IN THE CIRCUIT COURT OF THE EIGHTH JUDICIAL CIRCUIT
IN AND FOR ALACHUA COUNTY, FLORIDA

IN RE: GAINESVILLE POLICE DEPARTMENT
INVESTIGATION 02-19-005221,

CASE NO: 01-2020-CA-0350

CIRCUIT CIVIL DIVISION: K

_____/

THIRD PARTY MOTION TO QUASH SEARCH WARRANT AND MOTION FOR PROTECTIVE ORDER

Third Party JOHN DOE, by and through undersigned counsel, files this motion to quash the search warrant issued to Google, Inc. on April 2, 2019 by Gainesville Police Department regarding investigation 02-19-005221. This search warrant is null and void as it lacks the particularity required by the Florida constitution. In support Third Party JOHN DOE offers:

FACTUAL BACKGROUND:

On January 14, 2020, John Doe received a notice from Google that Google had received legal process from the Gainesville Police Department regarding case number 0219005221; it is attached as Exhibit A. A public records request from the Gainesville Police Department of case number 0219005221 returned the Investigative report attached as Exhibit B. Upon request by John Doe and undersigned counsel, Google provided a redacted copy of the search warrant received. (Exhibit C). Google represented to counsel that they did not have a copy of the affidavit and were providing all that they had. Exhibit C only contains pages "7–10 of 10," likely indicating there are six pages prior, all of which Google represents to not have received.

This type of warrant is often called a "geofence warrant." Google represented to undersigned counsel that they were waiting for a ruling on this motion before making a

determination to release information to Gainesville Police Department.

The Geofence warrant, as executed by Gainesville Police Department upon Google, requires disclosure of Google accounts that trigger a matching geographical location with the coordinates specified in the warrant. The geofence warrant targets three houses, the houses' back yards, and the public street in front of the houses in the Gainesville neighborhood of Springtree.

The public street located inside the geofenced area specified in the warrant is NW 32nd Street, near block number 4300. The Gainesville Police Department investigative report indicates that the house located at 4324 was burglarized at some point between 2:45 and 5:30 PM on Friday, March 29, 2019. (Exhibit B). Presumably from this window of time, Gainesville Police Department requested the geofence warrant to cover 2:15–5:30 PM.

TECHNOLOGICAL BACKGROUND:

In a similar but un unrelated case in the Eastern District of Virginia, 3:19-cr-00130-MHL, Google filed an amicus curiae brief in an effort to explain the technology behind responding to a geofence warrant. This brief is attached as Exhibit D and will be referred to throughout this motion. In case 3:19-cr-00130-MHL, Defendant Okello Chatrie filed a response to Google's Amicus Curiae Brief. This is attached as Exhibit E and incorporated to the extent it explains the voluntariness, or lack thereof, of "opting in" to Google's collection and storage of private data. In case 3:19-cr-00130-MHL, the government filed a response to Google's Amicus Curiae Brief, which is attached as Exhibit F to provide this Court with all arguments presented.

In May of 2017 Google announced that they have "2 billion monthly active Android devices." (Exhibit G). It is unclear how many Google accounts have been created or are in use, but a quick Google search would seem to indicate it was reported in the 1.5 billion users range in

2018.[1] For each Google user with their location history enabled, Google tracks and stores a *journal*—timeline—of all movements and locations with timestamps to the minute. (Exhibit D, p 11). Data entries to this timeline journal are private and only accessible with the Google username and password that each user maintains. This same password grants access to all Google products such as YouTube viewing history, Gmail inbox, etc. There is access, of course, to all Google data through Google's employees, much like hotel maintenance employees still have access to rented rooms for the purpose of further enhancing and maintaining a guest's stay.

