Nebraska State Bar Association | Young Lawyers Section

Submissions to the Young Lawyers Section Page from young attorneys across the state are always welcome. If you're interested in writing, please contact Amy Prenda, Editor, at aprenda@nebar.com.

CSLI and Your New Privacy Rights:

How Our Nation's High Court Decided *Carpenter v. United States* and its Application in Nebraska

by Elizabeth J. Chrisp

Do you want to add another acronym to your vocabulary? If you practice criminal law and your clients have a cell phone, then CSLI, which stands for "cell site location information," should make your short list. Perhaps you are one of the millions of people who listened to the first season of the infamous podcast, *Serial*, and are familiar with CSLI's use in Adnan Syed's murder trial.[1] *Serial*'s host, Sarah Koenig, generally explained how CSLI is data that is recorded when your cell phone "pings" a tower throughout the day. She then detailed how that evidence was used by the prosecution in narrowing the location of Mr. Syed around the time Hae Min Lee went missing.[2] Technology, of course, has rapidly developed since Lee's disappearance in 1999.

Just last summer, the Supreme Court of the United States addressed how the government may lawfully obtain CSLI in *Carpenter v. United States*.[3] In a 5–4 decision, the Court held that law enforcement must generally obtain a warrant in order to obtain an individual's CSLI.[4] This article will explain how *Carpenter v. United States* expanded data privacy protections, how the Supreme Court of Nebraska has applied *Carpenter*, and how *Carpenter* may potentially have an impact on Fourth, and even Fifth, Amendment protections in the future.[5]

Carpenter v. United States

Carpenter explains that CSLI is information that wireless carriers collect and store for business purposes.[6] Each time a phone scans for the best signal looking for a cell site—something your phone may do several times a minute, even if you are not actively using it—time-stamped CSLI is generated.[7] Wireless carriers use this information for various reasons, such as determining when to charge you for roaming services.[8] Some even sell this information to data brokers.[9] The heart of the privacy issue with CSLI is the fact that it contains the user's geographic location.[10] How precise this location is varies on the geographic area covered by the cell site; the larger the concentration of cell sites, the smaller the coverage area.[11]

In *Carpenter*, law enforcement suspected that four men were involved in a series of robberies in Detroit.[12] One of the four suspects confessed that the group robbed nine stores across Michigan and Ohio.[13] He identified fifteen other accomplices and provided law enforcement with their cell phone numbers.[14] Based on that information, the government applied for court orders under the Stored Communications Act[15] to obtain cell phone records for the defendant and many other suspects.[16] The Stored Communications Act allows the government to compel disclosure of certain telecommunication documents when it offers "specific and articulable facts showing that there are reasonable grounds to believe" that the information is "relevant and material" to a pending criminal investigation.[17]

The applications were granted, and the government was allowed to obtain information regarding the defendant's CSLI with two wireless carriers over a period of approximately five months.[18] This amounted to "12,898 location points . . . an average of 101 a day." The government charged the defendant with multiple counts, including six counts of robbery.[19] After the defendant unsuccessfully attempted to suppress his CSLI, the government was able to argue at trial that the defendant was at or near the scene of multiple robberies.[20]

On appeal, Carpenter argued that the government had violated his Fourth Amendment right to be free from unreasonable searches and seizures.[21] The Court of Appeals for the Sixth Circuit disagreed and affirmed, reasoning that the defendant "lacked a reasonable expectation of privacy in the location information collected . . . because he had shared that information with his wireless carriers."[22]

The Sixth Circuit's ruling was based on the long-standing "third-party doctrine."[23] This doctrine generally provides that an individual loses his or her right to privacy in information that is voluntarily given to a third party.[24] That doctrine "remains true 'even if the information is revealed on the assumption that it will be used only for a limited purpose.'"[25] Carpenter appealed to the Supreme Court of the United States. Under the third-party doctrine and precedent at the time, Carpenter seemed to face an uphill battle.

