 860, *supra* note 120.

which require communications for their consummation and the requirement that the evidence relate to the commission of the offense by the other party[314] should also help to prevent abuse of the privilege.

While the concept of section 633.5 is sound, the statute suffers from loose drafting. For example, it fails to specify what occurs when a party, reasonably believing that he will obtain evidence of one of the enumerated crimes, records a conversation which turns out either to be innocent or to contain evidence of a crime not listed in section 633.5.[315] If the recording is made upon reasonable belief there has been no violation of either the wiretapping or eavesdropping statutes, and their criminal sanctions would not come into play.[316] This is proper; there should be no criminal liability for a bona fide mistake. Unfortunately, however, in such a case the exclusionary and nondisclosure rules of those statutes are not operative either, since they apply only to evidence obtained in violation of the statutes.[317] Thus, as the statute now stands, there is no control over the recording party's use of mistakenly recorded information.[318]

In the situation where evidence of an unexpected crime is found, it would appear, by analogy to search and seizure law, that the evidence would still be admissible if obtained on reasonable belief, even though the admissibility rule of section 633.5 applies only to evidence of offenses named therein.[319] The situation is similar to a search incident to an arrest where an officer has probable cause to arrest for one crime and in the course of the associated search finds evidence related to another offense.[320] Such evidence is admissible,[321] and the same rule

314. *See* CAL. PENAL CODE § 633.5 (West Supp. 1968), quoted in note 312 *supra.*

315. *See generally* Degnan, *supra* note 122, at 262-63 & n.12. A related problem occurs when a recording of a conversation disclosing evidence of one of the enumerated crimes is introduced in a prosecution for a different offense. *See id.* at 263 n.12; *cf.* People v. Stanley, 67 Cal. 2d 837, 433 P.2d 913, 63 Cal. Rptr. 825 (1967). For example, a person on reasonable belief records obscene telephone calls in which the caller incriminates himself in a sex offense not covered by section 633.5. A literal reading of the statute would preclude admission of the recording in a prosecution for the sex offense, but that result seems questionable.

316. *See* CAL. PENAL CODE § 633.5 (West Supp. 1968), quoted in note 312 *supra.*

317. *See id.* §§ 631(a), (c), 632(d).

318. This would appear to be an error in drafting or an oversight for although the intercepting party should not be penalized for an honest mistake, he surely should not be allowed to take advantage of the mistake by making use of the information.

319. *See* CAL. PENAL CODE § 633.5 (West Supp. 1968), quoted in note 312 *supra.*

320. This is distinguishable from the case where a search pursuant to a warrant turns up evidence of a different crime than that specified in the warrant. In that situation, the seizure is limited by the description in the warrant. *See, e.g.*, Marron v. United States, 275 U.S. 192, 196 (1927). In legitimate warrantless searches, however, the courts are much more liberal and permit evidence of another crime to be used so long as the original search was reasonable and not a subterfuge. *See, e.g., id.* at 198-99; People v. Robinson, 62 Cal. 2d 889, 894, 402 P.2d 834, 837, 44 Cal. Rptr. 762, 765 (1965).

321. See note 320 *supra.*

probably would obtain here. However, in the interest of clarity the statute should spell out restrictions on both judicial and private use of erroneously recorded information.

In the abstract, California's broad proscription on all private participant monitoring seems desirable. Absent a compelling social need, such as that exemplified by the exception of section 633.5,[322] it is not unreasonable to require that a speaker at least be notified if his statements are to be recorded or otherwise monitored. Even the more innocuous forms of participant monitoring, if they became prevalent enough, could significantly affect patterns of communication. However, the adoption of such a rule in the abstract does not mean that all uses of participant monitoring should be subjected to possible felony criminal sanctions, as is the case in California.[323] The diversity of the purposes and motives for which participant monitoring is used suggest that a more discriminating application of sanctions might be desirable.

The uses of party monitoring cover a broad spectrum of social utility from blackmail at one end to behavioral research at the other,[324] and the uniform application of a severe criminal penalty to all of these activities is not a very sophisticated approach to the problem. In fashioning its solution the California Legislature either failed to appreciate these differences, or, recognizing the problem, opted for uniform sanctions, relying on prosecutorial discretion to differentiate between violations. Whatever the reason, the approach taken leaves much to be desired. Although prosecutorial discretion imparts flexibility to enforcement procedures, it is a two-edged sword. While it permits prosecution of only the most serious offenders, it also permits selective prosecution for other, less admirable reasons and it impairs the efficacy of the statute as a meaningful standard of conduct.[325] Furthermore, subjecting conduct of widely varying degrees of moral culpability to the same sanctions tends to breed a general disrespect for the law.[326] Finally, the application of such severe penalties to relatively harmless behavior may lead to a narrow interpretation of the statute as a whole.[327]

On the other hand, while some selectivity seems to be desirable,

322. A legislature could create additional exceptions if it felt the benefits of a particular type of monitoring outweighed its dangers. An example might be controlled scientific research or experimentation where confidentiality is maintained.

323. See note 385 *infra*.

324. In between these extremes participant monitoring is used for such multifarious purposes as investigating crime, determining customer reaction to a product or display, and preserving conversations to ensure they are not later distorted by one of the participants. *See generally* Greenawalt, *supra* note 58, at 212-24.

325. *See id.* at 232 n.206.

326. The law either deals too harshly with minor infractions or too leniently with serious ones.

327. *Cf.* People v. Vogel, 46 Cal. 2d 798, 804, 299 P.2d 850, 855 (1956).

the law cannot be broken down into a multitude of unwieldy distinctions. Although many possible bases for differentiation spring to mind,[328] the purpose for which the monitoring is accomplished appears to be the most relevant criterion on which to base criminal sanctions. The intended purpose of the monitoring is the factor which most clearly relates to the culpability of the defendant.[329] The Crime Control Act recognizes this distinction by exempting participant monitoring from its operation completely unless it is used for criminal, tortious, or injurious purposes.[330] While the federal Act goes too far in freeing much party monitoring from all controls—civil as well as criminal—it does provide a logical point at which to draw the line between differing criminal sanctions. The California penalty scheme is appropriate for tortious, injurious, or criminal uses, but less offensive monitoring should be classed as a misdemeanor at most and possibly freed from criminal sanctions altogether.

There is no need to so differentiate the other available sanctions, however.[331] The civil remedies are intrinsically discriminating, and so long as participant monitoring is illegal, its fruits should not be admissible as evidence. A civil cause of action (with a minimum damages provision) should be available to the victim who desires to vindicate his right to privacy. This would shift the onus of enforcing minor infractions to the aggrieved party and free an already overburdened criminal process from the task of policing petty breaches of confidence of marginal criminality.