LEGAL BACKGROUND:

The Fourth Amendment to the United States Constitution and Section 12 of Article I of the Florida Constitution prohibit unreasonable searches and seizures. *See* U.S. CONST. art. IV; Art. I, § 12, Fla. Const. This Florida Constitutional guarantee explicitly states that it mirrors the United States Constitutional right and is governed by all Supreme Court of the United States decisions. *Id.* In *Katz*, the United States Supreme Court ruled that a search implicated the fourth amendment if persons had a reasonable expectation of privacy in the place searched. *Katz v. United States*, 389 U.S. 347 (1967).

The United States Supreme Court has further held that persons have a reasonable expectation of privacy in their historic location data as created in "a time-stamped record known as cell-site location information (CSLI)." *Carpenter v. United States*, 138 S. Ct. 2206, 2211, 2219 (2018). The Court in *Carpenter* further held that the third-party doctrine does not defeat the reasonable expectation of privacy that persons have in CSLI. *Id.* at 2210. Since the United States

[1] https://www.statista.com/statistics/432390/active-gmail-users/

Supreme Court has found a reasonable expectation of privacy in CSLI, law enforcement officers must obtain a search warrant supported by probable cause in order to obtain a person's CSLI. *Id.* at 2211.

For a warrant to withstand Constitutional scrutiny, it must be specific and "particularly describe the property to be seized." *Carlton v. State*, 449 So. 2d 250, 251 (Fla. 1984) (citing Art. I, § 12, Fla. Const.); *see also Russ v. State*, 185 So. 3d 622, 626 (Fla. 5th DCA 2016) (reasoning that "The use of broad categories and generalities can render a search warrant overly broad."). A valid warrant's particularity protects the constitution through multiple ways. One, it "limits the searching officer's discretion in the execution of [the] search warrant, thus safeguarding the privacy and security of individuals against arbitrary invasions by governmental officials." *Carlton*, 449 So. 2d. at 252; *see also Russ*, 185 So. 3d at 625-26 (Fla. 5th DCA 2016) (holding that "Where a search warrant fails to adequately specify material to be seized, and leaves the scope of the seizure to the discretion of the executing officer, it is constitutionally overbroad."), *Winters v. State*, 615 So. 2d 262, 263 (Fla. 4th DCA 1993) (holding that a directive "to search diligently for stolen property" was a "failure of this warrant to limit the scope of the officer's search render[ing] it constitutionally infirm.").

Particularity in a valid warrant also dictates the warrant not be a "fishing expedition." *See Pollard v. State*, 44 Fla. L. Weekly D3050, *5 (Fla. 1st DCA June 20, 2019), reh'g denied (Dec. 23, 2019) (ruling "that unless the state can describe with reasonable particularity the information it seeks to access on a specific cellphone, an attempt to seek all communications, data and images amounts to a mere fishing expedition.") (internal quotation marks and edits omitted). A particular warrant, by its very nature, cannot be a general warrant as they are "of course, prohibited by the

Fourth Amendment." *Andresen v. Maryland*, 427 U.S. 463, 480 (1976); see also *Carlton*, 449 So. 2d at 252 (holding that "the particularity requirement stands as a bar to exploratory searches by officers armed with a general warrant.").

Additionally, a "generalized request[] for multiple categories" may fail the particularity test and be "a net cast far too broadly." *See Pollard*, 44 Fla. L. Weekly D3050 at *5. Everything satisfying these requirements for particularity "must be judged by looking only at the information contained within the four corners of the warrant." *Carlton*, 449 So. 2d at 251. *See also Green v. State*, 688 So. 2d 301, 306 (Fla. 1996) (holding "that in this case the warrant is facially overbroad.") There are special circumstances where broad sweeping warrants are allowed, but this is limited to situations where a *pervasive fraud* is taking place at the location to be searched. *See generally State v. Nuckolls*, 617 So. 2d 724, 726 (Fla. 5th DCA 1993) (citing the trial court's "order that the warrant 'would meet the particularity requirement in most federal courts, especially in light of the recent trend towards flexibility when criminal activity pervades an entire business.'"). Another exception allowing for "flexibility" in warrants is when there is an "investigation of complex white collar crime;" but this is only allowed in the Fourth District Court of Appeal. *Id.* at 726–27. This flexibility is granted due to the "difficulty of piecing together the 'paper puzzle.'" *Id.* at 727 (citing *State v. Showcase Products, Inc.*, 501 So.2d 11 (Fla. 4th DCA 1986)). The standard of particularity required in the Fifth District Court of Appeal, even in complex white collar cases, is "somewhat higher . . . ." *Id.*

