

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF ARKANSAS**

|                                 |   |                            |
|---------------------------------|---|----------------------------|
| <b>UNITED STATES OF AMERICA</b> | ) |                            |
|                                 | ) |                            |
| <b>V.</b>                       | ) | <b>No. 4:17CR00145 BSM</b> |
|                                 | ) |                            |
| <b>EDGAR K. RIDDICK</b>         | ) |                            |

**MOTION TO SUPPRESS EVIDENCE OBTAINED FROM WARRANTLESS SEIZURE  
FROM CHATSTEP**

This case is about law enforcement gathering comprehensive records that track a user’s movements from chatroom to chatroom without a warrant. The Little Rock Police Department obtained almost a year-and-a-half worth of data from Chatstep – a chatroom hosting website -- of Riddick’s movements (or who they believe was Riddick) through various chatrooms. Since the records were obtained without a warrant, Riddick, through his attorneys, J. Blake Hendrix and Annie Depper of Fuqua Campbell, P.A., moves to suppress the data.

**I.**

Riddick is charged in a four-count indictment with possessing child pornography on February 23, 2017, a violation of 18 U.S.C. §2252(a)(4)(B), and three counts of distributing child pornography -- on May 30, 2016 (Count 2), January 4, 2017 (Count 3), and February 2, 2017 (Count 4), violations of 18 U.S.C. §2252(a)(2).

On May 30, 2016, Chatstep, a third-party conferencing platform, reported to the National Center for Missing and Exploited Children (“NCMEC”) that an individual uploaded an image of suspected child pornography while logged in to one of its chatrooms. Chatstep reported that a person using the screenname “Missy” uploaded the image on May 30, 2016, at 4:17:54 UTC (Coordinated Universal Time) while in a chatroom named “Nuderoom” using the IP Address 71.238.241.25.

On August 17, 2016, a Deputy Prosecuting Attorney with the Office of the Pulaski County Prosecutor executed a subpoena duces tecum directing that Chatstep supply “[a]ny and all records regarding the identification of the individual using the IP address 71.238.241.25” on May 30, 2016 at 4:17:54 UTC. These records track “Missy’s” movements from room to room by listing scores of instances from March 30, 2015, to August 18, 2016, when the screenname “Missy” with an IP address of 71.238.241.25 entered a Chatstep chat room. As an example, the first entry shows that “Missy” entered room “mj34” on September 29, 2015, at 4:36:40 UTC<sup>1</sup>; the second entry shows that “Missy” entered room “mj34” on September 29, 2015, at 4:48:44 UTC, and so on through August 18, 2016. Relevant to Count 2 of the indictment is an entry showing that “Missy” entered “Nuderoom” on May 30, 2016, at 4:02:15.435 UTC.

NCMEC received another referral from Chatstep on January 4, 2017, reporting that an individual using the screenname “Missy” entered room “momsonx”, port 51420, using the IP address 2601:381:8105:1e30:459f:6048:d5f8 and uploaded one image of suspected child pornography on January 4, 2016, at 14:58:58 UTC. Chatstep later provided law enforcement with seven pages of data related to the IP address from November 4, 2016, to February 20, 2017 – over three months. The data, as before, tracks the movements of the IP address from room to room. Relevant to Count 3, the records show that “Missy” entered room “momsonx” using the IP address on January 4, 2017, at 14.44.31.52 UTC.

The discovery material we’ve reviewed does not reveal the process by which law enforcement received this information from Chatstep – no subpoena, order, or warrant.

On February 2, 2017, Chatstep reported to NCMEC that someone using the screenname “ccc” entered room “office” using IP address 2601:381:8105:1e30:8438:8cd8:e193:5499 and

---

<sup>1</sup> UTC time is five hours ahead of Central Daylight Savings Time (CDT). “Missy” entered the room at 11:46 p.m. CDT.

uploaded one image of suspected child pornography on January 2, 2017, at 19:53:37 UTC. Law enforcement received a page of data from Chatstep that tracked the movements of this IP address from room to room from November 4, 2016, to February 20, 2017. Relevant to Count 4, the data show that “ccc” entered room “office” on January 2, 2017, at 19:44:43.447 UTC.

The discovery material we’ve reviewed does not reveal the process by which law enforcement received this information from Chatstep – no subpoena, order, or warrant.

Further investigation revealed that Comcast owned all three IP addresses and that the addresses were registered to Riddick.

## **II.**

### **A.**

The Fourth Amendment provides,

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Amendment protects people from government intrusion in to those places in which we have a reasonable expectation of privacy. *Oliver v. United States*, 466 U.S. 170, 177 (1983) (“Since Katz v. United States, 389 U.S. 347 (1967), the touchstone of Fourth Amendment analysis has been the question whether a person has a ‘constitutionally protected reasonable expectation of privacy.’”).

