WIRETAP AND ELECTRONIC SURVEILLANCE

COURTS AND JUDGES – JURISDICTION AND PROCEDURE – CELLPHONE WARRANTS

August 30, 2016

The Honorable Matthew A. Maciarello
State's Attorney for Wicomico County

You have asked whether a judge of the Maryland District Court may sign search warrants or other similar court orders involving cellphones, or whether such warrants or orders may only be signed by a circuit court judge. The answer to your question depends on the type of search or other request for information that is at issue. Five different types of warrants or court orders might involve cellphones, each governed by its own statute: (1) a wiretap under § 10-406 of the Courts & Judicial Proceedings ("CJP") Article; (2) a pen register or trap and trace device under CJP § 10-4B-04; (3) a request for stored information from a telecommunications provider under CJP § 10-4A-04; (4) the live tracking of a cellphone's location under § 1-203.1 of the Criminal Procedure ("CP") Article; and (5) the physical search of an actual phone under the general warrant statute in CP § 1-203. As explained further below, a warrant or court order under the first three statutes must be signed by a circuit court judge, but a warrant or order under the last two statutes may be signed by either a circuit court judge or a district court judge.

I

Background

For as long as we have been using wires to transmit oral communications, people have been devising ways to intercept those communications. Although the earliest efforts at wiretapping appear to have been forms of corporate espionage, law enforcement officials first began using wiretaps as a crime-fighting tool in the 1890s. *See* Howard J. Kaplan, *et al.*, *The History and Law of Wiretapping*, ABA Section of Litigation, 2012 Section Annual Conference, at 2-3 (April 18-20, 2012); William Lee Adams, "Brief History: Wiretapping," Time (Oct. 11, 2010). The Supreme Court did not address the constitutionality of wiretapping until 1928, when it held that a wiretap was not a search under the Fourth Amendment. *Olmstead v. United States*, 277 U.S. 438, 464-65 (1928).

Six years after *Olmstead*, Congress enacted the Communications Act of 1934, which made it unlawful for any "person" to "intercept" and "divulge or publish" the contents of any wire or radio communication without the authorization of the sender. Pub. L. 73-426, Title VI, § 605, 48 Stat. 1103 (June 19, 1934), codified at 47 U.S.C. § 605. Soon thereafter, the Supreme Court held that the statute, because it applied to any "person" without exception, prohibited the use of wiretaps by law enforcement personnel, and rendered inadmissible in federal court any evidence obtained as a result of a wiretap. *Nardone v. United States*, 302 U.S. 379, 382-83 (1937); *see also Nardone v. United States*, 308 U.S. 338, 340-41 (1939).

Despite the prohibition on wiretapping in the Communications Act, many law enforcement officers continued to conduct wiretaps, though it remained a "somewhat stigmatized" investigative technique. Kaplan at 3; *see also, e.g.*, *Congressional Wiretapping Policy Overdue*, 2 Stan. L. Rev. 744, 748-50 (1950) (explaining that wiretapping was common at the time and that the U.S. Attorney General had interpreted the Communications Act to prohibit only the divulging of information gleaned from the wiretap, not the wiretapping itself). Then, by the 1950s and 1960s, public attitudes became more accepting of the practice, in part because the government found itself "struggling to enforce laws against organized crime, drug trafficking, and other highly dangerous criminal activities." Kaplan at 3. Some states thus began experimenting with their own wiretap statutes. Maryland, for example, enacted a law in 1956 that authorized law enforcement personnel to conduct wiretaps only if they received the functional equivalent of a warrant based on probable cause from a circuit court judge. 1956 Md. Laws, ch. 116, codified at Md. Ann. Code, art. 35 §§ 100-107 (1951, 1956 Cum. Supp.); *see also Manger v. State*, 214 Md. 71, 75 (1957) (discussing the enactment of the Maryland law); 53 *Opinions of the Attorney General* 456, 458-59 (1968).

