2015

For Now, New York State Investigators Can Ping Cellphones Without a Warrant in New York State

Wesley Cheng
New York County District Attorney's Office

For Now, New York State Investigators Can Ping Cellphones Without A Warrant in New York State

Author Wesley Cheng is currently an Associate General Counsel at the Office of the MTA Inspector General.

This article represents solely the views of the author, and not necessarily those of his employer.

Prior to his current position, Wesley was an Assistant District Attorney for the New York County District Attorney's Office and the Office of the Special Narcotics Prosecutor for the City of New York. He is also an Instructor for the Intensive Trial Advocacy Program at the Benjamin N. Cardozo School of Law.

Can New York State Inspectors General and other law enforcement agencies use real-time GPS tracking on cellphones without a judicially authorized warrant? At this time, the answer appears to be yes.

In 2013, for the first time, two New York State trial courts ruled on the use of global positioning system (GPS) information that was obtained without judicial authorization.[1] In both *People v. Moorer* and *People v. Wells*, detectives used GPS information obtained from carriers to track down their targets, without first obtaining a warrant.[2] Both the *Moorer* and *Wells* courts found that receiving live Geolocation data, commonly referred to as "pinging," from a cellphone in order to determine its location was not a search because the defendants did not have a legitimate expectation of privacy in this kind of data.[3]

This article examines the major factors shaping the *Moorer* and *Wells* decisions. It also analyzes the implications of decisions in other cases involving the use of Geolocation tracking devices, and looks ahead to other areas of litigation that may arise in the future with respect to GPS devices. Finally, it concludes that, assuming *Moorer* and *Wells* (or other trial court cases with similar findings) are not overturned on this issue in the higher courts, law enforcement agencies can be comfortable that pinging cellphones is a technique that can be utilized without a warrant in New York.

I. What it means to "ping" a phone

GPS, or Global Positioning System, provides highly accurate positioning, navigation and timing information worldwide for any device equipped with a GPS satellite receiver.[4] All cellphones have this kind of technology.[5] When a cellphone is turned on, it connects with its service provider's network of cell towers, and identifies itself to the

[1] *See People v. Moorer*, 39 Misc. 3d 603 (Monroe Cnty. Ct. 2013); *See also People v. Wells*, 1275/13, NYLJ 1202666087234, at *1 (Sup., QU, Decided July 28, 2014).
[2] *Id*.
[3] *Id*.
[4] *See Moorer*, 39 Misc. 3d at 609.
[5] *Wells*, 1275/13, NYLJ 1202666087234, at *4.

nearest cell tower.[6] If a subscriber moves to another location, the phone is then "handed off" to the nearest cellphone tower to the new location.[7] Service providers can generate location data at any time by sending a signal to the cellphone to determine its location, which can be sent back to the service provider, a process commonly known as "pinging."[8] However, once a cellphone is powered off, a provider can no longer receive location data from the subscriber's phone.[9]

In both *Moorer* and *Wells*, police investigators pinged the defendants' cellphones without a judicially authorized warrant to aid them in locating the defendants.[10] The defendants in those cases moved to suppress all evidence retrieved as a result of the ping technology.[11] Both the *Moorer* and *Wells* courts determined that obtaining the live Geolocation data from the defendants' cell phones did not constitute a search within the meaning of the Fourth Amendment.[12]

II. Factors driving the *Moorer* and *Wells* decisions

The courts arrived at their decisions based on four main findings: (1) the defendants had no reasonable expectation of privacy in the Geolocation data;[13] (2) there was no physical intrusion that resulted in investigators receiving Geolocation data from the defendants' cellphones;[14] (3) Geolocation tracking data sent from cellphone GPS to law enforcement was more akin to the technology of beepers or pagers;[15] and (4) societal norms have changed to the point where citizens are expected to know that GPS technology can be used to locate and track their phones.[16]