Beyond the protection from unreasonable searches and seizures guaranteed by article one, section 12 of the Florida Constitution, Florida also provides a Constitutional right to privacy. Art. I, § 23, Fla. Const. Florida's constitutional right to privacy "is much broader in scope than that of

the Federal Constitution." *Winfield v. Div. of Pari-Mutuel Wagering, Dept. of Bus. Regulation*, 477 So. 2d 544, 548 (Fla. 1985). In fact, it is not just a right to privacy granted, but an unqualified "right to be let alone and *free from governmental intrusion* into the person's private life except as otherwise provided herein." Art. I, § 23, Fla. Const. (emphasis added); *See also Winfield*, 477 So. 2d at 548 (noting that "The drafters of the amendment rejected the use of the words 'unreasonable' or 'unwarranted' before the phrase 'governmental intrusion' in order to make the privacy right as strong as possible."). Admittedly the First District Court of Appeal has held that

> In circumstances like the one at issue, involving search and seizure issues, the Florida Constitution's right of privacy provision, Article I, section 23, does not modify the applicability of Article I, section 12, so as to provide more protection than that provided under the Fourth Amendment, 'particularly since the people adopted section 23 prior to the present section 12.'

L.S. v. State, 805 So. 2d 1004, 1008 (Fla. 1st DCA 2001).

ARGUMENT:

Persons have a reasonable expectation of privacy in their private "journals" as kept by Google. This geofence search warrant, as issued, is unconstitutional and void for lack of particularity by 1) being facially overbroad and amounting to a general warrant; 2) giving law enforcement discretion in how they execute it. Lastly, this warrant is also void as it amounts to an initial invasion of privacy on innumerable persons worldwide, but, when fully executed, will egregiously intrude into the privacy of many neighbors and Florida citizens that reside in the Springtree neighborhood of Gainesville Florida in contravention of the Florida Constitution as enumerated by Article 1, section 23.

People have a reasonable expectation of privacy in their private "journals" tracking their location.

This is a matter of first impression before the Court. The only other pending litigation counsel is aware of regarding this issue is attached as exhibits. In the landmark *Carpenter* decision, the United States Supreme Court held that individuals had a reasonable expectation of privacy in their cell-site location information (CSLI). *Carpenter*, 138 S. Ct. at 2211. The Court expressed concern that tracking individuals based on their phone's location "provides an all-encompassing record of the holder's whereabouts." *Id.* at 2217. Location history of a Google account, however, provides a "significantly more granular" set of data than that ever considered in *Carpenter*. (Exhibit D, p. 23).

Google's amicus brief admits that "The privacy interests implicated by Google [location history] are thus even greater than in *Carpenter*." (Exhibit D, p. 23). A Google user's location history, despite being stored on Google's servers, is not a business record of Google's thereby implicating the third-party doctrine. A "journal" of location entries housed under lock-and-key—in this case called a username and password—is not a "business record" like that owned by the bank in *United States v. Miller*. *See United States v. Miller*, 425 U.S. 435 (1976).