Meanwhile, the Supreme Court revisited *Olmstead* and effectively overruled its holding that a wiretap is not a search within the meaning of the Fourth Amendment. *See Berger v. New York*, 388 U.S. 41, 51 (1967); *Katz v. United States*, 389 U.S. 347, 353 (1967). In *Berger*, the Court invalidated New York's wiretap statute, which had authorized wiretapping pursuant to a state court order, but identified circumstances under which such a statute would be constitutional. *Berger*, 388 U.S. at 54-63. Using *Berger* as a guide, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act, which, as amended, continues to govern wiretaps today. *See* Pub. L. 90-351, Title III, 82 Stat. 211 (June 19,

1968), codified at 18 U.S.C. §§ 2510 to 2520. Although Title III generally made it a crime to intercept any oral or wire communications or to divulge the contents of an intercepted communication, 18 U.S.C. § 2511 (1968), the statute for the first time explicitly authorized law enforcement personnel to intercept oral and wire communications in connection with investigations into a limited number of serious crimes so long as the government complied with certain requirements, 18 U.S.C. §§ 2516, 2517 (1968).

Specifically, Title III required that a federal prosecutor seeking a wiretap had to obtain an order from a federal "judge of competent jurisdiction," 18 U.S.C. § 2516(1) (1968), which the statute defined as a judge of a United States district court or court of appeals, 18 U.S.C. § 2510(9)(a) (1968). State prosecutors, if permitted by state law, similarly could obtain an order from a state court "judge of competent jurisdiction," 18 U.S.C. § 2516(2) (1968), defined as "a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire or oral communications," 18 U.S.C. § 2510(9)(b) (1968). Title III also provided that, before a federal or state court judge could authorize a wiretap, the law enforcement agency making the request had to demonstrate probable cause and satisfy other procedural and substantive requirements that were stricter than those for obtaining a warrant. *See* 18 U.S.C. § 2518 (1968). In essence, Title III established a "uniform minimum national standard governing the interception and use of [wire or oral] communications." *Ricks v. State*, 312 Md. 11, 13 (1988). Thus, while state laws authorizing wiretaps could be more protective of privacy, they at least had to meet the federal standards in Title III. *Id.* at 14.

To conform to the new federal standards, Maryland repealed its 1956 wiretap statute and adopted the Maryland Wiretap and Electronic Surveillance Act (the "Maryland Wiretap Act"). *See* 1977 Md. Laws, ch. 692, now codified at CJP §§ 10-401 to 10-414. The Maryland Wiretap Act "was modeled upon and closely tracked" Title III of the federal law, "although in some particulars [the state law] was more restrictive." *Ricks*, 312 Md. at 15; *see also* 85 *Opinions of the Attorney General* 225 (2000). The Maryland statute—like the federal law—required law enforcement personnel to obtain an order from a "judge of competent jurisdiction," which it defined as "a judge of a circuit court or the Supreme Bench of Baltimore City." 1977 Md. Laws, ch. 692, § 3, now codified at CJP §§ 10-401(12), 10-406(a).

In the 1980s, the federal government and the states revisited the issue of communication privacy in light of the increasing use of computers and other emerging technologies. In response to these new challenges, Congress enacted a series of reforms as part of the Electronic Communications Privacy Act of 1986. Pub. L. 99-508, 100 Stat. 1848 (Oct. 21, 1986). First, Congress updated Title III of the Crime Control and Safe Streets Act by prohibiting anyone from intercepting "electronic communications" without a valid court order that met the same heightened standards as those for the interception of wire and oral communications. *Id.* (Title I).

Second, Congress added the Stored Wire and Electronic Communications and Transactional Records Access Act. *Id.*, 100 Stat. 1860 (Title II), codified at 18 U.S.C. §§ 2701 to 2710 ("Stored Communications Act"). This new legislation covered two separate types of information: (1) the contents of communications stored in the service provider's electronic storage system; and (2) non-content records pertaining to subscribers. *See* 18 U.S.C. § 2703 (1986). The statute required service providers to disclose both types of information to a state or federal governmental entity if the government complied with certain requirements laid out in the statute, though the requirements varied with the type of information sought. *Id.* With respect to the contents of stored communications, law enforcement personnel were generally required to obtain a warrant under the Federal Rules of Criminal Procedure or an "equivalent State warrant." 18 U.S.C. § 2703(a) (1986). For non-content information, however, the government could require the service provider to disclose the information based on a subpoena or a special court order based on less than probable cause. 18 U.S.C. § 2703(c), (d) (1986) (government must show that there is "reason to believe" that the information is "relevant to a legitimate law enforcement inquiry").