---

[6] *Id.*
[7] *Id.* (citing *In Re Application of USA for an Order Releasing Historical Cell Site Info.*, 736 F. Supp. 2d 578 (E.D.N.Y. 2010)).
[8] *See In re United States ex rel. an Order Authorizing Disclosure of a Specified Wireless Tel.*, Case No. 10-2188-SKG, 849 F. Supp 2d 526, 534 (D. Md. 2011).
[9] *See Wells*, 1275/13, NYLJ 1202666087234, at *5.
[10] *See id.* at *2; *see also Moorer*, 39 Misc. 3d at 605.
[11] *See Moorer*, 39 Misc. 3d at 605; *Wells*, 1275/13, NYLJ 1202666087234, at *1.
[12] *See Moorer*, 39 Misc. 3d at 615; *Wells*, 1275/13, NYLJ 1202666087234, at *3.
[13] *See Moorer*, 39 Misc. 3d at 615; *Wells*, 1275/13, NYLJ 1202666087234, at *5.
[14] *See Moorer*, 39 Misc. 3d at 612-13; *Wells*, 1275/13, NYLJ 1202666087234, at *5.
[15] *See Moorer*, 39 Misc. 3d at 613-14.
[16] *See id* at 618; *See also Wells*, 1275/13, NYLJ 1202666087234, at *8-9.

A. No expectation of privacy in Geolocation data

The Fourth Amendment of the United States Constitution protects "against unreasonable searches and seizures" of a citizen's "person, house, papers and effects."[17] Conversely, the Fourth Amendment is not implicated in situations where a search has not occurred.[18] Search and seizure law originally followed a common-law physical trespass theory, but in 1967, the Supreme Court shifted its stance in *Katz v. United States*.[19] Under *Katz*, a search occurs within the meaning of the Fourth Amendment whenever a suspect's reasonable expectation of privacy has been violated.[20] *Katz* employed a two-step analysis: (1) whether the individual "has exhibited an actual (subjective) expectation of privacy;" and (2) whether society is prepared to recognize the expectation as (objectively) reasonable.[21]

The Supreme Court applied these principles to modern technology in *Smith v. Maryland*.[22] The *Smith* Court held that the installation of a device that records all numbers called from a particular telephone line, commonly referred to as a pen register, was

---

[17] U.S. CONST. amend. IV.
[18] *See Moorer*, 39 Misc. 3d at 612.
[19] *United States v. Katz*, 389 U.S. 347, 353 (1967) (rejecting the "trespass" doctrine, established by *United States v. Olmstead*, 277 U.S. 438 (1928), and articulating a different analysis for search cases).
[20] *Id.* at 350.
[21] *See id.* at 352-53 (dismissing the government's argument that Katz, the defendant, had no reasonable expectation of privacy). Katz was convicted of transmitting wagering information by telephone in violation of a federal statute. *Id.* At trial, the government introduced evidence of Katz's voice during telephone conversations which had been overheard by FBI agents. *Id.* The agents had attached an electronic listening and recording device to the outside of the public telephone booth in which Katz conducted his conversations. *Id.* The *Katz* Court found that Katz intended to keep his words private, not his actions, and that he was entitled to assume that his words would not be broadcast to the world. *Id.* Having determined that the interception of the telephone conversations was a search and seizure, the Supreme Court then considered whether the search complied with the Constitution. *Id.* The Court determined that the search would have been permissible with a warrant, but that the warrantless search and seizure was unreasonable and therefore a violation of the Fourth Amendment. *Id.*
[22] *Smith v. Maryland*, 442 U.S. 735 (1979). In 1976, a robbery victim began receiving threatening and obscene phone calls from a man who claimed to be the robber. *Id*. at 737. The police, without seeking a warrant, asked the telephone company to install a pen register on the defendant's phone. *Id*. Through this method, the police discovered that the defendant was indeed the person who had called the victim, and charged him with robbery. *Id*.

not a search under the Fourth Amendment.[23] In his majority opinion, Justice Blackmun focused on the fact that the defendant voluntarily turned over pen register information to a third party service provider.[24] Justice Blackmun reasoned that individuals were aware that the service provider had this information since all customers received a copy of all numbers dialed in their monthly bill.[25] Therefore, the *Smith* Court found that there was no reasonable expectation of privacy in that information.[26]

Both the *Moorer* and *Wells* cases drew analogies to the *Smith* case, likening Geolocation data to pen register information.[27] A subscriber's signal is necessary to make a call from a cellphone, and the information contained in the signal is voluntarily turned over to the third-party service provider.[28] Thus, in the same way that an individual has no reasonable expectations of privacy in pen register data, neither does he or she have a reasonable expectation of privacy in GPS information.[29, 30]

B. Distinguishing physical trespasses in *Jones* and *Weaver*

The defendants in *Moorer* and *Wells* both cited to the case of *United States v. Jones*, and its New York Court of Appeals counterpart,