### 2. *Monitoring for Law Enforcement Purposes*

If a state permits the use of third-party surveillance for law enforcement purposes, it would follow a fortiori that participant monitoring should also be allowed. Even if third-party surveillance is forbidden, a state might decide that participant monitoring should be permitted because of its lesser social disadvantages.[332] In either case, how-

328. Professor Greenawalt suggests such factors as location, degree of deception involved, relationship of the parties, and whether the use is offensive or defensive. *See* Greenawalt, *supra* note 58, at 223-25.

329. While this test does not correlate the seriousness of the invasion of privacy with the sanction, that function is probably better left to the civil remedies.

330. 18 U.S.C. § 2511(2)(d) (Supp. IV, 1965-68): "It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act . . . or for the purpose of committing any other injurious act."

331. Other sanctions include exclusion of evidence, civil damages suits, and injunctive relief. See Part V *infra* for a discussion of the available sanctions.

332. The dangers of participant monitoring are less in several respects. First, the victim is at least aware of the identity of his primary auditor and can base his disclosures

ever, it should not be left completely unregulated, as it is in California. Whether or not the Supreme Court ever imposes the warrant requirements of the fourth amendment on party monitoring,[333] the states themselves should subject it to judicial control. Both the unfairness and chilling effect arguments apply with special force when it is the state which is doing the monitoring. The unfairness of the practice is compounded by the exemplary effect of governmental immorality;[334] and widespread governmental use would have an Orwellian effect on communication.[335]

Application of the court order system envisioned for third-party surveillance could alleviate the problems mentioned above while still making participant monitoring available for legitimate police work.[336] Since the chilling effect of participant monitoring stems from indiscriminate use, a limited amount of controlled monitoring should not significantly affect communication habits. The requirement of probable cause will at least partially obviate the fairness problem.[337] Furthermore, the imposition of a warrant requirement should not seriously impair the usefulness of participant monitoring as a law enforcement tool; it will only ensure that probable cause exists for its use. In fact, participant monitoring is particularly amenable to judicial control. The most common techniques—outfitting an agent with a concealed microphone or recorder, or monitoring an informer's prescheduled telephone call—require a degree of prearrangement which could easily include obtaining a warrant.[338] Furthermore, the nature of participant monitoring is such that, as a practical matter, warrants would be easier to obtain than in third-party surveillance cases. The testimony of the

on his estimate of that party's reliability. Also, the chilling effect of participant monitoring is generally less than that of third-party surveillance. See text at notes 301-04 *supra*. Finally, because it is inherently more discriminating, participant monitoring can generally be restricted to the conversations of a particular suspect, thus producing a lesser number of intrusions upon the conversations of innocent third parties. *See generally* Enker, *supra* note 285, at 469-72; Greenawalt, *supra* note 58, at 221-27, 239.

333. See text at notes 88-92 *supra*.

334. Acts which are in themselves immoral take on added significance when performed by the government because the government sets an example for its citizens. See note 378 *infra* and accompanying text.

335. The chilling effect of governmental monitoring would be much more severe because of the omnipotence and omnipresence of the government. Whereas the ramifications of private monitoring do not normally extend past the immediate use of the information obtained, governmental monitoring is the first step toward governmental control. See text at note 20 *supra*.

336. *See* Enker, *supra* note 285, at 464; Greenawalt, *supra* note 58, at 229.

337. While it normally seems unfair to monitor a person's conversations without his consent, the fairness argument loses much of its vitality when there has been a judicial determination that there is probable cause to believe that the person has engaged in criminal activity and the conversations to be monitored are related to that activity.

338. *See* Greenawalt, *supra* note 58, at 229.

consenting party could help to establish probable cause. Because it is more selective, the particularity requirements are more easily met and the interception of innocent conversations can be minimized.[339] Indeed, participant monitoring appears to be the one type of surveillance which can be adapted to satisfy the demands of both law enforcement and privacy without major sacrifices on either side.

### C. *Problems of Consent*

In determining the legality of any particular instance of participant monitoring, it is always necessary to ascertain whether one or more parties consented to allow or to perform the monitoring. This is true whether or not participant monitoring is prohibited; for even when it is permitted, by definition the consent of one party is required. Determining the validity of consent is a judicial function and can involve a number of problems.

Perhaps the most important problem, and one that has not been fully explored, is defining what actually constitutes consent. California courts have held that express verbal approval is not necessary; consent may be established by reasonable inference from the surrounding circumstances.[340] The California surveillance statutes also make it clear that affirmative permission from every party is not always required. The definition of a "person" who eavesdrops in section 632(b) of the Penal Code excludes anyone known by all parties to be listening.[341] Similarly, the exemption for the use of recording equipment utilizing a tone signal device supplied by the telephone company[342] indicates that notice will usually obviate the need for express consent.

However, notice does not necessarily negate the speaker's desire for privacy, and there is obviously a limit to the amount of surveillance which mere notice will legitimize. When one party is allowed to dictate the conditions under which communication will take place, if at all, the problem of chilling the free flow of communication is again encountered. As surveillance becomes more widespread, the courts will be faced with a difficult task in determining where to draw the line. Already banks and large retail stores employ visual monitoring systems

339. In most participant monitoring situations the surveillance can be limited to the conversations of the particular suspect, and, where the participant himself is doing the recording, he may even be able to limit the recording to the particular conversations desired. *See* Enker, *supra* note 285, at 465-72; Greenawalt, *supra* note 58, at 230.

340. *E.g.*, People v. McShann, 177 Cal. App. 2d 195, 200, 2 Cal. Rptr. 71, 74 (1960); People v. Cox, 174 Cal. App. 2d 30, 36, 344 P.2d 399, 402 (1959).

341. CAL. PENAL CODE § 632(b) (West Supp. 1968): "The term 'person' . . . excludes an individual known by all parties to a confidential communication to be overhearing or recording such communication."

342. See text accompanying notes 140-43 *supra*.

for the detection of robbers and shoplifters.[343] Here, a conspicuously posted notice should suffice because the invasion of privacy—in view of the public nature of the place—is small compared to the evil deterred by the surveillance. But it is easy to imagine a situation where the balance would swing the other way. For example, it is doubtful that an employer could legalize the monitoring of all his employees' conversations merely by informing them that the plant was bugged. The effect such a massive violation of privacy would have on freedom of communication would far outweigh the interest of the employer.

As the above examples illustrate, the solution will again be one of balancing the interests involved. In so doing, the courts should consider such factors as the magnitude of the invasion of privacy, the availability of alternate means of communication, the availability of alternate methods of accomplishing the objective of the surveillance, the effect of the monitoring on social intercourse, and the social utility of the objective.

