UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 23 | Issue 3 Article 7

4-1-2022

Reverse Location Search Warrants: Law Enforcements' Transition to 'Big Brother'

Cassandra Zietlow

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 23, ISSUE 3: APRIL 2022

REVERSE LOCATION SEARCH WARRANTS: LAW ENFORCEMENT'S TRANSITION TO 'BIG BROTHER'

Cassandra Zietlow*

Law enforcement across the United States is knocking on Google's door with its use of reverse location search warrants ("RLSWs"). These warrants allow government officers to access locational data of every cellular device within a certain proximity and time range. RLSWs are an innovative technological tool that allow law enforcement to essentially work backward during investigations in creating a suspect list after a crime has been committed. RLSWs give the government oversight and knowledge regarding the movements of its citizens—oversight that comes remarkably close to that of the popular fictional novel, "Big Brother." This new investigative tool is increasingly being used by law enforcement, and few states and courts have made progress in addressing the constitutionality of these warrants, particularly in relation to the Fourth Amendment.

The use of these warrants has raised important questions regarding the privacy that individuals are expected to have in the current technological world. This Article explores the history of RLSWs and their relation to the Fourth Amendment. Further, this Article advocates for limitations to be placed upon the use of these warrants through laws and judicial adherence to the "probable cause" and "particularity" requirements of the Fourth Amendment. Finally, this Article recommends limiting the use of RLSWs to extreme circumstances and argues against the collection of innocent individuals' information.

* J.D. Candidate, University of North Carolina School of Law, 2023. The Author would like to thank the NC JOLT editors and staff, particularly Chris Jones, Meredith Doswell, and Anna Comer for their assistance during the editorial and writing process. The Author would also like to thank her family and friends for their support and encouragement.

TABLE OF CONTENTS

I. INTRODUCTION

In the summer of 2020, police responded to a "family trouble" call at a home outside downtown Kenosha, Wisconsin, which led to the tragic shooting and subsequent paralysis of Jacob Blake at the hands of an arresting officer.[1] The event was caught on video and

[1] Russell Brandom, *How Police Laid Down a Geofence Dragnet for Kenosha Protesters*, THE VERGE (Aug. 30, 2021, 9:20 AM), https://www.theverge.com/22644965/kenosha-protests-geofence-warrants-atf-android-data-police-jacob-blake [https://perma.cc/B497-RFLZ]; *see also* Scott Glover, *Lawyer Says Cop*

went viral within minutes, reigniting national protests for racial justice and police reform[2]—the protestors destroyed approximately forty buildings and had numerous physical altercations with law enforcement.[3] Additionally, a counter-protestor killed two individuals.[4]

In the midst of these protests, law enforcement attempted to identify the individuals responsible for burning or destroying the buildings.[5] This attempted identification proved nearly impossible because of the sheer volume of individuals at the protests and the lack of eyewitness testimony that would have given police an investigative lead.[6] It would seem as though law enforcement had reached a dead end; however, that was not the case due to the emergence of a new type of warrant that allows police to identify the location pattern of individuals based upon their geolocation data.[7] This tool is known as a Reverse Location Search Warrant ("RLSW") or a geofence warrant. RLSWs are an investigative tool increasingly being used by law enforcement to assist in criminal investigations with limited evidence or no suspects.[8] RLSWs increase law enforcements' ability to gather private information on

---

Shot Jacob Blake After Hearing a Mother's Desperate Plea: 'He's Got My Kid. He's Got My Keys', CNN (Sept. 25, 2020), https://www.cnn.com/2020/09/25/us/rusten-sheskey-account-jacob-blake-shooting-invs/index.html [https://perma.cc/5EFZ-T2L6]; Christina Morales, *What We Know About the Shooting of Jacob Blake*, N.Y. TIMES (Oct. 8, 2021), https://www.nytimes.com/article/jacob-blake-shooting-kenosha.html [https://perma.cc/Q5RL-A4TK]; *see generally* MICHAEL D. GRAVELEY, *Report on the Officer Involved Shooting of Jacob Blake*, COUNTY OF KENOSHA, DISTRICT ATTORNEY 2–3 (2020), https://www.kenoshacounty.org/DocumentCenter/View/11827/Report-on-the-Officer-Involved-Shooting-of-Jacob-Blake [https://perma.cc/XG5M-GKXF] (describing that, in the police department's statement, the officers on the scene assert, prior to opening fire, that Blake was combative, actively resisting arrest, and was about to use a weapon on one of the responding officers. In total, Jacob Blake was shot seven times).