---

[23] *Id.* at 742.
[24] *Id.* at 744.
[25] *Id.* at 742.
[26] *Id.* at 745.
[27] *See Moorer*, 39 Misc. 3d at 615 (concluding, nearly thirty years later, that the transmission of a subscriber's signal, which is necessary to make a call from a cellphone, does not entitle the subscriber to a reasonable expectation of privacy in that signal); *Wells*, 1275/13, NYLJ 1202666087234, at *7 (finding that the defendant had no standing to challenge information in the possession of a third party (in this case, the cellphone carrier)). It has long been settled that a person has no expectation of privacy in telephone records. *Id*. (citing *Smith*, 442 U.S. at 735, 743-44).
[28] *See Moorer*, 39 Misc. 3d at 615. *See also Wells*, 1275/13, NYLJ 1202666087234, at *7.
[29] *See Moorer*, 39 Misc. 3d at 615. *See also Wells*, 1275/13, NYLJ 1202666087234, at *7.
[30] The *Moorer* case also cited to *United States v. Skinner*, a Sixth Circuit case that held that the defendant did not have a reasonable expectation of privacy in his GPS data and the use of GPS information from his cell phone was not considered a search. Though not a binding case on New York courts, the facts mirrored the *Moorer* and *Wells* cases and supported their outcomes. *See United States v. Skinner*, 690 F.3d 772, 777 (6th Cir. 2012).

People v. Weaver.[31] Both *Jones* and *Weaver* involved the warrantless surreptitious physical attachment of GPS devices on vehicles to track movements over an extended period of time.[32] The *Jones* and *Weaver* courts held that the physical attachment of the GPS devices constituted searches pursuant to the Fourth Amendment, and therefore required a warrant.[33] The *Jones* Court applied a physical trespass theory in arriving at its conclusion.[34]

The *Moorer* and *Wells* courts easily distinguished *Jones* and *Weaver*, however, because neither *Jones* nor *Weaver* involved the pinging of a cellphone.[35] Rather, in *Moorer* and *Wells*, there was no physical installation by law enforcement of anything onto the defendants' cellphones.[36] Instead, investigators merely obtained Geolocation data that the phones were already emitting.[37] Thus, as the *Wells* court held, there was no intrusion into that defendant's "house, papers and effects."[38] The *Moorer* court added that neither the *Jones* nor *Weaver* majorities addressed the constitutionality of merely gathering information from GPS devices that had been installed in a car or cellphone with the owner's knowledge or consent.[39]

---

[31] *See People v. Weaver*, 909 N.E.2d 1195 (2009). (holding that physically attaching a GPS device to the automobile of a criminal suspect, and using that device to track the suspect's movements, is a search subject to constitutional limits). *See also United States v. Jones*, 132 S. Ct. 945 (2012).
[32] *See Weaver*, 909 N.E.2d at 1195. *See also Jones*, 132 S. Ct. at 945.
[33] *See Weaver*, 909 N.E.2d at 1195. *See also Jones*, 132 S. Ct. at 945.
[34] *See* Lauren Elena Smith, *Jonesing for a Test: Fourth Amendment Privacy in the Wake of United States v. Jones*, 58 BERKELEY TECH. L.J. 1003, 1015 (2013). The *Jones* majority explained that the common-law trespass test was essentially a minimum test and that the *Katz* test added to, and did not substitute for, the common-law trespassory test. *Id*. The *Jones* Court concluded that the fact that law enforcement "physically occupied private property" by encroaching on a "constitutionally protected area" (the car) "for the purpose of obtaining information" was sufficient to decide the case. *Id*. (citing *Jones*, 132 S. Ct. at 949).
[35] *See Wells*, 1275/13, NYLJ 1202666087234, at *5. *See also Moorer*, 39 Misc. 3d at 613-14.
[36] *See Wells*, 1275/13, NYLJ 1202666087234, at *2-4. *See also Moorer*, 39 Misc. 3d at 605-06.
[37] *See Wells*, 1275/13, NYLJ 1202666087234, at *5. *See also Moorer*, 39 Misc. 3d at 618.
[38] *Compare Wells*, 1275/13, NYLJ 1202666087234, at *5 (rejecting pinging as an intrusion (citing U.S. CONST. amend. IV)), *with Jones,* 132 S. Ct. 945, and *Weaver*, 909 N.E.2d 1195 (holding that surreptitious physical installation of a tracking device on defendant's car establishes an intrusion of a constitutionally protected area).
[39] *See Moorer*, 39 Misc. 3d at 613-14.