Another question that is certain to arise is whether consent can be given retroactively. For example, can a policeman who illegally intercepts a communication which incriminates one of the parties later validate his action and render the evidence admissible by obtaining the consent of the innocent party? Both the federal and California search and seizure cases hold that consent cannot be made retroactive,[344] and the same rule would probably apply here. If retroactive consent were allowed, the deterrent effect of the exclusionary rule would be largely nullified. Police would still perform illegal surveillance hoping to persuade—or coerce—one of the parties to ratify the action later.

Still another problem arises when the consenting party is in police custody. Any consent given is suspect because of the possibility of coercion. The fact that the consenting party is under arrest,[345] or is even given a promise of leniency,[346] does not necessarily negate the consent. Any additional pressure, however, would probably vitiate it. The courts have been quite lenient in this regard, probably because the victim of the coercion is not himself incriminated. Adoption of a court-order system for participant monitoring would to a large extent obviate this problem by subjecting the consent to judicial scrutiny before the surveillance takes place.

---

343. *See* THE EAVESDROPPERS, *supra* note 4, at 212.

344. *E.g.*, Weiss v. United States, 308 U.S. 321, 329-31 (1939); People v. Haven, 59 Cal. 2d 713, 719, 381 P.2d 927, 930, 31 Cal. Rptr. 47, 50 (1963). The legislative history of the Crime Control Act indicates that consent cannot be given retroactively under that statute either. *See* SENATE REPORT, *supra* note 95, at 94.

345. *See* People v. Jones, 237 Cal. App. 2d 499, 504, 47 Cal. Rptr. 40, 44 (1965).

346. *See* Black v. United States, 341 F.2d 583 (9th Cir.), *cert. denied*, 382 U.S. 584 (1965); People v. La Peluso, 239 Cal. App. 2d 715, 722-23, 49 Cal. Rptr. 85, 90, *cert. denied*, 385 U.S. 829 (1966).

## V

### SANCTIONS AND REMEDIES

The enforcement of rules governing the use of electronic surveillance has proved, through the years, to be an extraordinarily difficult task. The traditional sanctions—criminal penalties, civil damage suits, and exclusion of evidence—have been largely ineffective both in terms of deterring unlawful conduct and of providing redress for aggrieved parties.[347]

Probably the single biggest factor contributing to the enforcement problem is the difficulty of detection. Although almost all surveillance devices are susceptible of detection, most are vulnerable only to sophisticated and expensive countermeasures.[348] Furthermore, the victim must have some reason to believe that he is under surveillance before he can even attempt to determine its existence. Thus, practically speaking, most electronic surveillance is undetectable unless its fruits are used in such a way as to disclose its existence. This low probability of being caught renders much surveillance for covert purposes relatively undeterrable by threat of sanction. When the inherent shortcomings of the various sanctions which have been employed[349] are added to the problems of detection, the dismal enforcement record of the past is not difficult to explain.

A recognition of the enforcement problem resulted in major emphasis being placed on the remedial aspects of surveillance law in both the California Privacy Act and the Crime Control Act. Each provides a broad array of sanctions and remedies designed to secure compliance with its substantive provisions and to compensate the victims of illegal surveillance.[350] Old measures have been rejuvenated and new ones—new at least to electronic surveillance law—have been added in an attempt to make the new rules effective. Whether these enforcement provisions will be effective remains to be seen,[351] but the approach of

347. *See* People v. Cahan, 44 Cal. 2d 434, 445, 282 P.2d 905, 911 (1955); Paulsen, *Safeguards in the Law of Search and Seizure,* 52 NW. U.L. REV. 65, 72-76 (1957).

348. Detection techniques are so expeusive, complex, and time-consuming that for practical purposes properly installed devices are undetectable by the average victim. *See, e.g.,* PRIVACY AND FREEDOM, *supra* note 1, at 80-85; THE INTRUDERS, *supra* note 4, at 76; Westin, *supra* note 4, at 1009. *See generally* THE EAVESDROPPERS, *supra* note 4, at 305-81.

349. See text at notes 353, 386-96 *infra.*

350. *See* 18 U.S.C. §§ 2511-13, 2515, 2520 (Supp. IV, 1965-68); CAL. PENAL CODE §§ 631-32, 634-35, 637, 637.2 (West Supp. 1968). These provisions are discussed in the remainder of this section.

351. As yet there is uo record of either a criminal or civil action having been brought under either statute.

bringing to bear a wide variety of sanctions should help to compensate for the limitations of individual measures. Perhaps they will be able to accomplish collectively what they have been unable to do individually.

This section will briefly examine the enforcement provisions of the California Privacy Act and title III, which between them comprise most of the currently available remedial measures. An attempt will be made to point out the factors which limit the effectiveness of each, and refinements will be suggested in individual remedies.

### *A. The Exclusionary Rule*

Historically, the most controversial sanction has been the exclusion of evidence obtained through unconstitutional surveillance.[352] This "exclusionary rule" has been much criticized because it results in the suppression of reliable evidence and exonerates defendants for reasons unrelated to their guilt or innocence,[353] but it is now firmly entrenched in our constitutional jurisprudence as the primary remedy for deterring police violations of individual rights.[354] Under the rule, evidence which the government obtains by electronic surveillance in violation of the fourth amendment can be excluded in either federal or state criminal trials.[355]

Both the California Privacy Act[356] and the Crime Control

352. For discussions of the exclusionary rule, its theory and effectiveness see, *e.g.*, Allen, *The Wolf Case: Search and Seizure, Federalism, and the Civil Liberties*, 45 ILL. L. REV. 1 (1950); Barrett, *Exclusion of Evidence Obtained by Illegal Searches—A Comment on People vs. Cahan*, 43 CALIF. L. REV. 565, 583-88 (1955); Grant, *Circumventing the Fourth Amendment*, 14 S. CAL. L. REV. 359 (1941); *The Exclusionary Rule Regarding Illegally Seized Evidence: An International Symposium*, 52 J. CRIM. L.C. & P.S. 245 (1961). An excellent summary of the arguments pro and con the exclusionary rule will be found in Justice Traynor's exhaustive opinion in People v. Cahan, 44 Cal. 2d 434, 282 P.2d 905 (1955), in which California adopted the rule.

353. *See, e.g.*, Irvine v. California, 347 U.S. 128, 135-37 (1954); McGarr, *The Exclusionary Rule: An Ill Conceived and Ineffective Remedy*, 52 J. CRIM. L.C. & P.S. 266 (1961). See also the sources cited in People v. Cahan, 44 Cal. 2d 434, 442 n.*, 282 P.2d 905, 910 n.5 (1955).

