Transmission by a Wireless Carrier of Information Regarding a Cellular Phone User’s Physical Location to Public Safety Organizations

Neither 47 U.S.C. §1002(a) nor the Fourth Amendment of the Constitution prohibits a wireless carrier’s transmission to local public safety organizations of information regarding the physical location of a caller who uses a cellular telephone to dial the 911 emergency line.

Although 18 U.S.C. §2703 would apparently apply to the carrier’s transmission of such location information to public safety organizations, the caller, by dialing 911, has impliedly consented to such disclosure, thus permitting the federal government to require the carrier to disclose such information without a warrant or court order.

September 10, 1996

MEMORANDUM OPINION FOR THE ACTING ASSISTANT ATTORNEY GENERAL CRIMINAL DIVISION

You have asked for our opinion as to whether 47 U.S.C. §1002(a) prohibits a wireless carrier’s transmission to local public safety organizations of information regarding the physical location of a caller who uses a cellular telephone to dial the 911 emergency line. In addition, you have inquired as to the constraints, if any, imposed by the Fourth Amendment on such a transmission. As set forth in detail below, we conclude that §1002(a), by its terms, does not prohibit such transmission of location information. Although you have not inquired as to the applicability of 18 U.S.C. §2703(c), we conclude that, while the provision would apparently apply to the carrier’s transmission of such location information to public safety organizations, the caller, by dialing 911, has impliedly consented to such disclosure, thus permitting the federal government to require the carrier to disclose such information without a warrant or court order. Finally, the Fourth Amendment does not prohibit such transmission both because of the caller’s implied consent to the disclosure and because a caller who dials 911 has neither an actual nor a reasonable expectation of privacy with regard to his whereabouts at the time of the call.

1 Memorandum for Walter E. Dellinger, Assistant Attorney General, Office of Legal Counsel, from John C. Keeney, Acting Assistant Attorney General, Criminal Division, Re: Request for a Legal Opinion from the Federal Communications Commission as to the Applicability of 47 U.S.C. §1002(a) to the Transmission to Local Public Safety Agencies of the Physical Location of a Cellular Telephone Caller Who Dials the 911 Emergency Line (May 13, 1996).
Opinions of the Office of Legal Counsel in Volume 20

BACKGROUND

A. Facts

In its recently issued rule regarding Compatibility of Wireless Services With Enhanced 911 ("E-911"), the Federal Communications Commission (the "FCC") established a timetable for the development and deployment of new technologies through which wireless carriers (cellular telephone companies) will automatically provide a designated public safety answering point ("PSAP") with information regarding the physical location of a caller who dials 911 on a wireless cellular telephone. See id. §20.18. This information will significantly enhance the effectiveness of wireless 911 services by helping emergency service personnel locate the caller and more rapidly and accurately determine where the emergency has occurred.

The implementation and deployment of enhanced 911 features and functions will be accomplished in two phases. In phase one, covered carriers must relay to the PSAP the 911 caller's telephone number and the location of the cell site or base station through which the call originates. See id. §20.18(d). This information will identify the caller's location only in quite general terms, but will enable emergency service providers to call back if a 911 call is disconnected. See id. We understand that the information provided in phase one is currently available to wireless carriers, as it is regularly captured by them as part of their transmission of calls from cellular phones, but some carriers must develop the ability to pass it on to a third party.

A more precise identification of the caller's location will occur in phase two, when the carrier must provide the designated PSAP with the physical location of the mobile unit making the call by longitude and latitude within a radius of 125 meters in 67% of all cases. See id. §20.18(e). According to FCC representatives, the more precise location determination required in phase two will occur

---

2 A public safety answering point is a facility designated to receive 911 calls and route them to emergency service personnel. See 47 C.F.R. §20.3.

3 An E-911 system automatically identifies on a screen at the PSAP the telephone number and geographical location from which the call was made. This system permits a more efficient response to calls received, including silent calls, and deters false alarms, because such calls are capable of being traced. In many jurisdictions, E-911 systems are already operational for landline phones, identifying the telephone number and the address associated with that telephone number. The address of the subscriber to the cellular telephone will often be insufficient to identify the caller's physical location at the time of a call, however, because cellular telephones are mobile and calls are frequently made from someplace other than the caller's address. The need for this critical information regarding the location of the caller was the impetus for the new FCC rule.

4 The physical size of a cell depends upon the density of use: it could encompass only a few blocks in a populated city, or miles in a rural area.

