

JUN 26 1973

MEMORANDUM FOR THE ATTORNEY GENERAL

Re: National security electronic surveillances

This is in response to a memorandum from your office asking for an analysis of the state of the law regarding national security electronic surveillance. This memorandum will discuss (I) whether the Government presently has the power under the Constitution to engage in electronic surveillance without a warrant; (II) the scope of that power, and (III) what legal alternatives may be available.

I.

A year ago in the Keith case, */ the Supreme Court ruled unanimously that electronic surveillance in domestic as opposed to foreign intelligence matters could not be accomplished without a warrant. **/

The Court held that (1) the Omnibus Crime Control and Safe Streets Act (18 U.S.C. § 2511(3)) did not give the Executive authority to conduct warrantless national security electronic surveillances but merely disclaimed any intent to interfere with that power to the extent

*/ United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297 (1972). Keith was the District Judge in the case who was the subject of a petition for a writ of mandamus by the Government after he ruled that the surveillance carried out was unlawful.

**/ Immediately thereafter, Attorney General Kleindienst announced that in accordance with that decision the Department would terminate all electronic surveillance in cases involving domestic security that conflict with the Keith case. (Statement of June 19, 1972.)

that it might exist, */ and (2) the Fourth Amendment (which shields private speech from unreasonable surveillance) requires prior judicial approval for domestic security surveillance.

The Court also said in Keith that "the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers within or without this country." 407 U.S. at 308; see also 321-22. The question arises therefore as to what view this Department should take of the law in light of this disclaimer.

In this connection the following should be noted:

(1) There is a fairly substantial body of opinion in the lower courts upholding, without exception, the power of the Government to engage in electronic surveillance in foreign intelligence cases without a warrant. In the absence of a definitive ruling by the Supreme Court it seems that, as a legal matter, the Department can point to these opinions as justifying continued warrantless surveillance of this kind. These opinions are United States v. Clay a/k/a Ali (S.D. Tex. 1969, Cr. No. 67-H-94, unreported), affirmed, 430 F. 2d 165 (5th Cir. 1970), reversed on other grounds 403 U.S. 698 (1971); United States v. Butenko,

*/ "Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents (continued)

318 F. Supp. 66 (D.N.J. 1970), appeal pending (3d Cir., No. 72-1741); United States v. Smith, 321 F. Supp. 424 (C.D. Calif. 1971) (dictum); United States v. Brown, 317 F. Supp. 531, 536 (E.D. La. 1970); United States v. O'Baugh, 304 F. Supp. 767 (D.D.C. 1969); United States v. Stone, 305 F. Supp. 75 (D.D.C. 1969); United States v. Dellinger, (N.D. Ill. 1970, No. 69 CR 180, unreported); United States v. Enten, (D.D.C., 1971, Crim. No. 166-71, unreported) appeal pending (D.C. Cir. No. 71-1774); United States v. Hoffman, (D.D.C., 1971, Criminal No. 973-71, unreported).

In general, these cases rely either explicitly or implicitly on the view that the surveillances are authorized by the constitutional power of the President as Commander-in-Chief and as the Nation's organ for foreign affairs and that the courts are not equipped to decide what is and what is not a threat to national security. Cf. Chicago & Southern Airlines v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948).

(2) There may be an opportunity for the Supreme Court to rule on this matter at some time in the future. There are two cases which have been briefed and argued and await decision in the appellate courts, one in the Third Circuit and one in the U.S. Court of Appeals for the District of Columbia, both of which present the foreign intelligence issue squarely (United States v. Butenko and Ivanov, No. 72-1741, 3rd Cir.; United States v. Enten, No. 71-1774, D.C. Cir.). There is, of course, no assurance that the Supreme Court will take the opportunity, should it arise. As in Keith, the Supreme Court in the past has avoided opportunities to rule on the issue. After the Fifth Circuit

*/ (cont'd) of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power."

ruled in the Clay case in 1970 that electronic surveillance for foreign intelligence purposes was lawful (United States v. Clay, supra), certiorari was granted on issues other than surveillance and the decision below was reversed by the Court on other grounds. In United States v. Katz, 389 U.S. 347 (1967), the Court held that electronic surveillance was covered by the Fourth Amendment but, at the same time, specifically noted that it was not ruling on situations involving national security. 389 U.S. at 358, note 23.