Chief Justice Roberts delivered the opinion of the Court, beginning with this sentence: "There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people."[26] The Chief Justice explained how much of the Fourth Amendment's protection had stemmed from the common-law trespass doctrine which focused on the government *literally* intruding on a constitutionally protected area.[27] He also quoted, however, the ever-famous phrase that the Fourth Amendment protects "people, not places."[28] The Chief Justice

then explained how those "Founding-era understandings" were kept "in mind when applying the Fourth Amendment to innovations in surveillance tools." He acknowledged that "[a]s technology has enhanced" so has "the Government's capacity to encroach upon areas normally guarded from inquisitive eyes[.]"[29]

The Chief Justice then stated that the majority believed that the third-party doctrine was not applicable to Carpenter's "novel circumstances" and held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[30] "[T]ime stamped data," the Chief Justice wrote, "provides an intimate window into a person's life, revealing not only his particular movements but through them, his 'familial, political, professional, religious, and sexual associations."[31] As such, CSLI warrants constitutional protection. Now, law enforcement must generally obtain a warrant—requiring a showing of probable cause—in order to access CSLI.[32] The Chief Justice acknowledged, however, that there may be exceptions to the warrant requirement, including proof of exigent circumstances.[33]

Justices Kennedy, Thomas, Alito, and Gorsuch each wrote separate dissents, an unusual move that demonstrates their deep disagreement with the majority.[34] Justice Thomas and Justice Gorsuch complained on originalist grounds, protesting that the Court had moved beyond what the Framers intended. Justice Alito complained that the majority had overreacted to new technology. Finally, Justice Kennedy wrote that the Court had "unhinge[d]" the Fourth Amendment "from the property-based concepts that have long grounded" its "analytical framework."[35]

The Chief Justice, however, addressed the dissenting views, stating that the case was not just about "'using a phone' or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[36] Such information, he reasoned, implicates a "chronicle" of privacy concerns that go well-beyond those concerns addressed in the 1970's cases that the dissenters relied upon.[37] The third-party doctrine is not truly applicable to CSLI because CSLI is not voluntarily shared "as one normally understands the term."[38] Cell phones are now integrated in every aspect of American life and CSLI is captured "without any affirmative act on the part of the user beyond powering up."[39] The only way to stop CSLI from transmitting to the wireless carrier, is if the user disconnects entirely. Thus, in no meaningful sense does the user assume the risk of disclosing CSLI.[40]

Carpenter in Nebraska

Carpenter was examined for the first time in Nebraska in *State v. Brown* which was recently decided on January 18, 2019.[41] Following a denial of a suppression motion and conviction in the District Court of Douglas County, Brown appealed to the Nebraska Court of Appeals.[42] The Nebraska Supreme Court subsequently granted the State's unopposed Petition to Bypass on grounds that the appeal presented a novel question pursuant to Neb. Rev. Stat. § 24-1106(2) due to *Carpenter*'s conflict with *State v. Jenkins*.[43]

Brown was convicted of second degree murder and other firearm offenses arising out of the death of Carlos Alonzo.[44] Alonzo's had died from a single gunshot wound to the head near Doloma Curtis' home located by 20th and Lake Streets in Omaha.[45] Alonzo and Brown had both been dating Curtis at that time. As part of its investigation, law enforcement submitted an application to the district court under the Stored Communications Act seeking an order to obtain Brown's cell phone records, including his CSLI.[46] The application was granted.[47]

At a jury trial, the prosecution introduced evidence that Brown had called Curtis at 2:23 a.m. on May 28 and that his CSLI indicated that he was "in the area of 20th and Lake Streets when he made that call."[48] A minute later, at 2:24 a.m. "Omaha's 'ShotSpotter' location system detected a single gunshot in the vicinity of Curtis' home."[49] The prosecution also called a friend of Brown's as a witness who testified that in the early morning hours on May 28, Brown visited her home near 40th and Boyd.[50] She testified that Brown told her that he had just come from Curtis' home.[51] She testified that Brown explained to her how he "had been in an altercation with Alonzo, and that he 'had to put [Alonzo] down.'"[52] The prosecution also introduced Brown's CSLI that showed he was in the vicinity of 40th and Boyd at approximately 2:34 a.m.[53]

The jury found Brown guilty of second degree murder and other firearm offenses.[54] The district court sentenced him to 100 to 140 years' imprisonment.[55] Brown appealed his conviction, primarily arguing that the district court erred in denying his motion to suppress CSLI gathered by law enforcement in line with *Carpenter*.[56]

In a unanimous opinion authored by Justice Papik, the Nebraska Supreme Court affirmed Brown's conviction.[57] Justice Papik explained that the district court denied Brown's motion to suppress CSLI pursuant to a Supreme Court of Nebraska case, *State v. Jenkins*, which was decided in 2016, just two months after law enforcement obtained Brown's CSLI.[58] *Jenkins* "held that individuals do not have a reasonable expectation of privacy in CSLI and that thus, the acquisition of CSLI does not implicate, let alone violate, the Fourth Amendment."[59] After Brown initiated his appeal, however, *Carpenter* was decided, overruling *Jenkins*.[60]