[2] Morales, *supra* note 1.

[3] Brandom, *supra* note 1.

[4] *See id.* (referencing two of the intentional fires started during the protests and discussing the counter-protest, identifying "counter-protestors" as individuals that are engaged in a protest against the initial protest).

[5] *See id.*

[6] *See id.*

[7] *Id.*

[8] *Id.*

large groups of people without the need to provide the adequate basis or reasons for such a large intrusion. Specifically, RLSWs can generate the location points and movements of all of those who are within an identified geographic area without law enforcement having to expend any of their own resources to obtain the information.[9] A person's location and movements offer an intimate look into the activities of that person—activities that, in many instances, the person would not want publicly shared.[10] More concerning, RLSWs can incriminate innocent individuals who find themselves in the wrong place at the wrong time.

With RLSWs, the police were able to identify the Kenosha protesters who were seemingly exercising their freedom of expression afforded to each U.S. citizen.[11] The Kenosha protests were not even the first protests where RLSWs were used, as RLSWs were filed during the George Floyd protests in Minneapolis earlier in 2020.[12] Notably, the use of RLSWs has not been confined to protests; RLSWs have also been utilized in other criminal investigations, such as homicides and burglaries.[13]

RLSWs are problematic as they are in stark contrast to the freedom from extensive government oversight that is afforded to Americans.[14] Entrenched in the U.S. Constitution is the notion that people have a right to be free of government intrusion into their private affairs unless there is a showing of probable cause that the

---

[9] Aaron Mak, *Close Enough*, SLATE (Feb. 19, 2019, 5:55 AM), https://slate.com/technology/2019/02/reverse-location-search-warrants-google-police.html [https://perma.cc/UFN5-7A4N].

[10] *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

[11] U.S. CONST. amend. I.

[12] Brandom, *supra* note 1.

[13] *See* Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/W3ES-U2WF]; Tyler Dukes, *To Find Suspects, Police Quietly Turn to Google*, WRAL (Mar. 15, 2018, 5:05 AM), https://www.wral.com/Raleigh-police-search-google-location-history/17377435/ [https://perma.cc/585H-JA2P]; Brandom, *supra* note 1; *In re* Search of Information Stored at Premises Controlled by Google, No. 20 M 297 (N.D. Ill. July 8, 2020) (order denying request for RLSWs for stolen pharmaceuticals).

[14] *See* U.S. CONST. amend. I, VI.

individual engaged in criminal activity.[15] This principle is embedded into the Constitution through the Fourth Amendment, which aims to protect citizens from unreasonable searches and seizures.[16] The Fourth Amendment was enacted to serve as a restraint on the government's immense power.[17] Reminiscent of this idea, George Orwell authored *1984*—warning against the dangers of the feared "Big Brother,"[18] which symbolizes a totalitarian government that constantly monitors its citizens' every move.[19] The concept of perpetual surveillance has been, and remains, a fear for most Americans.[20] Thus, without proper limitations on RLSWs, the themes echoed in Orwell's novel could become a reality.

This Article argues that, as used today, RLSWs are unconstitutional; they satisfy neither the probable cause nor the particularity requirements of the Fourth Amendment. Further, RLSWs do not qualify under the "third-party doctrine," which allows law enforcement to receive geolocation data of all individuals within an area without a warrant. This Article proceeds in five parts. Part II explains the requirements for traditional search warrants. Part III provides an in-depth description of what an RLSW is and the process that is used in obtaining one. Part IV examines the

---

[15] *See* Eric Foner, *The Contested History of American Freedom*, 137 PA. MAG. HIS. & BIOGRAPHY 13, 24 (2013).