Moreover, in *Carpenter* the Court stressed the idea that the data collected was "not truly 'shared' as one normally understands the term." *Carpenter*, 138 S.Ct. at 2220. The very next sentence states "In the first place, cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society.'" *Id.* (citing *Riley v. California*, 573 U.S. 373, 384 (2014)). *Carpenter* then held that "Given the unique nature of cell phone location information" the Fourth Amendment protection did not yield to the third-party doctrine. *Id.* "The fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection." *Id.* To

the extent that the third-party doctrine is implicated in Google location history searches, there are additional unanswered questions about whether users are informed or even able to opt out of Google's collection of location history data. *See* (Exhibit E, p. 5–10); *See also Associated Press News*, https://apnews.com/ef95c6a91eeb4d8e9dda9cad887bf211 (last visited Jan. 31, 2020). Google's lack of transparency cannot vitiate citizen's constitutional rights. Lack of transparency by Google, if anything, bolsters the reasonableness of the privacy expectation.

This geofence warrant is a facially overbroad, general warrant.

Google's amicus brief (Exhibit E) explains that in order to comply with this search warrant, "Google must search across all [location history] journal entries to identify users with potentially responsive [location history] data, and then run a computation against every set of coordinates to determine which [location history] records match the time and space parameters in the warrant." (Exhibit E, p. 12–13). At first blush this may not sound like much, but a closer inspection of what Google does to comply with a geofence warrant shows that Google takes every single Google account with location history enabled and cross references that list against the geographical coordinates provided in the warrant. *See id.* In its amicus brief, Google asserted they run every single one of these users' "journals" with location history enabled through their algorithms to determine a match with the geofenced area. *See* (Exhibit E, p. 12–13). Hypothetically, if 1 out of every 3 Google accounts had location history enabled, Google would search through private "journals" of 500 million users; all to satisfy a single geofence search warrant.

Geofence warrants are a novel legal issue, yet common sense dictates that the broad sweeping search commanded smacks of facial overbreadth. *See generally Green*, 688 So. 2d at 306. Florida law has specified that "requests for multiple categories of communication" "amount[]

to a mere fishing expedition" in violation of the particularity requirement; how much more so then is a search warrant that requires searching through potentially hundreds of millions of users "journals?" *See generally Pollard*, 44 Fla. L. Weekly D3050 at *5 (internal quotation marks omitted). The utility Gainesville Police Department seeks Google location history data is understandable. It allows them to cast a wide net covering the entire window when the burglary may have occurred to round up potential suspects. This, however, is done at the expense of the Constitutional guarantees of the Florida Constitution. *See generally id.* (prohibiting fishing expeditions). This geofence warrant effectively blindly casts a net backwards in time hoping to ensnare a burglar. This concept is akin to the plotline in many a science fiction film featuring a dystopian, fascist government.

The search warrant makes no finding of probable cause that the burglar was carrying an android phone during the burglary—much less that one was turned on. The search warrant makes no finding of probable cause that a single Google server was accessed by the burglar. There is similarly no finding of probable cause that Google, Inc. is being used to perpetuate a "pervasive fraud" allowing for a general search warrant; nor is a burglary a complex "paper puzzle" allowing flexibility with the particularity requirement. *See generally Nuckolls*, 617 So. 2d at 727. This geofence warrant must be judged only by its four corners, *Green*, 688 So. 2d at 306, and it is constitutionally infirm.

This geofence warrant impermissibly leaves discretion to law enforcement officers

Quite possibly the most damning evidence of an invalid warrant present on this geofence warrant's face is the unconstitutional delegation of authority to law enforcement officers in their execution. The Florida Supreme Court has explicitly ruled that the particularity requirement serves

to limit "the searching officer's discretion in the execution of a search warrant, thus safeguarding the privacy and security of individuals against arbitrary invasions by governmental officials." *Carlton*, 449 So. 2d at 252. Regarding seizures, the Florida Supreme Court quoted Justice Butler saying "nothing is left to the discretion of the officer executing the warrant." *Id.* (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)).