Those perhaps unfamiliar with Fourth Amendment law may have thought that with this landscape, Brown's appeal would be successful; Justice Papik quickly stated, however, that "[t]he fact that Brown's Fourth Amendment rights were violat-

ed . . . does not necessarily mean that it was error for the district court to deny Brown's motion to suppress."[61] The exclusionary rule, he explained, is "not a personal constitutional right" and was judicially created to safeguard Fourth Amendment violations through its deterrent effect.[62]

Justice Papik then stated that there are, at least, four categorical instances where the exclusionary rule did not apply, and that one of those applied with "full force" in Brown's case.[63] In *Illinois v. Krull*, the Supreme Court of the United States held that the exclusionary rule did not apply where evidence was gathered by law enforcement who objectively relied on a statute that was later found to be unconstitutional.[64] In Brown's case, his CSLI was gathered by law enforcement pursuant to an order that granted an application that was filed under the Stored Communications Act. Although *Jenkins* had not yet been decided, many other courts, including the Fourth, Fifth and Eleventh Circuit Courts of Appeals, had held that CSLI did not implicate the Fourth Amendment.[65] Justice Papik explained that because law enforcement in *Brown* was following the current status of the law at that time, application of the exclusionary rule was not appropriate—it would not have any deterrent effect.[66] He noted that "[m]any other courts" have ruled the same post-*Carpenter*.[67]

So, if you were contemplating a potential appeal of a case that involved law enforcement obtaining CSLI pre-*Carpenter*, *Brown* makes it clear that if law enforcement was objectively relying upon the Store Communication Act, you should find another error to assign.

Potential Expansion from the Fourth to the Fifth

While *Carpenter* was a Fourth Amendment case, the question becomes, how far will Carpenter reach? While it may still be too early to tell, *Carpenter*, combined with other Supreme Court cases like *Riley v. California*,[68] create a foundation for additional arguments into the Fifth Amendment realm. *Riley*, if you may recall, held that an unlocked smartphone cannot be searched incident to arrest other than to determine whether it may be used as a weapon.[69] *Carpenter* and *Riley*, for example, can be used to argue that evidence of a defendant's ownership, use, or control of cell phone is testimonial under the Fifth Amendment.

Using similar reasoning, cases outside of our jurisdiction have held that the government cannot force a suspect to disclose biometric information, such as a fingerprint, thumbprint, face or iris scan, to unlock a smart phone.[70] At least one magistrate judge has reasoned that a finger or thumb scan is different than submitting a fingerprint or DNA to compare with physical evidence.[71] That magistrate reasoned the difference is what the finger or thumb scan is used for: granting government access to private information and to authenticate ownership or access.[72] Hence, the magistrate found that a finger's or thumb's use in that manner "is analogous to the nonverbal, physiological responses elicited during a polygraph test, which are used to determine guilt or innocence, and is considered testimonial."[73]

To be clear, not all judges have ruled like the magistrate above.[74] Those opinions, nonetheless, are instructive in crafting arguments here in Nebraska.

Conclusion

The Supreme Court of the United States once again moved beyond the rigid approach of Fourth Amendment law that has been following two steps behind advancements in technology. This is important because courts across the nation are recognizing that there are multiple privacy concerns which now include the disclosure of CSLI. How *Carpenter*'s decision, in conjunction with others, like *Riley*, will affect other aspects of criminal law is unknown. Defense attorneys, however, cannot ignore the landscape we have been given. Will this protection expand to other privacy areas such as internet protocal (IP) addresses and general forms of metadata? Only time will tell.

ELIZABETH CHRISP *is an Associate at Jacobsen, Orr, Lindstrom & Holbrook, P.C., L.L.O. and practices in a variety of areas, including criminal law. Ms. Chrisp obtained her Juris Doctor degree, with Sterling Honors, from the University of South Dakota School of Law in 2015. While in law school, she was Editor-in-Chief of the South Dakota Law Review, Volume 60. After graduation, she competed a one-year clerkship with the Honorable Roberto Lange at the United States District Court for the District of South Dakota. Through that clerkship, Ms. Chrisp was exposed to many aspects of criminal law, particularly serious felony cases occurring on Native American reservations.*

Endnotes

1 *See* Michelle Kaminsky, *In a Win for True Crime Podcasts Everywhere, Adnan Syed Granted New Trial*, Forbes (Mar. 30, 2018), https://www.forbes.com/sites/michellefabio/2018/03/30/in-win-for-true-crime-podcasts-everywhere-adnan-syed-granted-new-trial/#390a3cee2769.