[16] U.S. CONST. amend. I, VI.

[17] *See* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018); Henry Farrell, *America's Founders Hated General Warrants. So Why Has the Government Resurrected Them?*, WASH. POST (June 14, 2016), https://www.washingtonpost.com/news/monkey-cage/wp/2016/06/14/americas-founders-hated-general-warrants-so-why-has-the-government-resurrected-them/ [https://perma.cc/ZPJ5-G3L4].

[18] *See Bill of Rights*, HISTORY (Sept. 15, 2020), https://www.history.com/topics/united-states-constitution/bill-of-rights [https://perma.cc/MUR5-GQQZ]; GEORGE ORWELL, 1984 1 (1949) (referring to "Big Brother" as the government or the ruling power in the dystopian novel).

[19] ORWELL, *supra* note 18.

[20] *See* Megan Brenan & Helen Stubbs, *Americans Are Critical of Technology Companies Despite Changes to Misinformation Policies,* KNIGHT FOUND. (Oct. 21, 2020), https://knightfoundation.org/articles/americans-are-critical-of-technology-companies-despite-changes-to-misinformation-policies/?utm_source=link_newsv9&utm_campaign=item_329666&utm_medium=copy [https://perma.cc/MPX3-ZY9X] (indicating that approximately 94% of people are concerned about the privacy of personal data online from a survey).

relationship between the Fourth Amendment's safeguards and RLSWs' impact on them. Part V looks towards the recent development of RLSWs in both the legislative and judicial realms. Lastly, Part VI provides recommendations for how Congress, courts, and judges should address RLSWs in the future.

II. TRADITIONAL SEARCH WARRANTS EXPLAINED

In order for law enforcement to procure a search warrant, three things are required: (1) "warrants must be issued by neutral, disinterested magistrates," (2) "those seeking the warrant must demonstrate to the magistrate their probable cause to believe that 'the evidence sought will aid in a particular apprehension or conviction' for a particular offense," and (3) "warrants must particularly describe the 'things to be seized.'"[21] Probable cause exists when law enforcement believes "there is a fair probability that contraband or evidence of a crime will be found in a particular place."[22] This standard requires law enforcement to have *individualized suspicion*, which is the showing of more than a mere hunch, showing a probability that criminal activity has occurred.[23] "Particularity" refers to the specific identification of the area to be searched and the items to be seized during the search.[24]

Traditionally, U.S. government officials will not apply for a search warrant until late in an investigation when more information has been revealed[25]—i.e., after the police have gathered information regarding potential suspects and evidence of the crime or criminal intent.[26] The probable cause and particularity requirements also enforce this restraint in issuing search warrants because of the burden of proving probable cause to a magistrate and providing evidence that the places to be searched will have the evidence needed to convict. Thus, traditional search warrants tend to be

---

[21] Dalia v. United States, 441 U.S. 238, 255 (1979) (citations omitted).
[22] Illinois v. Gates, 462 U.S. 213, 238 (1983).
[23] *See id.* at 235.
[24] *See Dalia*, 441 U.S. at 255.
[25] *See generally* N.C. GEN. STAT. § 15A-244 (depicting the required contents in an application for a search warrant that includes facts and circumstances surrounding it, which would not be available without adequate time to investigate).
[26] *See id.*

extremely detailed and contain all the information obtained by law enforcement with the goal of persuading judges to look at all the facts and conclude the warrant is necessary for the investigation.[27]

III. REVERSE LOCATION SEARCH WARRANTS

The purpose of traditional search warrant requirements is to act as a procedural safeguard against the unreasonable intrusion upon an individual's privacy;[28] RLSWs contradict this safeguard. Specifically, RLSWs allow law enforcement to obtain the geolocations of all individuals within a precise location and at a particular time when law enforcement had not previously identified those individuals during the normal information-gathering of an investigation.[29] Although the initial procedure required to obtain an RLSW seems similar to procuring a traditional warrant, it is extremely different in substance.[30]

Compared to applications for traditional warrants,[31] applications for RLSWs may be significantly vaguer.[32] RLSWs inherently contain less information than traditional search warrants because the government applies for them when officers have no other investigative options.[33] Unlike traditional warrants, RLSWs work backward by first obtaining the geolocation of all individuals in a certain location during a specific time range.[34] From this information, police then have a list of potential suspects and attempt

---

[27] Spinelli v. United States, 393 U.S. 410, 415 (1969).