### **B.**

On June 22, 2018, the Supreme Court held that the warrantless seizure of cell-site-location-information (“CSLI”) violates the Fourth Amendment. *Carpenter v. United States*, 585 U.S. \_\_\_\_ (2018). CSLI is non-content data a smartphone generates when it emits a signal. That

signal pings off of the closest cell tower and records the time of the signal and the location of the tower. The wireless service provider collects the information and stores it on its servers. The CSLI is a record that tracks the movement of the cell phone's user.

Carpenter was suspected of being a member of a ring of robbers in the Detroit area. After four members were arrested, one incriminated Carpenter and gave the police Carpenter's cell phone number. A prosecutor then obtained a court order under the Stored Communications Act to obtain Carpenter's CSLI for a four-month period. The CSLI tracking information revealed that Carpenter's phone was near four of the robberies when they occurred. Based largely on the strength of the tracking records, Carpenter was convicted. *Id.* at \_\_\_\_ (slip opinion at 3-4).

Before trial, Carpenter moved to suppress the CSLI arguing that a warrant, not a SCA court order, was required to obtain the data. The District Court denied the motion and the Sixth Circuit affirmed, holding that Carpenter did not have a reasonable expectation of privacy in non-content information stored by a third party (his wireless carrier).

The Supreme Court reversed, holding, "Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one – get a warrant." *Id.* at \_\_\_\_ (slip opinion at 19). The Court reasoned through two lines of cases: the first, cases that involve the Government's tracking of our movements; the second, cases that involve information we voluntarily turn over to someone else (the third-party doctrine). *Jones v. United States*, 565 U.S. 400 (2012), controlled the first. In *Jones*, FBI agents, without a proper warrant, placed a GPS tracking device on Jones' car that allowed agents to monitor Jones' movements for 28 days, a physical trespass on Jones' property that the Court found offended the Fourth Amendment. In *Carpenter*, the Court adopted the reasoning of the concurring justices in *Jones*, finding,

Since GPS monitoring of a vehicle tracks 'every movement' a person makes in that vehicle, the concurring Justices concluded that 'longer term GPS monitoring

in investigations of most offenses impinges on expectations of privacy’ – regardless whether those movements were disclosed to the public at large. *Carpenter*, 585 U.S. at \_\_\_\_ (slip opinion at 8).

The second line of cases involve the third-party doctrine. The Court acknowledged that it had previously held that a person has no reasonable expectation of privacy in information he voluntarily turns over to third parties. A person, for instance, cannot reasonably expect his business records maintained by his bank to be private (*United States v. Miller*, 425 U.S. 435 (1976)) or the telephone numbers he dials that are maintained by his telephone company (*Smith v. Maryland*, 442 U.S. 735 (1979)). But, the Court found, CSLI is qualitatively different.

CSLI, like GPS data, provides time-stamped location information that “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.’” *Carpenter*, 585 U.S. at \_\_\_\_ (slip opinion at 12), quoting *Jones v. United States*, 565 U.S. at 415. “These location records,” the Court stated, “hold for many Americans the ‘privacies of life.’” *Id.* at \_\_\_\_ (slip opinion at 12, quoting *Riley v. California*, 573 U.S. \_\_\_\_, at \_\_\_\_ (slip opinion at 28)). The Court held that tracking this information for as little as seven days implicated the Fourth Amendment.

The Court in *Carpenter* recognized a new category of information subject to Fourth Amendment protection: non-content based information that tracks our movements. Without a properly issued warrant, the Government may not obtain this sensitive information.

### III.

Content-based information – letters, emails, and other communications – have always been presumed to be protected by the Fourth Amendment. See *Ex Parte Jackson*, 96 U.S. 727 (1878) (letters); *United States v. Warshak*, 631 F.3d 266 (6<sup>th</sup> Cir. 2010) (emails). *Carpenter* created a category of non-content information that deserves Fourth Amendment protection – cell site location information. This is so, because CSLI tracks a user’s movements. The

Government's ability to track one's movements, the Court found, reveals a user's "familial, political, professional, religious, and sexual associations." In other words, the "privacies of life." *Id.*

*Carpenter* involved the Government's ability to track one's movements in the physical world for seven days. This case involves the Little Rock Police Department's tracking of Riddick's movements in the virtual world for a year and a half. Because there is no meaningful distinction between tracking one's movements in the physical world and tracking one's movements in the virtual world, chatroom-tracking data, like cell phone tracking data, is protected by the Fourth Amendment.