354. *See* United States v. Wade, 388 U.S. 218 (1967) (lineup identification without counsel preseut); Miranda v. Arizona, 384 U.S. 436 (1966) (involuntary confessions); Mapp v. Ohio, 367 U.S. 643 (1961) (evidence obtained by unreasonable search and seizure).

355. *See* Mapp v. Ohio, 367 U.S. 643 (1961).

356. CAL. PENAL CODE §§ 631(c), 632(d) (West Supp. 1968): "Except as proof in an action or prosecution for violation of this section, no evidence obtained in violation of this section shall be admissible in any judicial, administrative, legislative or other proceeding."

The Privacy Act itself does not contain any procedures for suppressing the evidence. Where the interception constitutes an illegal search and seizure by governmental agents, the proper method of exclusion is through the mechanism of CAL. PENAL CODE § 1538.5 (West Supp. 1968). Section 1538.5 prescribes detailed procedures for the suppression of both tangible and intangible evidence and specifies that the pro-

Act[357] have codified the exclusionary rule, making evidence procured in violation of their substantive provisions inadmissible in court. The statutes have also expanded the scope of the rule by applying it to civil as well as criminal trials[358] and to evidence secured by private as well as governmental surveillance.[359] While the constitutional rule has largely

---

cedures outlined therein shall be the sole remedy of the defendant prior to conviction. *Id.* Where the evidence has been seized by a private party, the proper method of exclusion is by objection at trial. *See* People v. Superior Conrt, 70 Adv. Cal. 129, 449 P.2d 230, 74 Cal. Rptr. 294 (1969).

California's new divorce law also contains a provision forbidding the use of surveillance evidence obtained in violation of the Privacy Act in any proceedings for "dissolution of [a] marriage or legal separation or for a declaration of void or voidable marriage." CAL. CIV. CODE § 4250 (West Supp. 1969).

357. 18 U.S.C. § 2515 (Supp. IV, 1965-68): "Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter."

The method of exclusion is prescribed in *id.* § 2518(10), and is available for use in state as well as federal courts. Because title III covers almost the entire surveillance field, this mechanism will probably become a widely used method of suppressing surveillance evidence in state courts. State surveillance laws must still contain their own exclusionary provisions, however, to cover situations where the state laws are more stringent than the federal.

358. See notes 356 & 357 *supra.* The applicability of the constitutional exclusionary rule in purely civil proceedings is unclear. There is a California supreme court case holding unlawfully seized evidence admissible in civil proceedings, but the holding was based on the fact that at that time such evidence was also admissible in criminal trials. Munson v. Munson, 27 Cal. 2d 659, 664, 166 P.2d 268, 271 (1946). To what extent the adoption of the exclusionary rule in criminal proceedings has changed this rule remains to be seen, since there are no subsequent decisions in point. Since California does admit evidence illegally seized by private parties and subsequently turned over to the police in criminal proceedings, see note 359 *infra,* it seems likely that evidence seized by private litigants would still be admitted in civil trials. However, since the exclusionary rule in California is based exclusively on a police deterrence rationale, *see* People v. Cahan, 44 Cal. 2d 434, 447-49, 282 P.2d 905, 913-14 (1955), it seems unlikely that the courts would permit the use in civil proceedings of evidence illegally seized by law enforcement officers.

The question has not been disposed of in the federal system either. *Compare* Martin v. United States, 277 F.2d 785 (5th Cir. 1960) (admitting), *with* Lassoff v. Gray, 207 F. Supp. 843 (W.D. Ky. 1962) (excluding). However, the exclusionary rule does apply in forfeiture cases, *e.g.,* One 1958 Plymouth Sedan v. Pennsylvania, 380 U.S. 693 (1965), and the emphasis in forfeiture cases on classifying them as quasi-criminal in character implies that the rule may be inapplicable in purely civil proceedings.

359. In Burdeau v. McDowell, 256 U.S. 465 (1921), the Supreme Court ruled that evidence obtained by a private citizen in an unreasonable search and seizure and snbsequently turned over to federal authorities was admissible. The continued viability of this decision in light of Elkins v. United States, 364 U.S. 206 (1960) (repudiating the "silver platter" doctrine which allowed federal officers to use evidence seized illegally by state authorities), and Mapp v. Ohio, 367 U.S. 643 (1961), is open to question, but lower federal courts have consistently allowed such evidence to be admitted. *See, e.g.,*

been supplanted by the more expansive statutory provisions, it still has vitality in limited situations where an interception violates the fourth amendment without transgressing either the state or federal surveillance laws.[360]

There is a well-established corollary to the exclusionary rule which prohibits the use of secondary evidence derived from evidence which is itself the product of an unconstitutional search and seizure.[361] This "fruit of the poisonous tree"[362] doctrine is a necessary concomitant of the exclusionary rule; for the deterrent effect of the rule would be nullified if police were free to use illegally seized evidence to build their case even though they could not use it in court.[363]

The fruits doctrine also has been codified in the Crime Control Act which forbids the use of evidence derived from communications intercepted in violation of any of its provisions.[364] Although the California Act does not in terms refer to derivative evidence, the language

Barnes v. United States, 373 F.2d 517 (5th Cir. 1967); United States v. Goldberg, 330 F.2d 30 (3d Cir.), *cert. denied*, 377 U.S. 953 (1964); United States v. Masterson, 251 F. Supp. 937 (S.D.N.Y. 1966). California courts have also allowed its use. *See* People v. Randazzo, 220 Cal. App. 2d 768, 34 Cal. Rptr. 65 (1963); People v. Johnson, 153 Cal. App. 2d 870, 315 P.2d 468 (1957). A recent California supreme court decision seems to reaffirm this principle by indicating that there is no such thing as an "unreasonable search and seizure" by a private party. *See* People v. Superior Court, 70 Adv. Cal. 129, 135, 449 P.2d 230, 234, 74 Cal. Rptr. 294, 298 (1969).

However, the exclusionary provisions of the California Privacy Act and the Crime Control Act appear applicable no matter who performs the interception, so long as there is a violation. *See* CAL. PENAL CODE §§ 631(c), 632(d) (West Supp. 1968), quoted in note 356 *supra*; 18 U.S.C. § 2515 (Supp. IV, 1965-68), quoted in note 357 *supra*.

360. Unless the blanket proscription on the interception of oral communications in the Crime Control Act is held unconstitutional, see note 95 *supra*, the necessity for use of the constitutional rule should be rare because of the comprehensiveness of title III. One possible situation where the constitutional rule might have to be resorted to would arise if a California police officer monitored telephone conversations on an extension phone without the consent of any of the parties. This practice is seemingly exempted from the proscriptions of title III, see note 237 *supra*, and the California statute would not apply because of the law enforcement officer exclusion. See note 178 *supra* and accompanying text. However, in the absence of a warrant, such surveillance seems clearly unconstitutional under *Berger* and *Katz*.

