NOT TO BE PUBLISHED WITHOUT
THE APPROVAL OF THE COMMITTEE ON OPINIONS

SUPERIOR COURT OF NEW JERSEY
MORRIS COUNTY
LAW DIVISION, CRIMINAL PART
INDICTMENT NO. 18-08-0647

STATE OF NEW JERSEY,

Plaintiff,

v.

KELVIN BRIGGS,

Defendant.

APPROVED FOR PUBLICATION

September 19, 2022

COMMITTEE ON OPINIONS

———————————————

Decided: July 15, 2019.

Melissa Ercolano, Assistant Prosecutor, for plaintiff (Robert J. Carroll, Morris County Prosecutor, attorney).

Sean O'Connor, Assistant Deputy Public Defender, attorney for defendant (Joseph E. Krakora, Public Defender, attorney)

IRONSON, J. S. C.,

This matter comes before the court by way of defendant's Motion to Suppress internet protocol (IP) address data. The State has filed opposition. Oral argument was held on June 19, 2019.

By way of background,[1] on or about November 17, 2017, Sergeant Sean Krater of the Jefferson Township Police Department issued an Emergency Disclosure Request to TextNow, Inc., the service provider for telephone number (XXX)-XXX-7448, requesting the customer's name, email address and recent IP addresses used. On this same date, Sergeant Krater received subscriber information as well as an IP address log between the dates of November 15, 2017, and November 17, 2017, containing the following IP addresses: 24.120.54.20, 24.120.124.196, 24.120.144.34, 64.79.144.10 and 24.120.55.69.

A subsequent subpoena to Cox Communications revealed that IP address 24.120.54.20 belonged to Bally's Las Vegas Hotel & Casino; IP address 24.120.124.196 belonged to the Platinum Hotel in Las Vegas; IP address 24.120.144.34 belonged to the Wynn Las Vegas; and IP address 24.120.55.69 belonged to the Flamingo Las Vegas. A grand jury subpoena to the Venetian revealed that IP address 64.79.144.10 belonged to the Venetian Casino Resort in Las Vegas.

On November 28, 2018, the State issued a grand jury subpoena to Google for subscriber information and IP information, including IP history logs,

[1] These facts are from the State's Statement of Facts. Defense counsel did not provide a detailed Statement of Facts.

between August 1, 2017, and November 27, 2017, for email addresses: kxxxxxxxxx@gmail.com and kbxxxxxxxx0@gmail. com.

On December 1, 2017, the State issued a grand jury subpoena to Google for subscriber information and IP information, including IP history logs, between August 1, 2017, and November 30, 2017, for email address: cxxxxxxxxxxxx@gmail.com.

On January 18, 2018, the State issued a grand jury subpoena to Google for subscriber information and IP information, including IP history logs, between August 1, 2017, and November 28, 2017, for email addresses: fxxxxxxxxxx@gmail.com and dxxxxxxxx@ gmail.com.

On December 4, 2018, Google provided subscriber and IP information for kxxxxxxx@gmail.com and kbrxxxxxxx0@gmail.com. On December 12, 2017, Google provided subscriber and IP information for Cxxxxxxxxxxxx@gmail.com. On January 19, 2018, Google provided subscriber and IP information for fxxxxxxxx@gmail.com and dxxxxxxxxx@gmail.com.

The IP addresses from the Google subpoena returns contained IP addresses for Bally's Las Vegas Hotel & Casino and the Platinum Hotel in Las Vegas, as well as other unidentified IP addresses.

In support of defendant's motion, defendant argues that IP address data is akin to cell-site location information (CSLI) which was afforded protection by the United States Supreme Court in Carpenter v. U.S., ___ U.S. ___, 138 S. Ct. 2206 (2018). Defendant contends that like CSLI data, IP address data should be considered location data that requires a warrant. Defendant also cites a scholarly article in support of this proposition.

In opposition, the State maintains that IP address data does not require a warrant as it is not analogous to CSLI. The State submits that under the third-party doctrine established in U.S. v. Miller, 425 U.S. 435 (1976) and Smith v. Maryland, 442 U.S. 735 (1979), a defendant does not have a reasonable expectation of privacy in his location when he shares it with internet providers by logging into their network. As such, the State maintains that a warrant was not required to access the IP address data.

The Fourth Amendment of the United States Constitution, and Article I of the New Jersey Constitution, protect people from unreasonable searches and seizures. See U.S. Const. amend. IV; N.J. Const. art. I, ¶ 7; State v. Davila, 203 N.J. 97, 111 (2010); State v. Dickey, 152 N.J. 468, 475 (1998). The New Jersey State Constitution, through article I, paragraph 7, provides congruent guarantees against unreasonable searches and seizures by the State. State v. Macri, 39 N.J. 250, 256 (1963) (stating that the New Jersey State Constitution, while mirroring

the Federal Constitution, provides greater protection for its citizens). The Federal and State Constitutions bar only "unreasonable" searches and seizures. State v. McKnight, 52 N.J. 35, 58 (1968). The Fourth Amendment generally requires that the government obtain a warrant based on probable cause before conducting a search. Katz v. United States, 389 U.S. 347 (1967). For an "intrusion into [the] private sphere" to constitute a "search," a defendant must "seek to preserve something as private," and "society [must be] prepared to recognize [that privacy expectation] as reasonable." Carpenter, 138 S. Ct. at 2213 (quoting Maryland, 442 U.S. at 740).