2 *Serial, This American Life* (2015), https://serialpodcast.org/season-one.

3 138 S. Ct. 2206 (2018).

4 *Id.* at 2223.

5 I have always been amazed at how the high Court applies the Fourth Amendment in a society that continues to evolve. If you would like a detailed history of the Fourth Amendment with multiple citations included, *see Paws Off My Porch: Sniffing Out Florida v. Jardines' Effect on Drug Dogs and Homes*, 59 S.D. L. Rev. 109 (2014). That article details how the Supreme Court applied the archaic, property-based search analysis to hold that a warrantless drug dog sniff of a home was unlawful. *Id.*

6 *Carpenter*, 138 S. Ct. at 2211–2212.

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.* at 2212.

[13] *Id.*

[14] *Id.*

[15] 18 U.S.C. §§ 2701–2713.

[16] *Id.*

[17] 18 U.S.C. § 2703(d).

[18] *Carpenter*, 138 S. Ct. at 2212.

[19] *Id.*

[20] *Id.*

[21] *Id.* at 2212–13.

[22] *Id.*

[23] *See id.*

[24] *Id.* at 2216.

[25] *Id.* (quoting *United States v. Miller*, 425 U.S. 435, 443 (1976)).

[26] *Id.* at 2211.

[27] *Id.* at 2213.

[28] *Id.* (citing *United States v. Jones*, 565 U.S. 400, 405 (2012); *Smith v. Maryland*, 442 U.S. 735 740 (1979)).

[29] *Id.* at 2214.

[30] *Id.* at 2217.

[31] *Id.* (quoting Jones, 565 U.S. at 415).

[32] *Id.* at 2221.

[33] *Id.* at 2222–23.

[34] *Id.* at 2223–72 (spanning all dissents)

[35] *Id.* at 2224 (Kennedy, J., dissenting)

[36] *Id.* at 2220 (majority opinion).

[37] *Id.* (citing *Smith*, 442 U.S. 735; *Miller*, 425 U.S. 435).

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] 302 Neb. 52, ___ N.W.2d ___ (Neb. 2019).

[42] *Id.* at 58.

[43] *Id.*; *State v. Brown*, A-17-1039 (Neb. Ct. App. July 24, 2018); *State v. Brown*, A-17-1039 (Neb. Ct. App. July 25, 2018) (citing *Carpenter* was in direct conflict with *State v. Jenkins*, 294 Neb. 684, 884 N.W.2d 429 (2016)).

[44] *Id.* at 55.

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] *Id.* at 56.

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] *Id.* at 57.

[54] *Id.*

[55] *Id.*

[56] *Id.* at 55.

[57] *Id.*

[58] *Id.* at 60.

[59] *Id.* (citing *Jenkins*, 294 Neb. at 702, 884 N.W.2d at 443–44).

[60] *Id.*

[61] *Id.*

[62] *Id.* at 61 (quotations and citations omitted).

[63] *Id.* (citations omitted).

[64] *Illinois v. Krull*, 480 U.S. 340, 358–59 (1987).

[65] *Brown*, 302 Neb. at 62 (citations omitted).

[66] *Id.*

[67] *Id.*

[68] 134 S. Ct. 2473 (2014).

[69] *Id.* at 2485–95

[70] *Matter of Residence in Oakland, California*, No. 4-19-70053, 2019 WL 176937, at *5 (N.D. Cal. Jan. 10, 2019).

[71] *Id.* at *3–4.

[72] *Id.*

[73] *Id.* (citing *Schmerber v. California*, 384 U.S. 757, 764 (1966)).

[74] *See* Mandy Wakely, *California Judge Makes Major Decision in Biometric Privacy Rights*, Bigger Law Firm (Feb. 1, 2019), https://www.biggerlawfirm.com/california-judge-makes-major-decision-in-biometric-privacy-rights/ (stating that a district judge overruled another magistrates similar ruling in Illinois in 2017). This author was unable to find that Illinois decision.