Yet, in this geofence warrant, law enforcement officers are given tremendous discretion. The search warrant dictates Google is to do the preliminary search and provide law enforcement officers with "anonymized information." (Exhibit C, p. 9 of 10). The Court's next directive is that "Law enforcement officers will attempt to narrow down the list by reviewing the time stamped location coordinates for each account and comparing that against the known time and location information that is specific to this crime." (Exhibit C, p. 9 of 10). This in itself is ambiguous and gives law enforcement some discretion in the manner they execute the warrant. Next, however, is the unfettered discretion given to law enforcement. The warrant says that after reviewing the "anonymized information . . . and upon request by Law Enforcement, Google Inc. shall provided identifying account information . . . ." (Exhibit C, p. 9 of 10). Under the court ordered geofence warrant, law enforcement has the absolute discretion to ask for identifying information on all or none of the Google accounts initially returned and presented as "anonymized information."

This bequeathing of authority is expressly impermissible under the Constitution as established by *Carlton*. *See also Winters v. State*, 615 So. 2d 262, 263 (Fla. 4th DCA 1993) (holding "The failure of this warrant to limit the scope of the officer's search renders it constitutionally infirm."), *Russ v. State*, 185 So. 3d 622, 626 (Fla. 5th DCA 2016) (holding "Where a search warrant fails to adequately specify material to be seized, and leaves the scope of the

seizure to the discretion of the executing officer, it is constitutionally overbroad."). Just like the warrants in *Winters* and *Russ*, this geofence warrant leaves the scope of data linked to Google accounts to be seized up to the discretion of the Gainesville Police Department—which cannot stand under the constitution.

This geofence warrant unconstitutionally intrudes into persons' private lives in a manner never previously addressed under Florida law

Florida courts have held that "Article I, section 23, does not modify the applicability of Article I, section 12, so as to provide more protection than that provided under the Fourth Amendment." *L.S.*, 805 So. 2d at 1008 (citing to *State v. Hume*, 512 So. 2d 185 (Fla. 1987)). *Hume* and all of its progeny—approximately 20 decisions sprinkled through the districts—deal with a known suspect and a warrant executed to search for and seize evidence related to a specific crime.

This geofence warrant, however, strikes a resoundingly different chord. Presumably used to find an unknown suspect when leads are few and far between, it directly permits government intrusion into an inordinate number of different persons' lives. This geofence warrant, specifies a location covering a public street, in a 5 hour window—most notably including a time many persons drive home from work on a Friday: 4–5:30 PM. As the warrant dictates, all these innocent individuals will have their private data intruded into by the Gainesville Police Department. This reality distinguishes it from all situations where Florida courts have addressed the seeming intersection between the right to be free from unreasonable search and seizures and the right to be free from governmental intrusion.

The broad, sweeping right to privacy of countless neighbors and innocent passerby, including John Doe, demands that governmental officials—in this case the Gainesville Police

Department—are proscribed from intruding into their private lives by accessing their personal timelines all in the hopes of catching a single fish. A fishing expedition cannot satisfy the "compelling state interest" required to overcome innocent persons' fundamental right of privacy. *See generally L.S.*, 805 So. 2d at 1008.

THEREFORE, third party JOHN DOE requests this Court enter an order quashing the search warrant signed on April 2, 2019 regarding the Gainesville Police Department investigation 02-19-005221 and requests this Court enter a protective order for all of John Doe's location history information that Google holds for him as a bailee. JOHN DOE respectfully requests this Court set a hearing in this matter.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing document has been electronically delivered to the following:

Gainesville Police Department
545 NW 8th Avenue
Gainesville, FL 32601
court@cityofgainesville.org

Respectfully submitted this 31st day of January, 2020.

TURNER O'CONNOR KOZLOWSKI, P.L.

/s/ Caleb S. Kenyon
CALEB S. KENYON
Florida Bar No. 1002297
csk@toklegal.com
102 N.W. Second Avenue
Gainesville, FL 32601
(352) 372-4263
(352) 375-5365 (facsimile)
Secondary E-mail:
eservice@toklegal.com