361. *See* Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920). *See generally* Pitler, *"The Fruit of the Poisonous Tree" Revisited and Shepardized*, 56 CALIF. L. REV. 579 (1968); *Developments in the Law of Confessions*, 79 HARV. L. REV. 935, 1024-30 (1966).

362. Nardone v. United States, 308 U.S. 338, 341 (1939). In *Nardone* the Court held that evidence derived from conversations intercepted in violaton of section 605 of the Communications Act of 1934 was inadmissible. It was from Justice Frankfurter's opinion in this case that the doctrine acquired its name.

363. "The essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court but that it shall not be used at all." Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 (1920) (Holmes, J.).

364. 18 U.S.C. § 2515 (Supp. IV, 1965-68), quoted in note 357 *supra*.

"no evidence obtained in violation of this section"[365] will almost certainly be interpreted to include such evidence. California's exclusionary rule is grounded on a deterrence rationale,[366] and the California supreme court has readily accepted the fruits doctrine in conventional search and seizure cases.[367]

Although the exclusionary rule and the fruit of the poisonous tree doctrine are no longer seriously challenged, another problem associated with the rule is the subject of ongoing controversy. It is the question of who has standing to challenge the admissibility of illegally seized evidence. The Supreme Court, the Congress, and the State of California have taken markedly different positions on the standing question, and such divergence merits a brief appraisal of the various rules.

Under traditional fourth amendment theory the exclusionary rule is available only to those whose own constitutional rights have been violated.[368] Thus, in order to assert the constitutional exclusionary rule, the objectant must himself have been a party to the intercepted conversation or have a proprietary interest in the premises where the surveillance took place.[369] Under the Crime Control Act, a defendant has standing to object if he was a party to the conversation or if the surveillance was directed against him.[370] California imposes no stand-

365. CAL. PENAL CODE §§ 631(c), 632(d) (West Supp. 1968), quoted in note 356 *supra*.

366. *See* People v. Cahan, 44 Cal. 2d 434, 447-49, 282 P.2d 905, 913-14 (1955); People v. Martin, 45 Cal. 2d 755, 760, 290 P.2d 855, 857 (1955).

367. *See, e.g.*, People v. Stoner, 65 Cal. 2d 595, 422 P.2d 585, 55 Cal. Rptr. 897 (1967); People v. Bilderbach, 62 Cal. 2d 757, 401 P.2d 921, 44 Cal. Rptr. 313 (1965). In both of these cases confessions obtained when a defendant was confronted with evidence procured by an illegal search were held inadmissible.

368. *See, e.g.*, Wong Sun v. United States, 371 U.S. 471, 492 (1963); Jones v. United States, 362 U.S. 257, 261 (1960). *See generally* Comment, *Standing to Object to an Unreasonable Search and Seizure*, 34 U. CHI. L. REV. 342 (1967); Note, *Standing to Object to an Unlawful Search and Seizure*, 1965 WASH. U.L.Q. 488.

369. Alderman v. United States, 394 U.S. 165 (1969). Just what type of proprietary interest is required is left unclear by *Alderman*. The Court spoke exclusively of homeowners and the owners of premises in the opinion, *see id.* at 171-80, and apparently reserved the question of what other property interests would suffice to confer standing. *See id.* at 195-96 (Harlan, J., concurring and dissenting). In conventional search and seizure cases the proprietary interest requirement is fulfilled when the objectant was legitimately on the premises where the search occurred. Jones v. United States, 362 U.S. 257, 267 (1960).

*Alderman*'s grant of standing to those whose houses are bugged, regardless of their relationship to the conversation, is a throwback to the old property concepts of *Olmstead*. See note 27 *supra*. Of all possible bases for standing, this is the most irrational. It bears no relation to either the deterrence of police misconduct or the protection of the constitutional rights of the party. The right which is being protected, at least under *Katz*, is the right to be free from unreasonable interception of private conversations wherever located, not the right to be free from police trespasses. For a cogent criticism of this aspect of the *Alderman* holding see the concurring and dissenting opinion of Justice Harlan, 394 U.S. at 188-94.

370. Under the Crime Control Act, a motion to suppress evidence can be made

ing requirement at all; any defendant can seek to suppress illegally seized evidence, no matter what his standing vis-à-vis the illegality.[371]

The standing requirement supposedly rests on the principle that constitutional rights are personal and generally cannot be asserted vicariously.[372] True as that maxim may be, the primary purpose of forbidding the use of illegally seized evidence is not to vindicate the constitutional rights of the guilty, but to protect society in general from unwarranted police intrusions into their private affairs.[373] Proponents argue that even if deterrence is the primary objective of the rule, the additional deterrent effect created by abolishing the standing requirement is only marginal and is outweighed by the need for reliable evidence.[374] Although this argument may be persuasive in situations where "the constable has blundered,"[375] it loses its vitality where the police attempt to circumvent the exclusionary rule by engaging in surveillance for the express purpose of using the results against nonparties. In such cases, permitting nonparties to challenge the evidence would have more than a marginal deterrent effect. It was the opportunity for the use of such abusive practices which prompted the California supreme court to abolish the standing requirement entirely.[376]

Where the police act in willful disregard of the law, the argument

---

by an "aggrieved person", 18 U.S.C. § 2518(10)(a) (Supp. IV, 1965-68), who is defined to include "a person who was a party to any intercepted wire or oral communication or a person against whom the interception was directed." *Id.* § 2510(11).

371. This is the rule with respect to unconstitutionally seized evidence, *see* People v. Martin, 45 Cal. 2d 755, 290 P.2d 855 (1955), and since the Privacy Act mentions no standing requirement, the same rule presumably will apply to illegal surveillance evidence.

The California rule was carried to its extreme in People v. Jager, 145 Cal. App. 2d 792, 303 P.2d 115 (1956), where the police, having learned of an impending burglary from an informer, picked the lock on the office of the intended victim and installed a microphone through which they recorded conversations later used in the burglary prosecution. The defendants successfully suppressed the evidence on the grounds that the police had violated the constitutional rights of the victim, and under the rule of *Martin* they could assert this violation to have the evidence excluded. The same result would obtain today by a less tortured rationale, since under *Berger* and *Katz* the police conduct would be unconstitutional vis-à-vis the defendants.

372. *See* Alderman v. United States, 394 U.S. 165, 174 (1969). See note 369 *supra.*

373. *See, e.g.*, Linkletter v. Walker, 381 U.S. 618, 636-37 (1965).