C. Analogizing 'beepers' in the *Knotts* and *Karo* cases

The *Moorer* court went a step further in its analysis of the *Jones* case.[40] The *Jones* decision made reference to two post-*Katz* cases: *United States v. Knotts* and *United States v. Karo*.[41] Both *Knotts* and *Karo* involved the use of "beepers,"[42] which are electronic tracking devices that were precursors to modern GPS devices.[43] In both cases, beepers were installed in containers before the defendants took possession of them, and the information gathered aided investigators in finding the defendants.[44] The Supreme Court ruled in both cases that the installation of the beepers did not constitute a search even though the defendants did not have knowledge of the beepers' presence.[45]

Likewise, in *Moorer* and *Wells*, pinging the defendants' cellphones narrowed the area in which police searched for the defendants.[46] In both cases, investigators combined the general

---

[40] *See id.* at 613.

[41] *See United States v. Knotts*, 460 U.S. 276 (1983) (holding that a person traveling in public has no expectation of privacy in his movements. In *Knotts*, a 'beeper' device attached to a drum inside the defendant's vehicle was determined not to have violated a legitimate expectation of privacy and the beeper's installation did not require a warrant). *See also United States v. Karo*, 468 U.S. 705 (1984) (finding the installation of a beeper in a can of ether did not constitute "search' or "seizure," and the Fourth Amendment was not implicated until the beeper was turned on and used to track the ether shipment on private property).

[42] *See Knotts*, 460 U.S. at 277. A beeper is a radio transmitter, usually battery-operated, which emits periodic signals that can be picked up by a radio receiver. *Id*. In this case, a beeper was placed in a five-gallon drum containing chloroform purchased by one of respondent's codefendants. *Id*. By monitoring the progress of a car carrying the chloroform, law enforcement agents were able to trace the chloroform from its place of purchase to respondent's secluded cabin in a nearby state. *Id*. *See also Karo*, 468 U.S. at 713.

[43] Ramya Shah, *From Beepers To GPS: Can the Fourth Amendment Keep Up With Electronic Tracking Technology?*, 2009 U. ILL. J. L. TECH. & POL'Y 281, 283 (2009).

[44] *See Knotts*, 460 U.S. at 277. *See also Karo*, 468 U.S. at 713.

[45] *See Knotts*, 460 U.S. at 282. The Court noted that visual surveillance from public places along the co-defendant's route or adjoining Knotts's premises would have sufficed to reveal all of these facts to the police, and that nothing in the Fourth Amendment prohibited the police from augmenting their own sensory faculties with the beeper technology in this case. *Id*. *See also Karo*, 468 U.S. at 712 (finding that although the can may have contained an unknown and unwanted foreign object, it cannot be said that anyone's possessory interest was interfered with in a meaningful way).

[46] *See Wells*, 1275/13, NYLJ 1202666087234, at *6. *Id*. *See also Moorer*, 39 Misc. 3d at 616.

location information received from the ping with other investigative techniques to track down the defendants' cellphones.[47] Indeed, the *Wells* court made specific note of the generality of the information received from the ping, stating that it merely provided investigators with the general area near cellphone towers, based on a calculation of latitude and longitude, within which the cellphone could be found.[48] The defendant simply could not assert an expectation of privacy in such a large space.[49]

The *Moorer* court also cited a non-precedential case, *Devega v. State of Georgia*, in which investigators used GPS information from the defendant's cellphone to locate him, in the same manner as in *Wells*.[50] The *Devega* court held that ping information received from cellphones was merely "the next generation of tracking science and technology" that built upon beepers.[51] *Devega* concluded that warrantless pinging of the defendant's cellphone revealed the same information that physical surveillance would provide, so there was no search within the context of the Fourth Amendment.[52]

D. Analyzing social norms and expectations

As part of their decisions, both the *Moorer* and *Wells* opinions also found that societal norms and expectations are such that there is no reasonable expectation of privacy in GPS data from cellphones.[53] The *Wells* Court argued that modern day cellphone users are aware of "the capacity for their phone to be located by GPS."[54] Similarly, the