5 When a cellular caller makes a call, the carrier captures his signal (his electronic serial number) and the data carried on that signal, which is generally a mobile identification number ("MIN"). A MIN is a 34-bit binary number that a cellular handset transmits as part of the process of identifying itself to wireless networks. Each handset has one MIN, which is derived from the ten-digit North American Numbering Plan telephone number that is generally programmed into the handset by a provider when it initiates service for a new subscriber. See id. §20.18. The carrier's records include transactional information, such as the caller's address, associated with the MIN.
through the development of new technologies enabling the carrier to combine and analyze information regarding the strength, angle and timing of the caller's signal measured at two or more cell sites. A caller's signal, and its strength, are already often picked up by more than one cell site. In addition, many cell sites have sectorized antennas, and, depending upon the angle of the signal’s arrival, a particular antenna will pick up the signal, thus informing the carrier what sector of the cell the caller is located in. Finally, each site records the arrival time of a signal. By developing new computer programs, switching technology, protocols and network architecture, the carrier will be able to combine and analyze all of this information—the strength of the signal at each of the cell sites picking up the signal, the sector of a cell from which a signal emanates, and the time that it takes for the signal to arrive at one cell site compared to other sites—to identify more precisely the caller’s location.

B. Relevant Statutory Provisions

The Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), among other things, requires telecommunications carriers to ensure that their equipment is capable of permitting the government (pursuant to a court order or other lawful authorization) to access certain "call-identifying information" 6 that is reasonably available to the carrier. 47 U.S.C. § 1002(a)(2). CALEA includes limitations, however, and specifically prohibits telecommunications carriers from providing the government with "information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18) . . . that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)." Id. § 1002(a)(2)(B). 7 Section 3127 of title 18 (part of the Electronic Communications Privacy Act of 1986 ("ECPA")) in turn prohibits the installation or use of pen registers and trap and trace devices absent a court order, with the exception of particular uses by providers of electronic or wire communication services. 8

6 "The term 'call-identifying information' means dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2).

7 18 U.S.C. § 3127 defines "pen register" and "trap and trace device" as follows:

(3) the term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

(4) the term 'trap and trace device' means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.

8 18 U.S.C. § 3121 provides in pertinent part: Continued
Another provision of ECPA, 18 U.S.C. § 2703, ‘‘Requirements for governmental access,’’ sets forth the terms under which carriers may provide governmental entities with information relating to electronic communications. In particular, § 2703(c) provides that a carrier shall only disclose a record or other information pertaining to one of its customers (excluding the contents of communications covered elsewhere in the section) to a governmental entity when the governmental entity obtains a warrant, a court order or the consent of the customer.9

ANALYSIS

A. Section 1002(a) Does Not Prohibit Wireless Carriers From Transmitting Information Regarding the Physical Location of Cellular Telephone Callers to Public Safety Agencies

By its terms, 47 U.S.C. § 1002(a)(2) does not prohibit a wireless carrier’s transmission of physical location information as required by the new FCC rule. As set forth above, § 1002(a)(2) only prohibits carriers from providing physical location information ‘‘acquired solely pursuant to the authority [under 18 U.S.C. § 3127] for pen registers and trap and trace devices.’’ The physical location of a cellular caller would not be obtained pursuant to legal authority requested and obtained by law enforcement officers as part of a government-initiated investigation, but instead pursuant to the recently issued FCC rule in response to an individual’s request for help. Indeed, the cellular caller’s physical location would not be determined by use of a pen register or trap and trace device at all,10 but rather

9 A provider of electronic communication service . . . shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity — (i) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; (ii) obtains a court order for such disclosure under subsection (d) of this section; or (iii) has the consent of the subscriber or customer to such disclosure.

10 Although pen registers and trap and trace devices would be used to obtain the caller’s telephone number and to relay the call to the PSAP, they would not provide any information on the actual physical location of the cellular caller.
Transmission by a Wireless Carrier of Information Regarding a Cellular Phone User's Physical Location to Public Safety Organizations

by advanced technologies that aggregate and analyze the strength and angle of the caller's signal measured at various cell sites. At the very least, it certainly cannot be said that the caller's physical location would be determined "solely" through use of a pen register or trap and trace device. 47 U.S.C. § 1002(a). Thus § 1002 does not prohibit a telecommunications carrier from transmitting to a public safety organization the physical location information pertaining to a cellular caller required by the FCC rule. 11