Third, Congress enacted new provisions governing pen registers and trap and trace devices.[1] Pub. L. 99-508, 100 Stat. 1868 (Title III), codified at 18 U.S.C. §§ 3121 to 3126. These provisions required law enforcement personnel to obtain an order based on less than probable cause from a "court of competent jurisdiction," 18 U.S.C. §§ 3122, 3123 (1986), and defined "court of competent jurisdiction" to mean either (1) "a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals," or (2) "a court of general criminal

[1] A pen register is an electronic device that records every *outgoing* phone number called from a particular telephone line in real time, while a trap and trace device records every *incoming* number that dials a particular phone. *See* 18 U.S.C. § 3126(3), (4) (1986).

jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device," 18 U.S.C. § 3126(2) (1986). Congress gave the states two years to amend their wiretap and pen register statutes to meet the new federal minimum standards under Title I and Title III of the 1986 Act. Pub. L. 99-508, Title I, § 111; Title III, § 302.

In 1988, the General Assembly enacted legislation intended largely to bring Maryland into compliance with the new federal law. *See* 1988 Md. Laws, ch. 607. In a single piece of legislation, the Legislature amended the Maryland Wiretap Act to cover "electronic" communications, added a new subtitle governing access to the stored communications and transactional records of service providers, *id.* (codified at CJP Title 10, Subt. 3A), and added a second new subtitle governing pen registers and trap and trace devices, *id.* (codified at CJP Title 10, Subt. 3B). The new Maryland laws were again modeled closely on federal law, sometimes using the same language of the federal act. *See id.*; 75 *Opinions of the Attorney General* 382, 384-85 (1990). We will discuss the requirements of these Maryland laws in more detail below.

Finally, in more recent years, further technological advances—particularly those involving cellphones—have raised new questions about access to, and the privacy of, wire and electronic communications. The Supreme Court resolved one such question in *Riley v. California*, 134 S. Ct. 2473 (2014), holding that the police must generally secure a warrant before searching the digital data on a cellphone seized from an arrestee. Other questions remain, however, including whether the government needs a warrant to track a person's location using information obtained from his or her cellphone. *See generally*, *e.g.*, R. Craig Curtis, *et al.*, *Using Technology the Founders Never Dreamed of: Cell Phones As Tracking Devices and the Fourth Amendment*, 4 U. Denv. Crim. L. Rev. 61 (2014). Some lower courts have drawn a distinction between *historical* location information obtained after-the-fact from a service provider and *prospective* information that allows the police to track cellphone location in real time, concluding that the latter requires a warrant but the former requires only an order under the Stored Communications Act. *See United States v. Jones*, 908 F. Supp. 2d 203, 208-09 nn. 5 & 6 (D.D.C. 2012) (collecting cases); *see also*, *e.g.*, *United States v. Graham*, 824 F.3d 421, 426-27 (4th Cir. 2016) (en banc) (holding that the Fourth Amendment does not require police to obtain a warrant for

historical cell location information but suggesting that the opposite may be true for prospective location information).

Maryland law specifically addresses the availability of prospective location information. In 2014, the General Assembly enacted a statute under which a court may issue an order permitting law enforcement personnel to obtain real time "location information from an electronic device" if there is "probable cause to believe" that a crime "has been, is being, or will be committed by" the user of the device and the location information will lead to evidence of the crime or an arrest on an active warrant. *See* 2014 Md. Laws, ch. 191, codified at CP § 1-203.1(b)(1). In addition, the Court of Special Appeals recently held that tracking a cellphone's location in real time using a cell-site simulator is a search under the Fourth Amendment and requires a warrant based on probable cause. *State v. Andrews*, 227 Md. App. 350, 395 (2016).[2] With this background in mind, we turn to your question.