374. *See* Alderman v. United States, 394 U.S. 165, 174-75 (1969); Weeks, *Standing to Object in the Field of Search and Seizure*, 6 ARIZ. L. REV. 65, 79 (1964).

375. People v. Defore, 242 N.Y. 13, 21, 150 N.E. 585, 587 (1926). The phrase is from Justice (then Judge) Cardozo's famous criticism of the exclusionary rule: "The criminal is to go free because the constable has blundered." *Id.*

376. "[I]f law enforcement officers are allowed to evade the exclusionary rule by obtaining evidence in violation of the rights of third parties, its deterrent effect is to that extent nullified. Moreover, such a limitation virtually invites law enforcement officers to violate the rights of third parties and to trade the escape of a criminal whose rights are violated for the conviction of others by the use of evidence illegally obtained against them." People v. Martin, 45 Cal. 2d 755, 760, 290 P.2d 855, 857 (1955).

that the government should not profit from its own immorality also weighs heavily against the imposition of a standing requirement.[377] It is one thing to permit the use of illegally intercepted evidence against nonparties where there has been a bona fide attempt to comply with the law, as where a warrant is obtained which later turns out to be defective. It is another thing entirely to allow such use where the surveillance was performed in open disregard of the terms and conditions of the warrant or where no attempt was even made to secure a warrant. As Justice Brandeis warned many years ago, the government is the teacher of the people, and to condone official lawlessness can only serve to breed disrespect for the law and encourage similar conduct on the part of individuals.[378]

Thus, at a minimum, standing should be conferred on parties to illegally intercepted conversations and on persons who can show that the surveillance was directed against them.[379] While there has been a reluctance to go further,[380] it would seem that under a warrant system the standing requirement should be abrogated completely where there has been a failure to obtain and execute the warrant in good faith.

### *B. Criminal Sanctions*

Since 1937, when Section 605 of the Communications Act was interpreted as forbidding wiretapping,[381] there have been fewer than 20 federal prosecutions for violations unconnected with other crimes.[382] None of the prosecutions were against law enforcement officers.[383] In California, research has uncovered only five convictions for violation of the old Penal Code sections on electronic surveillance, and again, all were against private parties.[384]

---

377. *See id.* at 761, 290 P.2d at 857.

378. "In a government of laws, existence of the government will be imperilled if it fails to observe the law scrupulously. Our Government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the Government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy." Olmstead v. United States, 277 U.S. 438, 485 (1928) (Brandeis, J., dissenting). *See also* Paulsen, *supra* note 347, at 76.

379. While a warrant should provide prima facie evidence of whom the search was directed against, ample opportunity should be given to any defendant to show that he was the actual target of the surveillance even though not named in the warrant.

380. California is the only jurisdiction to have abolished the standing requirement completely.

381. *See* Nardone v. United States, 302 U.S. 379 (1937).

382. Professor Westin reported that up to 1963 there had been 15 federal prosecutions against private wiretappers, 14 of them successful. PRIVACY AND FREEDOM, *supra* note 1, at 192. This author has been able to find only nine reported prosecutions, none of which took place after 1963.

383. "Research has failed to uncover a single reported prosecution of a law enforcement officer for violation of § 605 since that statute was enacted." Lee v. Florida, 392 U.S. 378, 386 (1968).

384. There are four reported appellate cases: People v. Trieber, 28 Cal. 2d 657,

Both the California Privacy Act and the Crime Control Act provide substantial penalties for wiretapping, eavesdropping, and the manufacture or distribution of surveillance equipment.[385] But, impressive as this array of penal sanctions may appear, there is little reason to believe that criminal penalties will be any more effective than they have been in the past.

There are several reasons for the ineffectiveness of criminal penalties in deterring illegal surveillance. The problem of detection, mentioned previously,[386] is probably the factor most responsible for the small number of prosecutions against private parties. However, even in private violations, prosecutorial and investigatorial reluctance probably plays a role. It is only natural that police would be less than zealous in investigating activities in which they themselves were also engaged. Also, where private snoopers are employed to perform law enforcement surveillance, prosecutors might be reluctant to act on complaints against those upon whose services they rely.[387]

As for law enforcement officers, the dearth of successful prosecutions is easily explained. Prosecutors do not often initiate actions against the police, upon whom they depend for their investigations. Even when a prosecution is initiated, juries are reluctant to convict one whose only failure was an overzealous effort to detect crime. These problems are, for the most part, inherent in our system of criminal justice administration, and it is unlikely that criminal sanctions, outside of their moral force, will ever prove very effective.[388]

---

171 P.2d 1 (1946); People v. Potter, 240 Cal. App. 2d 621, 49 Cal. Rptr. 892 (1966); People v. Snowdy, 237 Cal. App. 2d 677, 47 Cal. Rptr. 83 (1965); People v. Abbey, 223 Cal. App. 2d 514, 35 Cal. Rptr. 784 (1963). In addition, the conviction of a private investigator named Russell Mason was reported in THE EAVESDROPPERS, *supra* note 4, at 208, and three prosecutions and two arrests were reported in PRIVACY AND FREEDOM, *supra* note 1, at 205.

385. The standard penalty in California is a fine of up to 2,500 dollars, or imprisonment for up to three years, or both, for the first offense and a fine of up to 10,000 dollars, or imprisonment for up to five years, or both, for subsequent offenses. CAL. PENAL CODE §§ 631(a), 632(a), 634, 635(a) (West Supp. 1968). An exception is *id.* § 636, violation of which is punishable as a felony—imprisonment not exceeding five years. *See id.* § 18.

The standard sanction provided by the federal scheme is a fine of up to 10,000 dollars, or imprisonment for up to five years, or both. *See* 18 U.S.C. §§ 2511(1), 2512(1) (Supp. IV, 1965-68).

California also makes trespassing for the purpose of violating the surveillance laws a separate offense. CAL. PENAL CODE § 637 (West Supp. 1968).