B. 18 U.S.C. § 2703 Permits Wireless Carriers to Transmit to Public Safety Authorities the Physical Location of Cellular Callers Dialing 911 Because Such Callers Have Impliedly Consented to Such Disclosure

As set forth above, 18 U.S.C. § 2703 requires wireless carriers to obtain a warrant, a court order or the consent of the customer before disclosing to governmental authorities information relating to such customer. Although the disclosure of information regarding the physical location of a customer would likely fall within this provision, it is our view that, by dialing 911, the caller impliedly consents to the disclosure of information regarding his location at the time of the call. 12

The whole purpose of a 911 call is to seek the aid of appropriate government officials in responding to an emergency at a particular place. Typically, that emergency is in the immediate vicinity of the caller — indeed, it often involves the caller himself and thus his exact location — and the whole purpose of the call

11 The legislative history of § 1002(a) supports our conclusion. As explained in the House Report (there was no Senate Report submitted with CALEA), Congress was acting to ensure that "the authority for pen registers and trap and trace devices cannot be used to obtain tracking or location information, other than that which can be determined from the phone number." H.R. Rep. No. 103-827, at 17 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3497; see also id. at 22, reprinted in 1994 U.S.C.C.A.N. at 3502 ("Call identifying information obtained pursuant to pen register and trap and trace orders may not include information disclosing the physical location of the subscriber sending or receiving the message, except to the extent that location is indicated by the phone number.") (emphasis added). "Currently, in some cellular systems, transactional data that could be obtained by a pen register may include location information." Id. at 17, reprinted in 1994 U.S.C.C.A.N. at 3497 (emphasis added).

12 Although there appear to be no cases interpreting §2703's consent provision, and the legislative history of the section is silent on the matter, some guidance can be found in analyses of the consent provision in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2511(2)(c). Section 2511(2)(c) provides in part that "[i]t shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where . . . one of the parties to the communication has given prior consent to such interception." According to the legislative history of §2511(2)(c), "[c]onsent may be expressed or implied." S. Rep. No. 90-1097, at 94 (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2182 ("Surveillance devices in banks or apartment houses for institutional or personal protection would be impliedly consented to."). "In the Title III milieu as in other settings, consent inheres where a person's behavior manifest acquiescence or a comparable voluntary diminution of his or her otherwise protected rights." Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990) (citations omitted). "[I]mplied consent — or the absence of it — may be deduced from 'the circumstances prevailing' in a given situation. . . . The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private." Id. at 117 (citation omitted). See also United States v. Amen, 831 F.2d 373, 378-79 (2d Cir. 1987) (no violation of Title III where tapping of prison inmates' telephone calls was impliedly consented to by inmates who used phones when on notice of the monitoring procedures at prison; "[h]ere we imply consent in fact from surrounding circumstances indicating that the appellants knowingly agreed to the surveillance") (citations omitted), cert. denied, 485 U.S. 1021 (1988).
is to inform officials of that location in order for the caller to obtain, and the emergency service officials to provide, help. The caller is the source of the location information needed by the government to respond, and his call evidences not merely an expectation, but in fact a purpose, of conveying that information to the authorities. If the caller himself does not tell the authorities where he is located (which he generally does), it is presumably due to the exigent circumstances resulting from the emergency, and not to any desire to withhold such information. Even if the emergency is in a different location, his decision to reach out to government officials to seek their help indicates that he would similarly tell them his location if it would help them respond to the emergency. The mere possibility that a caller subjectively does not wish his location to be revealed would not negate the consent presumed from his making the 911 call. 14

C. Wireless Carriers May Transmit to Public Safety Authorities Information Regarding the Physical Location of Cellular Callers Dialing 911 Without Violating the Fourth Amendment

1. There is no “Search” Within the Meaning of the Fourth Amendment Because 911 Callers Have No Actual or Reasonable Expectation of Privacy in Information Regarding Their Location

The Fourth Amendment protects individuals from “unreasonable searches.” U.S. Const. amend. IV. For the Fourth Amendment even to apply to a particular government action, the person invoking its protection must be able to claim “a ‘justifiable,’ a ‘reasonable,’ or a ‘legitimate expectation of privacy’ that has been