II

Analysis

You have asked whether a judge of the Maryland District Court may sign warrants or other similar court orders involving cellphones. As described above, no single statute governs the respective authority of district court and circuit court judges over cellphone warrants. Instead, the answer to your question depends on the type of search or request for information at issue and the specific statutory provision under which the warrant or court order is authorized.

A. The Maryland Wiretap Act

The first type of order authorizing a search that might involve a cellphone is a wiretap order under the Maryland Wiretap Act. *See* CJP §§ 10-401 to 10-414. Generally speaking, under the Wiretap Act "it is unlawful for any person to . . . [w]illfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic

[2] Because *Andrews* involved the use of a cell-site simulator—a device that forces a suspect's cell phone to transmit signals and thus enables the police, on their own, to track the suspect—the court did not decide whether the government needs a warrant to obtain location information from a service provider. 227 Md. App. at 358 n.3. The court also did not decide whether the new type of court order provided for under CP § 1-203.1 for the real-time tracking of cellphones would suffice to meet the Fourth Amendment warrant requirement. *Id.* at 408.

communication." CJP § 10-402(a)(1). However, a "judge of competent jurisdiction" may "grant an order authorizing the interception of wire, oral, or electronic communications by investigative or law enforcement officers" when there is probable cause to believe that the interception will yield evidence of one of a series of specified crimes. CJP § 10-406(a); *see also* CJP § 10-408 (outlining the probable cause requirement and other requirements for wiretap orders). The statute specifically defines a "judge of competent jurisdiction" as a "judge of *any circuit court* within the State having jurisdiction over the offense under investigation." CJP § 10-401(12) (emphasis added). Thus, a wiretap order may be issued only by a circuit court judge.

In fact, allowing a district court judge to issue such an order would likely conflict with federal law. As explained above, the federal counterpart to Maryland's wiretap statute prohibits the intercept of a telephone communication without authorization from either a federal judge or "a State court judge of competent jurisdiction." 18 U.S.C. § 2516(2); *see also* 18 U.S.C. § 2511. The federal statute in turn defines "judge of competent jurisdiction" to mean "a judge of any court of *general criminal jurisdiction* of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications." 18 U.S.C. § 2510(9)(b) (emphasis added). Because the Maryland District Court is a court of "limited jurisdiction," not of general jurisdiction, CJP § 1-601, the federal statute effectively prevents Maryland from authorizing a district court judge to grant wiretap orders.

B. Pen Registers and Trap and Trace Devices

A second type of order potentially involving cellphones is an order under Maryland's statute governing pen registers and trap and trace devices. *See* CJP §§ 10-4B-01 to 10-4B-05. Although State law generally makes it a crime to use a pen register, CJP § 10-4B-02(a), a law enforcement officer may apply to "a court of competent jurisdiction" for an order authorizing a pen register. CJP § 10-4B-03(a). The court may issue such an order if it "finds that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation." CJP § 10-4B-04(a).

Under the plain terms of this statute, "court of competent jurisdiction" means "any *circuit court* having jurisdiction over the crime being investigated regardless of the location of the instrument or process from which a wire or electronic

communication is transmitted or received." CJP § 10-4B-01(b) (emphasis added). As with the Wiretap Act, this definition was likely informed by federal law, under which a pen register or trap and trace device may only be authorized by "a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device." 18 U.S.C. § 3127(2)(B). Thus, a court order issued under subtitle 4B must be issued by a circuit court judge.

C. Stored Communications and Transactional Records

A different statute governs transactional records and historical information stored by a service provider in that provider's electronic storage system. *See* CJP §§ 10-4A-01 to 10-4A-08. If the stored information will reveal the content of a communication, law enforcement officials may compel the service provider to disclose that content "only in accordance with a search warrant issued by a court of competent jurisdiction." CJP § 10-4A-04(a). Alternatively, if the information will not reveal any content, the police do not need a search warrant based on probable cause. Instead, a "court of competent jurisdiction" may "issue an order requiring disclosure" of that non-content information "if the investigative or law enforcement officer shows that there is reason to believe the records or other information sought are relevant to a legitimate law enforcement inquiry." CJP § 10-4A-04(c).