In Carpenter, the issue before the United States Supreme Court was whether the government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of a user's past movements. Id. at 2211. There, after the cell phone numbers of robbery suspects were obtained, prosecutors were granted court orders to obtain the suspects' cell phone records under the Stored Communications Act. Id. at 2212 (citing 18 U.S.C. § 2703(d)). As a result, wireless carriers produced CSLI for one defendant, which revealed 12,898 location points cataloging the defendant's movements over 127 days, an average of 101 data points a day. Ibid. The United States Supreme Court held that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured

through CSLI and that the government will generally need a warrant to access CSLI. Id. at 2217, 2222.

In so holding, the Court analyzed how CSLI is generated. Id. at 2211. The Court reasoned that "[c]ell phones continuously scan their environment looking for the best signal . . . [m]ost modern devices . . . tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features." Ibid. Each time a cell phone connects to a cell site, it generates a time-stamped record known as CSLI. The "precision of this information depends on the size of the geographic area . . . modern cell phones generate increasingly vast amounts of increasingly precise CSLI." Id. at 2212-13. The Court noted that CSLI "partakes of many of the qualities of GPS monitoring . . . [m]uch like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic and effortlessly compiled." Id. at 2216. The Court reasoned that "[m]aping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts . . . the time-stamped data 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." Id. at 2217 (internal citation omitted). Thus, when the "government tracks the location of a cell

phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." Id. at 2218.

The Carpenter Court declined to extend the third-party doctrine to CSLI. The Court reasoned that the third-party doctrine stems from the notion that an individual has a reduced expectation of privacy in information "knowingly shared with another." Id. at 2219. The doctrine also considers the nature of the documents sought in order to determine whether there is a legitimate expectation of privacy concerning their contents. Ibid. (citation and quotation omitted).

The third-party doctrine was largely developed in Miller, 425 U.S. at 435. There, the United States Supreme Court held that an individual does not have a reasonable expectation of privacy in bank records as they were business records of the bank and exposed to the bank in the ordinary course of business. Ibid. The Court reasoned that the defendant "had taken the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government." Carpenter, 138 S. Ct. at 2216. After Miller, the Court extended the third-party doctrine to telephone records. In Smith, the United States Supreme Court held that an individual does not have a reasonable expectation of privacy in telephone numbers since the caller voluntarily conveyed the dialed number to the telephone company. 442 U.S. at 743. Additionally, the caller assumed the risk that the company's records would be

divulged to police. Carpenter, 138 S. Ct. at 2216-17 (citing Smith, 442 U.S at 744-45).

The Carpenter Court distinguished Miller and Smith on the basis that CSLI is "qualitatively different" from telephone records and bank records as CSLI "chronicles a person's past movement through the record of his cell phone signals" and it is obtained without an "affirmative act on the user beyond powering up." Id. at 2216-17. The Court likened CSLI to GPS monitoring and cited United States v. Jones, 565 U.S. 400, 405 (2012), where FBI agents installed a GPS tracking device on the defendant's vehicle and monitored the vehicle's movements for 28 days. The Jones Court reasoned that because GPS monitoring tracks "'every movement' a person makes in that vehicle . . . [it] impinges on expectations of privacy regardless [of] whether those movements were disclosed to the public." Id. at 2215. The Carpenter Court noted that CSLI creates a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years." Id. at 2220. The Court reasoned that CSLI is even more invasive as "[u]nlike GPS device[s] . . . police need not even know in advance whether they want to follow a particular individual" and that the user "has effectively been tailed every moment of every day for five years . . . ." Id. at 2218.

In reaching its holding, the Court indicated that its decision was "a narrow one" and does not "disturb the application of Smith and Miller." Id. at 2220.

In the present matter, defendant argues that CSLI is akin to IP address data and that same should be afforded the protections that CSLI is guaranteed under the Fourth Amendment. This issue is one of first impression in New Jersey.