13 Calling 911 and triggering the government’s emergency response invalidates any claim by a caller that he does not in fact consent to the disclosure of information regarding his location. If he chooses to seek such emergency aid, he implicitly consents both to aiding the authorities in this limited way and to action taken by the government to verify his call. See Nolan v. United States, 423 F.2d 1031, 1043 (10th Cir. 1969) (telephone company’s monitoring of calls does not violate 47 U.S.C. § 605 because illegal user has impliedly consented to company’s attempts to properly bill user), cert. denied, 400 U.S. 848 (1970); Bubis v. United States, 384 F.2d 643, 648 (9th Cir. 1967) (“[w]hen a subscriber of a telephone system uses the system’s facilities in a manner which reasonably justifies the telephone company’s belief that he is violating his subscription rights, then he must be deemed to have consented to the company’s monitoring of his calls to an extent reasonably necessary for the company’s investigation” and there is no violation of 47 U.S.C. § 605); Commonwealth v. Gullett, 329 A.2d 513, 519 (Pa. 1974) (Party calling police to report homicide, its location and number of bodies has no claim for violation of Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S.A. § 5703, where, “[f]rom the nature of the call, the non-confidential quality of the information conveyed, the emergency atmosphere the communication engendered, and the particular agency to which the disclosure was directed, it is apparent that the caller did not intend the privacy of the communication to be maintained. Rather, the conclusion is inescapable that a call made under these circumstances carried with it the permission of the caller to divulge the communication to authorized police personnel other than the officer who happened to take the message and to use the communication to investigate the reported crime by any reasonable means.”).

14 See United States v. Tzakis, 736 F.2d 867, 871–72 (2d Cir. 1984) (defendant cannot assert post-hoc limits on a listener’s recording of conversation by alleging that his willingness to allow overhearing did not encompass permission to record); United States v. Jachimko, 19 F.3d 296, 299 (7th Cir. 1994) (“where a suspect does not withdraw his valid consent to a search for illegal substances before they are discovered, the consent remains valid”); Jones v. Berry, 722 F.2d 443, 449 (9th Cir. 1983) (consent search is valid where consent revoked after search complete), cert. denied, 466 U.S. 971 (1984).
invaded by government action." Smith v. Maryland, 442 U.S. 735, 740 (1979) (citations omitted). This inquiry embraces two discrete questions. The first is "whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy,'" — whether the individual "has shown that 'he seeks to preserve [something] as private.'" Id. at 740 (quoting Katz v. United States, 389 U.S. 347, 361 (Harlan, J., concurring), 351 (1967)). The second question is "whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as 'reasonable,''" — whether "the individual's expectation, viewed objectively, is 'justifiable' under the circumstances." Id. (quoting Katz, 389 U.S. at 361 (Harlan, J., concurring), 353).

In our opinion, a cellular caller dialing the 911 emergency line has not exhibited an "actual (subjective) expectation of privacy" in information regarding his physical location, much less a "reasonable" one. It is hard to imagine any clearer indication of the absence of an expectation of privacy than a cry for help; by reaching out to government officials to seek their help, the caller indicates that he has no expectation of privacy in information that could help the authorities respond to the emergency.15

Even assuming that, in some number of cases, the caller actually expects his physical location to remain private, we believe that expectation is not "one that society is prepared to recognize as 'reasonable.'" Katz, 389 U.S. at 361. A caller dialing 911 seeking assistance cannot reasonably expect that information regarding his location will remain private when public service organizations need such information first and foremost to expeditiously provide the emergency assistance requested by the caller, and secondly to ensure that the call is legitimate and thus worthy of response.16

In addition, the Supreme Court has repeatedly held that a person has no expectation of privacy in information he voluntarily turns over to third parties.17 In order to complete his call, the cellular caller must convey his signal and its corresponding cell site location to the carrier. The caller therefore has no reasonable

---

15 Although no court has directly addressed this issue, our conclusion is supported by cases holding that a person calling 911 has no expectation of privacy in the contents of his call. "There is no expectation of privacy when a person makes a 911 call. Instead, there is an expectation that the information provided will be recorded and disclosed to the public." State ex rel. Cincinnati Enquirer v. Hamilton County, Ohio, 662 N.E.2d 334, 337 (Ohio 1996) (tape recordings of 911 calls are public records that are not exempt from disclosure and must be immediately released upon request); see also State v. Cain, 613 A.2d 804, 809 (Conn. 1992) (tape recordings of 911 calls are public records); State v. Gray, 741 S.W.2d 35, 38 (Mo. App. 1987) (same).

16 See United States v. Van Poyck, 77 F.3d 285, 290-91 (9th Cir.) (prisoner has no reasonable expectation of privacy in outbound calls), cert. denied, 519 U.S. 912 (1996); People v. Suite, 161 Cal. Rptr. 825, 829 (Cal. App. 1980) (person telephoning police and threatening to bomb public building "cannot reasonably expect that records of the call will be private; the only reasonable expectation under such circumstances is that police will make use of every available technology to trace the source of that call").