(3) There are indications that the Supreme Court at best will be divided on the issue and it is possible that a majority might rule against the Department.

Three Justices now sitting appear to have already expressed their views on this issue. In Katz, supra, where electronic eavesdropping was held covered by the Fourth Amendment, Justices Douglas and Brennan stated forcefully in a concurring opinion that the Fourth Amendment prohibited national security surveillance without a warrant (389 U.S. at 359), while Justice White, in a separate concurrence took the opposite view (389 U.S. at 362).

The Douglas-Brennan opinion stated:

Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be. Under the separation of powers created by the Constitution, the Executive Branch is not supposed to be neutral and disinterested. Rather it should vigorously investigate and prevent breaches of national security and prosecute those who violate the pertinent federal laws. The President and Attorney General are properly interested parties, cast in the role of adversary, in national security cases. They may even be the intended victims of subversive action. Since spies and saboteurs are as entitled to the protection of

the Fourth Amendment as suspected gamblers like petitioner, I cannot agree that where spies and saboteurs are involved adequate protection of Fourth Amendment rights is assured when the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate. (389 U.S. at 359).

Clearly, the argument that electronic surveillance without warrant is necessary for counter-intelligence or similar matters is not going to sit well with these two members of the Court.

Moreover, the reasoning in the Keith case itself suggests that the Court may not be readily persuaded of the Government's case. Although it is true that the Court specifically reserved the foreign intelligence issue, at no point did it volunteer any reasons as to why, as a matter of constitutional law it might be willing to make this distinction when presented with a proper case. To the contrary, the reasoning in Keith seems to anticipate and reject arguments the Department is making at this time in the "foreign intelligence" cases in the lower courts. Thus, in the case pending in the Third Circuit the Department has presented the following arguments why judicial approval should not be required for foreign intelligence surveillance (Brief for Appellee, United States v. Butenko and Ivanov, Docket No. 72-1741, pp. 34-34.):

(a) Information on which such surveillance is based is highly confidential and must be kept secret.

(b) Sensitive information is "simply not susceptible of evaluation by persons who do not regularly deal with foreign affairs matters."

(c) In foreign intelligence surveillances, "the justification * * * cannot be simply stated or easily demonstrated;" it requires the drawing of subtle inferences. Almost without exception there is no known criminal activity involved as such.

The opinion in Keith appears to respond to the listed arguments with the following:

(a) As to secrecy: "The investigation of criminal activity has long involved imparting sensitive information to judicial officers who have respected the confidentialities involved. Judges may be counted upon to be especially conscious of security requirements in national security cases. [The 1968 electronic surveillance statute] already has imposed this responsibility on the judiciary in connection with such crimes as espionage, sabotage, and treason * * *, each of which may involve domestic as well as foreign security threats. Moreover, a warrant application involves no public or adversary proceedings: it is an ex parte request * * *. Whatever security dangers clerical and secretarial personnel may pose can be minimized by proper administrative procedures, possibly to the point of allowing the Government itself to provide the necessary clerical assistance." 407 U.S. at 320-21.

(b) As to complexity and the need for sophistication: "We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. Courts regularly deal with the most difficult issues of our society. * * * security surveillance involves different considerations from the surveillance of 'ordinary crime.'" 407 U.S. at 320.

The Court also suggested that in "sensitive cases," authorizations might be made by a designated court, such as the Court of Appeals for the District of Columbia. 407 U.S. at 323. Although the Court did not explicitly say so, one implication is that if all foreign intelligence applications were made to the same court, it might be more difficult for the Government to argue that the court lacked the necessary background to understand them.