The New Jersey Constitution protects an individual's privacy interest in the subscriber information that he or she provides to an internet service provider. State v. Reid, 194 N.J. 386, 398 (2008). In Reid, the Court reasoned that the New Jersey Constitution affords citizens greater protection against unreasonable searches and seizures than the Fourth Amendment and thus federal case law. Id. at 396. The Court highlighted the fact that "[i]ndividuals need an ISP address in order to access the Internet. However, when users surf the Web from the privacy of their homes, they have reason to expect that their actions are confidential." Id. at 398. The Court further highlighted the fact that while "IP addresses do not reveal the content of Internet communications, subscriber information alone can tell a great deal about a person. With a complete listing of IP addresses, one can track a person's internet usage." Ibid. With this information, "[t]he government can learn the names of stores at which a person shops, the political organizations a person finds interesting, a person's . . . fantasies, her health concerns, and so on." Ibid. (citing Daniel Solove, The

Future of Internet Surveillance Law, 72 Geo. Wash. L. Rev. 1264, 1287 (2004)). This information reveals "intimate" details about one's personal affairs. Id. at 398-99. Law enforcement in Reid utilized a defective municipal subpoena to obtain the defendant's information. The Court did not hold that a warrant was required to obtain the IP address information and did not bar the State from utilizing this information. Rather, the Court indicated that the State may dismiss the pending indictment, serve a proper grand jury subpoena on Comcast, and seek a new indictment. Id. at 407.

Moreover, the First Circuit has declined to extend the Fourth Amendment protections of CSLI to IP address data. In U.S. v. Hood, 920 F.3d 87, 92 (1st Cir. 2019), the court held that the defendant did not have a reasonable expectation of privacy in IP address data. The defendant argued that under Carpenter, the third-party doctrine should not apply to IP address information that the government gathered from a smartphone company. The court distinguished CSLI from IP address data on the basis that an internet user generates IP address data by making an affirmative decision to access a website or application, whereas CSLI is generated without the user "lifting a finger." Ibid. The court further distinguished CSLI on the basis that IP address data does not convey any location information. Ibid. The data is "merely a string of numbers associated with a device that had, at one time, accessed a wireless

network. By contrast, CSLI itself reveals - - without any independent investigation – the (at least approximate) location of a cell phone user who generates that data simply by possessing the phone." Ibid.

Thereafter, in U.S. v. Morel, 922 F.3d 1 (1st Cir. 2019), the First Circuit revisited IP address data. There, the defendant uploaded child pornography to an image hosting website, Imgur. Id. at 3. The National Center for Missing and Exploited Children (NCMEC) received an anonymous report regarding suspected child pornography. NCMEC alerted Imgur to the images and Imgur provided the IP address data to the NCMEC. Using a publicly available website, NCMEC looked up the IP address information and learned that it was associated with a Comcast subscriber. Law enforcement learned of the images on Imgur from the NCMEC. Ibid. Upon receiving the reports, law enforcement entered the IP address data from the report into a publicly available website and learned that it was associated with a Comcast account. Law enforcement then obtained a subpoena requesting information from Comcast regarding the owner of the IP address. Id. at 4. The defendant there argued that under Carpenter, the third-party doctrine should not apply to IP address data that the government gathered from the smartphone messaging company. Id. at 9. The District Court for the District of New Hampshire rejected this argument. Ibid. The First Circuit affirmed on the basis of Hood and recognized that "IP address information of

the kind and amount collected here – gathered from an internet company – simply does not give rise to the concerns identified in Carpenter." Id. at 9. Thus, the court held that the defendant did not have a reasonable expectation of privacy in the IP address data that the government obtained. Ibid.

Furthermore, the Fifth Circuit has declined to extend the Fourth Amendment protections of CSLI to IP address data. In United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018), the court held that IP address data fell "comfortably within the scope of the third-party doctrine" because "[t]hey had no bearing on any person's day-to-day movement." The court further noted that the defendant "lacked a reasonable expectation of privacy in that information." Ibid.

Based on the foregoing, this court concludes that IP address data should not be afforded the same protections as CSLI. The Carpenter "decision is a narrow one." Carpenter, 138 S. Ct. at 2220. An internet user, such as defendant, generates IP address data by affirmatively accessing a website or application. Conversely, "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering" and "apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data." Ibid. As stated in Hood, a "cellphone sitting untouched in a suspect's pocket is continually chronicling that user's

movements through the day." Hood, 920 F.3d at 92. In the present matter, defendant made a conscious choice, and engaged in an affirmative act, to access a website or application while using public WiFi, connected to an IP address.

Moreover, the proofs in the present matter fail to establish that the IP address data obtained "near perfect surveillance" of defendant. IP address data reveals where a user accessed the internet, but it cannot create a "detailed and comprehensive record of the person's movements." Carpenter, 138 S. Ct. at 2217. In this case, it revealed that the IP addresses belonged to Bally's Las Vegas Hotel & Casino, Platinum Hotel in Las Vegas, Wynn Las Vegas, Flamingo Las Vegas and the Venetian Casino & Resort in Las Vegas. Unlike Carpenter, where the CSLI catalogued the defendant's movements over the course of 127 days and generated "12,868 location points – an average of 101 data points per day[]", these records did not track defendant's movements over the course of four months. Instead, these records generated limited information regarding where the user accessed the internet from fixed locations.

Therefore, based on the above, the State did not require a warrant to obtain the IP address data. IP address data does not generate the privacy concerns enunciated in Carpenter. Furthermore, the State complied with the provisions of Reid by obtaining a grand jury subpoena for the IP address data. Accordingly, defendant's Motion to Suppress is DENIED.