17 "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." United States v. Miller, 425 U.S. 435, 443 (1976) (bank depositor has no legitimate expectation of privacy in financial information voluntarily conveyed to banks and exposed to their employees in the ordinary course of business); see also Smith, 442 U.S. at 744 (telephone caller has no reasonable expectation of privacy in phone number voluntarily dialed).
expectation of privacy with regard to that information, which is exactly the location information that will be disclosed in phase one of the new FCC rule. And it is the strength of this same signal — information voluntarily turned over by the caller to a third party — that would be measured from different antennas and cell sites, and then analyzed in phase two in order more precisely to determine his location. An expectation of privacy simply is not "justified" in these circumstances.

In sum, because a cellular caller dialing 911 has no actual or reasonable expectation of privacy as to information regarding his physical location, there will be no "search" within the meaning of the Fourth Amendment, and thus no constraints imposed by the Fourth Amendment, when wireless carriers transmit such information to public safety authorities.

2. Cellular Callers Dialing 911 Have Impliedly Consented to the Transmission of Information Regarding Their Physical Location

Even assuming that the provision to public safety agencies of information regarding the physical location of a cellular caller dialing 911 would constitute a search within the meaning of the Fourth Amendment, that search would be lawful if the caller consented to it, as consent is "one of the specifically established exceptions to the requirements of both a warrant and probable cause." *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973). As set forth above, we believe that dialing 911 evidences such consent.

Consent to a warrantless search can be explicit or can be implied from conduct. The Seventh Circuit recently reviewed the caselaw on implied consent, summarizing the pertinent analysis as follows:

Generally, in deciding whether to uphold a warrantless search on the basis of implied consent, courts consider whether (1) the person searched was on notice that undertaking certain conduct, like attempting to enter a building or board an airplane, would subject him to a search, (2) the person voluntarily engaged in the specified conduct, (3) the search was justified by a 'vital interest', (4) the search was reasonably effective in securing the interests at stake, (5) the search was only as intrusive as necessary to further the interests justifying the search and (6) the search curtailed, to some extent, unbridled discretion in the searching officers.


18 "We decline to regard these six factors as dispositive criteria. Rather, these factors should be examined carefully in each case in evaluating the totality of the circumstances and in respecting the consideration that the courts not unnecessarily extend exceptions to the warrant requirement." Id. at 1181. See also Almeida-Sanchez v. United States,
Applying this analysis to the "search" here at issue leads us to conclude that a person using his cellular telephone to call 911 impliedly consents to the carrier providing public safety officials with information as to his physical location. Almost all, if not all, of the above-enumerated factors will be satisfied. The caller will have voluntarily called 911; the search will be justified by a vital interest in responding to an emergency and should be quite effective in facilitating that response; and the search will be limited to determining the caller's physical location, and thus will be only as intrusive as necessary to respond quickly and efficiently to the emergency and should minimize any risk of unbridled discretion by officers. The only factor possibly raising a question would be the first. In most instances, a person calling 911 will be doing so to obtain help for himself or someone in his immediate vicinity, and thus he will undoubtedly be "on notice" that calling 911 will entail disclosure of his location. Even if the caller is seeking help for a third party in a different location, he should be deemed to be on notice that his call will entail disclosure of his physical location in order to expedite the government's response.\footnote{Although we think it unnecessary, the FCC could consider publishing a notice in the telephone book and/or in the standard service contract signed by each subscriber that anyone calling 911 will be deemed to consent to disclosure of their physical location.} Moreover, this simply is not a situation with any of the indicia of unwarranted interference into the private aspects of a person's life. In particular, the government's "search" is in response to the caller's request for assistance; it is not a government-initiated intrusion into a person's private life.

RICHARD L. SHIFFRIN
Deputy Assistant Attorney General
Office of Legal Counsel

\footnote{413 U.S. 266, 271 (1973) (warrantless inspections are constitutional where businessmen engaged in federally regulated enterprises "accept the burdens as well as the benefits of their trade . . . [and] in effect consent[ ] to the restrictions placed upon [them]"); \textit{United States v. Bonanno}, 487 F.2d 654, 658–59 (2d Cir. 1973) (consent shown where "informer went ahead with a call after knowing what the law enforcement officers were about").}