---

[47] *See Wells*, 1275/13, NYLJ 1202666087234, at *6. *See also Moorer*, 39 Misc. 3d at 615-16.
[48] *See Wells*, 1275/13, NYLJ 1202666087234, at *6.
[49] *Id.*
[50] *See Devega v. State,* 286 Ga. 448 (2010) (finding defendant had no expectation of privacy when the ping occurred because the defendant was driving on a public road after killing the buyer in a cocaine transaction).
[51] *See Moorer*, 39 Misc. 3d at 615 (citing *Devega,* 286 Ga. at 454).
[52] *See Devega*, 286 Ga. at 454 ("Due to the absence of any expectation of privacy, the Supreme Court held that the warrantless monitoring of signals from a beeper inside an automobile traveling on public roads did not violate the Fourth Amendment because it did not reveal any information that was not also available through visual surveillance." (citing *Knotts*, 460 U.S. at 285)).
[53] *See Wells*, 1275/13, NYLJ 1202666087234, at *6. *See also Moorer*, 39 Misc. 3d at 615-16.
[54] *See Wells*, 1275/13, NYLJ 1202666087234, at *8 ("Based on both the wide use of this technology for car navigation, car location, lost cellphones, and a myriad of other uses, it can no longer be said that one can reasonably expect that a cellphone

Moorer Court reasoned that "public ignorance about cell phone technology can no longer be maintained."[55] Both courts also found that cellphone users could easily avoid being potentially tracked by government investigators simply by shutting off their cellphones.[56]

III. What the *Moorer* and *Wells* decisions mean for practitioners

The two trial court decisions in *Moorer* and *Wells* have implications for Fourth Amendment law and practitioners. The decisions, if not overturned by higher courts, clearly allow government investigators in New York to obtain Geolocation data for employees' cellphones without first obtaining a judicially authorized warrant. The prevailing theory is that citizens have no expectation of privacy over their GPS data because they freely share it with third-party service providers.

The decisions also seem to implicitly endorse the use of Geolocation tracking on vehicles, or any other device, that come preloaded with GPS technology. This falls directly in line with the two United States Supreme Court cases cited in *Moorer* that involved beepers. Both the *Moorer* and *Wells* courts reasoned that it was within a citizen's general knowledge that he may be located by the GPS that is pre-installed on his phone. Thus, these two cases will become even more relevant as more vehicles and other devices come preinstalled with Geolocation systems, such as General Motors' Onstar system.

Not all courts to have considered this issue agree with the *Wells* and *Moorer* courts, however. The New Jersey Supreme Court, for example, found in 2013 that cellphone GPS information fell within the ambit of the Fourth Amendment in ruling that police needed a judicially authorized search warrant in obtaining tracking information through

---

that is turned on will have its location remain private."); *see also Moorer*, 39 Misc. 3d at 615-16.

[55] *See Moorer*, 39 Misc. 3d at 618. ("People are not so oblivious that they are not aware that cellphones purchased today come with GPS technology which can pinpoint the location of the phone at any given time so long as it is turned on and the GPS technology has not been deactivated or disabled.")

[56] *See Wells*, 1275/13, NYLJ 1202666087234, at *8. *See also Moorer*, 39 Misc. 3d at 618.

the use of a cell phone.[57] That court reasoned that modern cellphones "blurred the lines" in terms of privacy concerns because location signals can be transmitted from both public and private places, which created an intrusion that "a reasonable person would not anticipate."[58] Legal commentators have also argued that a search warrant may be required to ping a cellphone based on the theory that such a ping is actually a physical trespass (albeit an electronic one) by the service provider at the behest of law enforcement.[59] While finding some support in tort law concepts, however, this theory has yet to be adopted by a court considering this particular issue.[60]

IV. Conclusion

Both *Moorer* and *Wells* provide meaningful guidance in terms of how the Fourth Amendment will be applied as it relates to receiving live Geolocation data, although certainty on the issue requires that it be taken up by higher courts. Until that time, however, government investigators do not need a search warrant to obtain Geolocation data from a cellphone in New York State. This also should apply to other devices that have pre-installed GPS capability.

---

[57] *See State v. Earls*, 214 N.J. 564, 586 (2013) ("Using a cell phone to determine the location of its owner can be far more revealing than acquiring toll billing, bank, or Internet subscriber records. It is akin to using a tracking device and can function as a substitute for 24/7 surveillance without police having to confront the limits of their resources. It also involves a degree of intrusion that a reasonable person would not anticipate.").

[58] *See id* (noting that the defendant was located in a motel room, not on a public highway).

[59] *See Criminal Procedure – Fourth Amendment – Sixth Circuit Holds that "Pinging" a Target's Cell Phone to Obtain GPS Data Is Not a Search Subject to the Warrant Requirement – United States v. Skinner, 690 F.3d 772 (6th Cir. 2012)*, reh'g and reh'g en banc denied, No. 09-6497 (6th Cir. Sept. 26, 2012), 126 HARV. L. REV. 802 (2013).

[60] *See id*. at 807.