Thus, as under subtitle 4B governing pen registers and trap and trace devices, a warrant or court order seeking stored communications under subtitle 4A must be signed by a "court of competent jurisdiction." Unlike subtitle 4B, however, subtitle 4A does not explicitly define that term. Although a "*judge* of competent jurisdiction" in subtitle 4A has the same meaning as under the Maryland Wiretap Act, CJP § 10-4A-01(b)(12) (emphasis added)—namely, "a judge of any circuit court within the State having jurisdiction over the offense under investigation," CJP § 10-401(12)—the operative provisions of subtitle 4A never actually use the term "judge of competent jurisdiction."

Despite this ambiguity, we conclude that a court of competent jurisdiction under Maryland's stored communications statute means a circuit court. The General Assembly enacted this statute in subtitle 4A at the same time and as part of the same piece of legislation as the pen register statute in subtitle 4B, which expressly defined "court of competent jurisdiction" to mean "a circuit court." 1988 Md. Laws, ch. 607, codified at CJP § 10-4B-01(c) (1984 Repl. Vol, 1988 Supp.). When, as here, a provision is part of a larger statutory scheme, "the legislative intention must be gathered

from the entire statute, rather than from only one part." *Bridges v. Nicely*, 304 Md. 1, 10 (1985). Thus, courts generally presume that a term used in one part of a statute has the same meaning when used elsewhere in the same statute. *See, e.g.*, *Lockett v. Blue Ocean Bristol*, 446 Md. 397, 422 (2016); *Baltimore & Annap. R. Co. v. Lichtenberg*, 176 Md. 383, 391-92 (1939); *Edmonds v. Cytology Servs. of Md., Inc.*, 111 Md. App. 233, 251 n.19 (1996), *aff'd sub nom. Rivera v. Edmonds*, 347 Md. 208 (1997); *cf. Whack v. State*, 338 Md. 665, 673 (1995) (noting that the presumption may be overcome if "apparent" that the Legislature intended the words to have different meanings). Applying that longstanding rule here, we conclude that the General Assembly likely intended the term "court of competent jurisdiction" in subtitle 4A to have the same meaning as in subtitle 4B: a circuit court.[3]

We recognize that the interpretive rule we apply here has its limits, and that the use of different terms in different parts of a statutory scheme usually indicates that the terms should have different meanings, *see, e.g.*, *Toler v. Motor Vehicle Admin.*, 373 Md. 214, 223 (2003), but here the use of "judge" rather than "court" in § 10-4A-01 appears to have been a historical accident. The federal laws on which the General Assembly closely modeled its own legislation happened to use "judge of competent jurisdiction" in the wiretap act, 18 U.S.C. § 2516(2), and "court of competent jurisdiction" in the pen register statute, 18 U.S.C. § 3122(a)(2), and these two terms seem to have been carried over into the analogous Maryland laws. There is no evidence that Congress intended those two terms to have different meanings. To the contrary, in both contexts Congress granted authority to issue orders only to State courts of "general criminal jurisdiction." 18 U.S.C. §§ 2510(9)(b), 3127(2)(b). We thus see no indication that the General Assembly intended to ascribe different meaning to those terms by incorporating them into the analogous Maryland laws.