386. See note 348 *supra* and accompanying text.

387. See note 223 *supra* and accompanying text.

388. The moral force of statutory prohibitions should not be underestimated. The mere existence of a prohibitory statute serves as a salutary deterrent even where few prosecutions are forthcoming. *See* Beaney, *supra* note 13, at 267 & n.54. The Regan Committee investigating electronic surveillance activities in California found

### C. Civil Remedies

Although the possibility of recovering damages for at least some types of electronic surveillance has existed for some time,[389] the civil damage suit has proved to be an elusive remedy, both in terms of deterring unlawful conduct and of redressing injuries. The problem of detection is again partly responsible, and the difficulty of proving damages has undoubtedly discouraged many prospective plaintiffs. Although most courts have indicated a willingness to give awards for mental anguish,[390] proving actual damage from so nebulous a thing as the overhearing of a conversation is still a highly speculative endeavor.[391] Where recovery is sought against a law enforcement officer, the plaintiff encounters the special obstacles common to all tort actions against police officers.[392] The problems of the unattractive plaintiff,[393] the unsympathetic jury,[394] and the impecunious defendant[395] are usually present in varying degrees. The combination of these factors has resulted in few successful recoveries.[396]

---

that, as a result of the adoption of the exclusionary rule, there was a significant decrease in the amount of surveillance performed by California law enforcement agencies. *See* REGAN COMM. REPORT, *supra* note 125, at 16.

389. As early as 1931, a Kentucky court held that a cause of action for invasion of privacy would lie for wiretapping. Rhodes v. Graham, 238 Ky. 225, 37 S.W.2d 46 (1931); *accord* McDaniel v. Atlanta Coca-Cola Bottling Co., 60 Ga. App. 92, 2 S.E.2d 810 (1939) (electronic eavesdropping). In 1947, section 605 of the Communications Act of 1934 was interpreted as giving rise to a civil cause of action against a violator. Reitmeister v. Reitmeister, 162 F.2d 691 (2d Cir. 1947). However, there are no reported recoveries under section 605, and a recent case from the same court indicates that the cause of action was available only against private violators. *See* Guido v. City of Schenectady, 404 F.2d 728 (2d Cir. 1968). There are no California decisions authorizing recovery, but, since California recognizes invasion of privacy as an actionable tort, there is little doubt that electronic surveillance would be actionable, even exclusive of statute.

Although again there are no reported recoveries, an action could be brought under 42 U.S.C. § 1983 (1964) for deprivation of constitutional rights. Until *Katz*, however, such actions were largely foreclosed by the trespass requirement. *See* Craska v. New York Tel. Co., 239 F. Supp. 932 (N.D.N.Y. 1965).

390. *See generally* PRIVACY AND FREEDOM, *supra* note 1, at 344-49.

391. *See, e.g,* LeCrone v. Ohio Bell Telephone Co., 120 Ohio App. 129, 201 N.E.2d 533 (1963); McDaniel v. Atlanta Coca-Cola Bottling Co., 60 Ga. App. 92, 2 S.E.2d 810 (1939); Rhodes v. Graham, 238 Ky. 225, 37 S.W.2d 46 (1931).

392. *See generally* Wolf v. Colorado, 338 U.S. 25, 41-44 (1949) (Murphy, J., dissenting); Foote, *Tort Remedies for Police Violations of Individual Rights*, 39 MINN. L. REV. 493 (1955); Paulsen, *supra* note 347, at 72-76.

393. Although the typical plaintiff in an electronic surveillance case would probably tend to be a more substantial citizen than the average victim of an unlawful search, many victims will still be from lower social and economic brackets, and all are accused, if not already convicted, of a crime.

394. Jury sympathy would normally tend to be on the side of a policeman who was merely attempting, albeit too eagerly, to enforce the law.

395. Police officers are seldom men of great wealth. *See* Foote, *supra* note 392, at 499.

396. The exact number of civil recoveries is not known, but appellate cases author-

Perhaps spurred on by prosecutorial inertia and the failure of criminal sanctions, both Congress and the California Legislature attempted to breathe new life into this remedy. In their respective statutes each created a statutory cause of action and guaranteed a minimum damages award to the successful plaintiff. In addition, the California statute provides for treble damages, and the federal scheme offers punitive damages, actual damages, and attorneys' fees.[397] It is hoped that these innovations will bolster the effectiveness of this remedy by eliminating the necessity for proving damages and by furnishing an incentive for private law enforcement. Because they are to some extent punitive, these provisions may also prove to be a more effective deterrent.[398]

In order to maximize the effectiveness of the damage suit as a deterrent to unlawful police surveillance, it has been urged that a cause of action should also lie against the governmental unit employing the violator.[399] This might be either in addition to, or in lieu of, a suit against the offender himself. Such governmental liability serves two important purposes. It maximizes the incentive value of the remedy

---

izing recovery for an electronic invasion of privacy number less than eight. *See* cases collected in Annot., 11 A.L.R.3d 1296 (1967). There is no record of a successful civil suit having been brought in California, although the filing of a suit is reported in PRIVACY AND FREEDOM, *supra* note 1, at 206.

397. 18 U.S.C. § 2520 (Supp. IV, 1965-68):

> Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communication, and (2) be entitled to recover from any such person—
>
> (a) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;
>
> (b) punitive damages; and
>
> (c) a reasonable attorney's fee and other litigation costs reasonably incurred.

CAL. PENAL CODE § 637.2 (West Supp. 1968):

> (a) Any person who has been injured by a violation of this chapter may bring an action against the person who committed the violation for the greater of the following amounts:
>
> (1) Three thousand dollars ($3,000).
>
> (2) Three times the amount of actual damages, if any, sustained by the plaintiff.
>
> (b) Any person may . . . bring an action to enjoin and restrain any violation of this chapter, and may in the same action seek damages. . . .
>
> (c) It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages.

398. One apparent purpose of the California treble damage provision was to deter industrial espionage by making the penalty exceed the probable advantage to be gained from surveillance. *See* Digest of A.B. 860, *supra* note 120.

399. *See* 3 K. DAVIS, ADMINISTRATIVE LAW TREATISE § 26.07 (1958); Barrett, *supra* note 352, at 592-95; Foote, *supra* note 392, at 514-15. *But see* Paulsen, *supra* note 347, at 73 (doubting that substantial awards would be given in practice).

by guaranteeing a financially responsible defendant, and it exerts the deterrent effect at the point where it presumably is most effective—at the level where surveillance policies are formulated.[400]

This result is accomplished in part in California by statutory provisions which make public entities responsible for injuries caused by their employees.[401] However, this liability does not extend to punitive or exemplary damages,[402] so the benefits of governmental liability are greatly limited. Although a sympathetic court might interpret the 3,000 dollar minimum recovery[403] as liquidated damages rather than a penalty, any treble damages would almost certainly be characterized as punitive. This could be remedied by amending section 818 of the Government Code[404] to make public entities liable for all statutory damages under the Privacy Act. Most states would require a similar abrogation of governmental immunity to reach this result.[405]

California also provides for injunctive relief to terminate an interception or other violation.[406] It is unlikely that this remedy would often be needed to force cessation of surveillance as mere discovery would normally bring it to a halt.[407] However, the injunction can be an important tool to restrain the use of unlawfully intercepted information, as in cases of industrial espionage.[408]

---

400. *See* 3 K. DAVIS, *supra* note 399, § 25.17 at 120 (Supp. 1965); Barrett, *supra* note 352, at 595; Foote, *supra* note 392, at 514-15.