Tracking a user's movements from chatroom to chatroom implicates the same privacy concerns the Court found are implicated in tracking one's movements in the physical world – it reveals the privacies of our lives. The internet provides endless chatroom platforms. A brief review of three such platforms demonstrates the personal nature of the chatrooms. The chatroom platform Wireclub, [www.wireclub.com](http://www.wireclub.com), provides chatrooms covering numerous topics. Some of the chatrooms available on Wireclub are:

- No Strings Attached
- Mental Health Support Group
- Lesbian Café
- Crossdressandtransgender
- Jesus Christ 101
- Catholic Theology
- Espanglishchat
- Support for Survivors
- Atheism

Buzzen, [www.buzzen.com](http://www.buzzen.com), another chatroom platform hosts chatrooms labeled:

- Politics Without Borders
- America! LoveIt-HateIt! Debate It!
- The Chronic Pain Cooperative

- Chat Evangelico
- Politics Firearms and the 2nd Amendment

Chatstep, [www.chatstep.com](http://www.chatstep.com), the chatroom platform at issue in the instant case, also supports chatrooms with various topics. They include:

- ChristianChatOldTime
- WorldCupEnjoyment
- USAIndians123
- UKEastMidlandChat
- Scuba
- ChurchChat
- USjobportal
- ChristianWorld
- MarriedAndMiserable

To be sure, not all of these rooms are associated with the privacies of individuals' lives, but many are. They touch deeply personal topics like religion, mental health, politics, domestic abuse, ethnic identity, personal relationships, and professional advancement.

In *Carpenter*, the Court emphasized that CSLI provides “an intimate window into a person’s life”, revealing that person’s “familial, political, professional, religious, and sexual associations.” These are the “privacies of life” that require protection under the Fourth Amendment. As in *Carpenter*, the records obtained in this case reveal the privacies of an individual’s life. By obtaining records pinpointing an individual’s movement through chatrooms, the government uncovers information related to an individual’s “familial, political, professional, religious, and sexual associations”. If the records indicate that an individual frequents the “Lesbian Café” or “Crossdressandtransgender” chatrooms on Wireclub, the government then has knowledge of that individual’s sexual orientation. Records showing an individual’s entry into the “Jesus Christ 101” or “Atheism” chatrooms on Wireclub, the “Chat Evangelico” chatroom on Buzzen, or the “ChristianChatOldTime” chatroom on Chatstep provide information on that

individual's religious or non-religious affiliation. Involvement in the "Politics Firearms and the 2nd Amendment" chatroom on Buzzen indicates an individual's position on the 2nd Amendment. Records revealing that an individual frequents the "Mental Health Support Group" chatroom on Wireclub tell the government that the individual struggles with mental health. Records indicating that an individual frequents the "MarriedAndMiserable" chatroom on Chatstep informs the government that the individual has marital problems. Such records acquired by the government provide a roadmap of an individual's personal life.

The *Carpenter* Court determined that individuals maintain a reasonable expectation of privacy in CSLI. The expectation of privacy on chatroom platforms, however, is even greater and more reasonable than an individual's expectation of privacy with respect to CSLI. CSLI identifies the physical location of an individual. Because that individual exists in the physical world, they may be seen by others in locations they frequent. An individual's expectation of privacy in CSLI is therefore somewhat limited. In chatrooms, that is not the case. A participant in chatrooms may move in and out of them without recognition by others. The vast majority of individuals in chatrooms choose a username that is not their own name. They prefer this anonymity. Indeed, people may choose to explore their sexuality, their religion, their politics, their mental health concerns, in the anonymous world of the internet so that they may avoid being recognized in physical locations that would indicate personal preferences, beliefs, or struggles - a homosexual club, a religious facility, the location of a support group, or a political rally.

Further, unlike cellular providers that collect CSLI, the majority of chatroom platforms do not require any type of registration or account creation. This is even greater evidence of a reasonable expectation of privacy in records identifying entry into chatrooms. Users do not need

to create an account to participate. They simply enter a username and they can begin chatting. This is likely part of the draw. It reinforces a user's sense of anonymity, of privacy.

Records from chatroom platforms identifying the rooms that a user frequents reveal the exact personal aspects of an individual's life that concerned the *Carpenter* Court. Chatroom platform users have a reasonable expectation of privacy to those records. As such, prior to obtaining those records, the government must obtain a warrant.

#### IV.

The government obtained volumes of records tracking Riddick's movement through numerous chatrooms. It tracked his movements for a year-and-a-half, revealing the privacies of his life. But, it didn't get a warrant. The evidence, therefore, should be suppressed.

Respectfully submitted by,

/s/ J. Blake Hendrix  
J. Blake Hendrix  
Arkansas Bar No. 86066  
Fuqua Campbell P.A.  
Riviera Tower  
3700 Cantrell Road, Ste. 205  
Little Rock, AR 72202  
(501) 975-7123 (direct dial)  
bhendrix@fc-lawyers.com

and

/s/ Annie Depper  
Annie Depper  
Arkansas Bar No. 2009267  
Fuqua Campbell P.A.  
Riviera Tower  
3700 Cantrell Road, Ste. 205  
Little Rock, AR 72202  
(501) 975-7144 (direct dial)  
adepper@fc-lawyers.com