(c) As to the difficulty of justification and the absence of conventional criminal activity, the Court said: "Different standards may be compatible with the Fourth Amendment if they were reasonable both in relation to the legitimate need of Government for intelligence information

and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection." 407 U.S. at 322-23. In support, the Court cited its recent decision holding that a health official need not show the same kind of proof to a magistrate to obtain a warrant as one who would search for the fruits of crime. Camara v. Municipal Court, 387 U.S. 523 (1967).

The Court made the following additional points in Keith which suggest that it may not readily recognize an exception to the warrant clause of the Fourth Amendment even for foreign intelligence:

(a) The use of electronic surveillance is not a welcome development "even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens." (407 U.S. at 312).

(b) "Though physical entry of the home is the chief evil against which the * * * Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance. * * * [B]road and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate Fourth Amendment safeguards." (407 U.S. 313.)

(c) "National security cases * * * often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech." (407 U.S. 313).

(d) "Inherent in the concept of a warrant is its issuance by a 'neutral and detached magistrate.' * * * The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." 407 U.S. at 316-17.

As we noted earlier, we believe that the Department is justified in continuing to rely on the clear weight of the case law until the Supreme Court rules otherwise. However, close analysis of Katz and Keith suggests that the ultimate decision of the Court may be against the position the Department is now arguing.

II.

The next question which arises relates to defining the scope of surveillance that may still be carried on without a warrant after Keith.

At the outset, we note that the Omnibus Crime Control and Safe Streets Act of 1968 merged procedures for obtaining warrants for wiretapping and microphone surveillance or bugging. 18 U.S.C. 2510. The statement of facts in Keith shows that wiretapping was there involved. 407 U.S. at 300. However, the Court uses the generic term "electronic surveillance" throughout its opinion. The Court has also indicated that it sees no distinction in constitutional principle between the two (cf. Katz v. United States, 389 U.S. 347 (1967)), and we therefore use the term "electronic surveillance" here to include both wiretapping and bugging.

The 1968 Act stated that Congress did not intend to interfere with the constitutional power of the President. 18 U.S.C. 2511(3). The Act purported to describe the possible outlines of that power in the light of the criteria set out below, leaving it to the courts to resolve the issues involved. See Keith at 407 U.S. 301-308. As noted, Keith held that 18 U.S.C. 2511(3) is not in itself a grant of authority to conduct warrantless national security surveillances and that there is no power to conduct such surveillance in domestic security situations.

We are thus left with the "foreign security" criteria in 18 U.S.C. 2511(3), which have not been discussed by the Supreme Court and which relate to presidential power necessary: (1) to protect the nation against actual or potential attack or other hostile acts of a foreign power;

(2) to obtain foreign intelligence information deemed essential to the security of the United States; or (3) to protect national security information against foreign intelligence activities. 18 U.S.C. 2511(3).

The Court said these criteria, as they appear in § 2511(3), are an expression of neutrality rather than a measure of executive authority. 407 U.S. at 308. However, they are not totally neutral since they can be read as setting outer limits on possible constitutional power in this area. Section 2511(3) is, in effect, an exception from prohibitions in the 1968 Act and the Communications Act. Failure to bring surveillances within the rubric of § 2511(3) would seem to make them illegal per se under the general prohibitions relating to electronic surveillance found in 18 U.S.C. 2510-20. See White, J., concurring in Keith (407 U.S. at 335).

Keith itself provides other limits which relate more to the nature of the subjects of surveillance rather than to ultimate purpose (which is the focus of 18 U.S.C. 2511 (3)). Thus the Court made clear that the surveillance power described may not be used against "domestic organizations" which have "no significant connection with a foreign power, its agents or agencies." 407 U.S. at 309, note 8. The lower court decisions, which are all pre-Keith, do not make any further distinctions along this line. This Department has publicly placed the following gloss on these words:

"We do not interpret this as meaning casual, unrelated contacts and communications with foreign governments or agencies thereof. We would not try to apply this standard without the presence of such factors as substantial financing, control by or active collaboration with a foreign government and agencies thereof in unlawful activities directed against the Government of the United States."