401. CAL. GOV'T CODE § 815.2 (West 1966). The limitation on the liability to acts performed within the scope of employment would leave a law enforcement officer individually responsible for violations unrelated to his police function, such as blackmail or extortion.

402. *Id.* § 818: "Notwithstanding any other provision of law, a public entity is not liable for damages . . . imposed primarily for the sake of example and by way of punishing the defendant."

403. See note 397 *supra.*

404. See note 402 *supra.*

405. Although sovereign immunity for the torts of governmental agents is on the wane, a majority of jurisdictions still embrace the doctrine to some degree. *See* 3 K. DAVIS, *supra* note 399, at § 25.01 (Supp. 1965). And many of those which have abolished immunity have, like California, retained some type of limitation on damages. *See,* e.g., ILL. ANN. STAT. ch. 85, § 2-102 (Smith-Hurd 1966) (no punitive damages); MINN. STAT. ANN. § 466.04(1) (1963) ($50,000 per claim maximum and no punitive damages).

406. CAL. PENAL CODE § 637.2(b) (West Supp. 1968), quoted in note 397 *supra.* The federal statute does not provide for injunctive relief, and the legislative history indicates that it was not intended that it should be available. *See* SENATE REPORT, *supra* note 95, at 107.

407. If the subject of the surveillance becomes aware of its existence, he can normally take precautions to render the surveillance ineffective, thus making continuation impractical.

408. Another form of injunctive relief is also available in California. In Wirin v. Parker, 48 Cal. 2d 890, 313 P.2d 844 (1957), a taxpayer successfully enjoined the Los Angeles Chief of Police from expending public funds for the conduct of illegal surveillance.

An additional sanction, created by the Crime Control Act, which should be incorporated into state schemes is the confiscation of surveillance equipment.[409] While its range of effectiveness is rather limited,[410] it could be a potent sanction against professional eavesdroppers, whose equipment can run into many thousands of dollars,[411] and manufacturers or sellers, whose inventory could be seized.[412] Not only does it impose a fiscal penalty which may well be more severe than the statutory fine, it removes the equipment from circulation, preventing its further use.

California has created one additional penalty to curb the use of surveillance equipment by private investigators. Private detectives have been responsible for a major share of electronic snooping in the past, particularly in domestic relations cases.[413] Section 7551 of the Business and Professions Code provides that a private investigator's license can be suspended or revoked for violations of the surveillance laws.[414] This sanction suffers from the same limitations as criminal penalties, since it operates only upon criminal conviction. But the prospect of a loss of license and livelihood might be a more effective deterrent than the possibility of facing a relatively light prison sentence.

### *D. Manufacture and Distribution of Surveillance Devices*

In addition to imposing criminal and civil sanctions on various types of illicit electronic surveillance, both the state and federal statutes have attempted to attack the problem at an earlier stage by depriving the eavesdropper of the tools of his trade. The California Privacy Act and title III both prohibit the manufacture, sale, transportation, possession or advertising of devices designed primarily for use in surreptitious electronic surveillance.[415] These provisions are a desirable part of any regulatory program, but their value should not be overestimated. Despite the sophisticated gadgetry available for snooping today most electronic surveillance is still accomplished by relatively simple devices which also have considerable utility in legitimate roles.[416] Except for

409. 18 U.S.C. § 2513 (Supp. IV, 1965-68): "Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States."

410. For the casual or one-time snooper utilizing inexpensive equipment, this sanction is not significant compared to the possibility of criminal and civil liability.

411. *See* THE EAVESDROPPERS, *supra* note 4, at 210 (investigator's equipment worth $50,000); *id.* at 213 (equipment valued at $20,000).

412. *See* SENATE REPORT, *supra* note 95, at 95.

413. *See* REGAN COMM. REPORT, *supra* note 125, at 11.

414. CAL. BUS. & PROF. CODE § 7551(m) (West Supp. 1968).

415. CAL. PENAL CODE § 635 (West Supp. 1968); 18 U.S.C. § 2512 (Supp. IV, 1965-68).

416. *See* THE EAVESDROPPERS, *supra* note 4, at 306; THE INTRUDERS, *supra* note

those devices which are blatantly promoted for snooping, it is difficult to characterize most of this equipment as being primarily useful for surreptitious electronic surveillance.[417] Despite the difficulties in enforcement, however, this type of regulation should at least keep some equipment out of the hands of amateur snoopers who lack the technical expertise to manufacture their own equipment from common components.[418]

## CONCLUSION

In the past three years, the Supreme Court and the Congress have taken significant steps to close the gap between law and technology and create a meaningful right to privacy from electronic snooping. Even the states, long dormant in this area, are beginning to move on the problem. More action has been taken in the last three years than in the preceding 30. Yet there remains much to be done. The Crime Control Act, comprehensive though it is, is not without weaknesses; its permissiveness with respect to law enforcement surveillance and the virtual exclusion of participant monitoring make it far from perfect. And although it at last achieves a degree of national standardization, it is no substitute for state laws—the burden of day-to-day policing of invasions of privacy will still fall to the states. The federal law should, however, provide an impetus to states to reexamine their own laws. Even states like California which have fairly recent legislation on the subject may already need to revise their laws to meet the new federal standards.

The California scheme, although innovative in some respects was in large part dated when it was passed, and it has since become more obsolete. It is unduly complex and confusing and could well be replaced by a more straightforward scheme. With title III, the *ABA Standards*, and other recent state legislation to draw upon, California has the means to create a model surveillance law. It also has the opportunity. A joint legislative committee has undertaken a complete revision of the California Penal Code. Although the project unfortunately was sidetracked temporarily because of political pressure, it apparently will be completed. Hopefully, the committee will make the

4, at 65; Note, *A Proposal for Legislative Control of Electronic Surveillance*, 43 IND. L.J. 130, 135-37 (1967).

417. *See* ABA STANDARDS, *supra* note 5, at 108; Note, *supra* note 416, at 135-37.

418. A ban on the manufacture and sale of snooping devices should not seriously hamper the professional eavesdropper because most of them are capable of building their own equipment and often do so. *See* THE EAVESDROPPERS, *supra* note 4, at 76, 210, 213, 306. However, the curiosity seeker or the irate husband who is trying to check up on his wife no longer has the former dazzling array of inexpensive devices at his disposal, and his lack of technical expertise will probably keep him out of the snooping business altogether.

most of this opportunity to keep California in the forefront in protecting the privacy of its citizens.

*H. Lee Van Boven*