Furthermore, as discussed above with respect to the Maryland Wiretap Act and the pen register statute, allowing a district court

---

[3] The pen register statute in subtitle 4B has since been amended to define "court of competent jurisdiction" as "any circuit court having jurisdiction over the crime being investigated regardless of the location of the instrument or process from which a wire or electronic communication is transmitted or received." CJP § 10-4B-01(b). We express no opinion on whether the new aspects of that definition should also be read into the definition of "court of competent jurisdiction" in subtitle 4A.

judge to sign a warrant or order under subtitle 4A would likely conflict with federal law. Under the analogous federal Stored Communications Act, the government may only require a communications provider to turn over stored communications or records with a warrant or court order from "a court of *general criminal jurisdiction* of a State."[4] 18 U.S.C. § 2711(3)(B) (emphasis added); *see also* 18 U.S.C. § 2703. Because the Maryland District Court is not a court of general criminal jurisdiction, the definition of court of competent jurisdiction in subtitle 4A should be read to exclude district court judges.[5] In our view, therefore, only a circuit court judge may sign a warrant or court order under CJP § 10-4A-04.

D. Live-Tracking of Phone Location

As noted above, in 2014, the General Assembly enacted a statute authorizing law enforcement personnel to track a cellphone user's location in real time. *See* 2014 Md. Laws, ch. 191 (codified at CP § 1-203.1). Under the statute, the police must obtain an order from a "court," CP § 1-203.1(b)(1), and "court" is defined to include "the District Court *or* a circuit court having jurisdiction over the crime being investigated." CP § 1-203.1(a)(2) (emphasis added). An order under this section thus may signed by a judge of the District Court.

However, this new statute's grant of power to the District Court does not mean that a district court judge may now sign any and all orders involving cellphones. The other statutes discussed

---

[4] Whether a warrant or some type of lesser court order is required depends on the type of information at issue. A warrant is usually required for content information, but a lesser court order will suffice for non-content records. *See* 18 U.S.C. § 2703(a), (b)(1)(A), (d).

[5] As originally enacted, the federal Stored Communications Act did not expressly require the warrant or order to be issued by a "court of competent jurisdiction." The statute instead required a "warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant" in some circumstances and, in other circumstances, a "court order for disclosure" from an unspecified court. Pub. L. 99-508, 100 Stat. 1862, codified at 18 U.S.C. § 2703(a), (d) (1986). But Congress later amended the statute to clarify that a state court warrant or order had to be from "court of general criminal jurisdiction." Pub. L. 100-690, Title VII, § 7039, 102 Stat. 4399 (Nov. 18, 1988); Pub. L. 111-79, 123 Stat. 2086 (Oct. 19, 2009). Given that the General Assembly saw no need to amend its own law to bring it into compliance with the new federal language, the Legislature presumably thought that the authority to grant such orders in Maryland was already limited to the circuit court.

above define "court" differently, and there is no requirement that the term be defined the same way in every statute. It also makes sense that the General Assembly would allow the District Court to sign court orders here but withhold that authority in other contexts. Unlike the other statutes discussed above, federal law does not expressly limit the power to grant warrants or court orders of this type to a court of general jurisdiction.

E. Physical Inspection of Actual Phone

Finally, if a police officer merely wants to turn on a cellphone and physically examine its contents—perhaps after making an arrest of a suspect who was in possession of the phone—that search would be governed by the general warrant statute in CP § 1-203. *See Riley*, 134 S. Ct. at 2495 (holding that a warrant is generally required to search the contents of a cellphone, even as part of a search incident to an arrest). Because such a search does not involve a wiretap, pen register, the live tracking of a phone's location, or the compelled disclosure of stored information from a service provider, none of the specialized statutes applicable to those circumstances would apply. Under Maryland's general warrant statute, a search warrant may be issued by either "[a] circuit court judge or District Court judge." CP § 1-203(a)(1). Thus, a judge of the District Court may legally sign a search warrant for this type of search.

III

Conclusion

A district court judge may sign a warrant or court order for the physical inspection of a cellphone under CP § 1-203 and for real time cellphone location information under CP § 1-203.1. A district court judge may not, however, sign a warrant or court order under Title 10 of the Courts & Judicial Proceedings Article for a wiretap, for stored electronic or wire communications or transactional records from a service provider, or for a pen register or trap and trace device.

Brian E. Frosh
Attorney General of Maryland

Patrick B. Hughes
Assistant Attorney General

Adam D. Snyder
Chief Counsel, Opinions & Advice