(Statement by Kevin Maroney, Deputy Assistant Attorney

General, Internal Security Division, on Electronic Surveillance before Senate Subcommittee on Administrative Practice and Procedure, June 29, 1972). Presumably, this means that before electronic surveillance power is used against groups composed of citizens a rather clear showing of possible law violation must be shown. When dealing with purely foreign entities, the only limits, as of now, are those found in § 2511(3).

III.

The Department now has a number of alternatives which it may follow:

(1) It can continue the existing policy of engaging in electronic surveillance for foreign intelligence purposes without a warrant. The difficulty with this posture is its uncertainty. Before a final decision is made by the Supreme Court, there may be several years of remands and hearings to determine whether electronic surveillance is foreign or domestic within the meaning of Keith. This may be time consuming and, since illegal taps and bugs must be disclosed (Alderman v. United States, 394 U.S. 165 (1969)), embarrassing. Even if the Supreme Court does ultimately hold that there are exceptions to the Fourth Amendment for foreign intelligence surveillance there is no assurance that the warrant exception will be as wide in scope as what is suggested by 18 U.S.C. 2511(3).

If the Government loses in the Supreme Court, the fall-out may be extensive since each tap or bug is capable of picking up hundreds of subjects. As past cases demonstrate, there is no such thing as a "purely foreign" tap since citizens who later become involved as defendants are also picked up. See e.g., United States v. Clay, supra. The recent Watergate hearings have even revealed an instance of a defendant deliberately making calls to embassies whose lines he believed tapped in order to complicate matters for the prosecution.

One of the arguments raised against obtaining warrants

is the possibility that there will be security leaks. However, it can be argued that as long as the legality of this surveillance remains in a gray area, the necessary hearings and inspections (both in camera and in open court) and the proliferation of private suits will actually produce more leaks and more publicity than any system for obtaining warrants.

(2) There are a number of possibilities for obtaining warrants for surveillance for foreign intelligence purposes. .

(a) Title III of the Omnibus Crime Control and Safe Streets Act now authorizes warrants for such crimes as espionage, sabotage, and treason. 18 U.S.C. 2516(1)(a) and (c). It may be that there are cases where a warrant could be obtained under Title III but where warrantless surveillance is now used instead. In applications to the Attorney General for warrantless surveillance perhaps an explanation should be included as to why Title III is not being used.

(b) It is possible that without new legislation the courts will grant warrants for electronic surveillance under standards less onerous than Title III. In Osborn v. United States, 385 U.S. 323, 328-311 (1966), judicial approval was obtained for electronic surveillance even though no statute or rule authorized such a procedure at the time. Similarly, following Camara, supra, 387 U.S. 523, which held that warrants were necessary for administrative inspections, the Bureau of Narcotics and Dangerous Drugs succeeded in getting some courts to issue administrative warrants although legislation authorizing them had not yet been enacted. The Keith (407 U.S. at 322-23) and Camara (387 U.S. at 534-35) cases seem to indicate that the Court would rather make the

warrant requirement flexible than create exceptions to it. Mr. Maroney's statement of June 29, 1972, (quoted in Part II) indicates that, at least in cases involving United States citizens or groups, there must be evidence of "unlawful activities directed against the Government of the United States." Therefore, it may well be possible to demonstrate to a court something akin to conventional notions of probable cause when requesting warrants in this type of case.

(c) Another possibility is legislation specifically authorizing the kind of procedure contemplated under (b). In Keith the Court suggested that procedures with standards different from those in Title III could be enacted for domestic intelligence purposes. (407 U.S. at 322.) Presumably, the same reasoning would support legislation with standards that are less rigorous than Title III in the foreign intelligence field.

Since our Office has never seen the applications for electronic surveillance submitted to the Attorney General and since we have no specific knowledge of cases now pending and the problems they present, we cannot make any firm recommendation as to how the Department should proceed. We suggest only that a risk-benefit analysis based on a hard appraisal of the legal situation may well prove useful to the Department in the long run.

Robert G. Dixon, Jr.
Assistant Attorney General
Office of Legal Counsel