[28] William Andrew Kerr & Frances Lee Watson, CRIMINAL PROCEDURE § 2.3f (Vols. 16–16B, Ind. Prac. Series 2021).

[29] Mak, *supra* note 9.

[30] *See* Brandom, *supra* note 1; *see generally Affidavit for Search Warrant*, COMMONWEALTH OF VIRGINIA (2019), https://www.nacdl.org/getattachment/fc0182fd-fe6c-452f-b31f-d7a63acc135a/edva-geofence-warrant.pdf [https://perma.cc/X8VW-CKEL] (depicting a geofence warrant application).

[31] *Supra* Part II.

[32] *See* Brandom, *supra* note 1; *see generally Affidavit for Search Warrant*, *supra* note 30 (portraying the information within a geofence warrant application).

[33] Brandom, *supra* note 1.

[34] Sean Broderick, *Google Data and Geofence Warrant Process*, NAT'L LITIG. SUPPORT BLOG (Jan. 8, 2021), https://nlsblog.org/2021/01/08/google-data-and-geofence-warrant-process/#_edn7 [https://perma.cc/RZ6D-TURD].

to narrow their search to find the perpetrator of the particular crime they are investigating.[35]

While applying for an RLSW entails the same requirements as a traditional warrant (probable cause, particularity, and issuance by a judge),[36] the difference lies in the substance of each of these requirements.[37] For instance, the government uses the commission of a crime to satisfy the probable cause requirement; and, to satisfy the particularity requirement, the government describes the place to be searched as a set location and provides a time range.[38] Unlike traditional warrants, RLSWs are issued to Google, which holds this location data.[39] An RLSW itself contains little to no information—the law enforcement officers themselves do not even know for whom they are looking.[40] In these situations, the government intends to cast a wide net and gather exponential amounts of data about anyone who may have passed within the geolocation search area.[41] In fact, police readily capture information of innocent individuals who are found to be in a wrong-place-at-the-wrong-time scenario.[42]

A. The Process for Acquiring an RLSW

Obtaining an RLSW is a multi-warrant process.[43] In the first warrant step, the government requests location data from Google for a specific geographical area and time range.[44] Google provides the government with location data on all devices that were within the

---

[35] Mak, *supra* note 9.

[36] Daniel K. Gelb, *Is the Reverse Location Search Warrant Heading in the Wrong Direction?*, 34 CRIM. JUST., Summer 2019, at 68.

[37] *Compare supra* Part II with, *Affidavit for Search Warrant, supra* note 30, and Broderick, *supra* note 34 (highlighting the substantive differences between applications of a traditional search warrant and an RLSW).

[38] *See* Broderick, *supra* note 34; *see generally Affidavit for Search Warrant, supra* note 30 (depicting the information in a geofence warrant application).

[39] *See* Broderick, *supra* note 34; *see generally Affidavit for Search Warrant, supra* note 30; *In re* Search of Information Stored at Premises Controlled by Google, No. 20 M 297 (N.D. Ill. July 8, 2020) (order denying request for warrant).

[40] *See* Broderick, *supra* note 34.

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.*

set location during the time range.[45] The location data is "anonymized" so that law enforcement is unable to identify the user.[46] This location data includes the date and time of any device that connected to Bluetooth, Wi-Fi, or cellular service within the area, as well as the approximate latitudinal and longitudinal coordinates of the device.[47]

After reviewing the location data from the first warrant, law enforcement can ask for additional location information for devices to "eliminate false positives" or determine whether that device is a potential suspect.[48] This warrant can include asking Google to provide additional location coordinates beyond those in the original warrant.[49] This request for more information does not happen for every RLSW but is a possibility.[50] Lastly, the government applies for a second, more traditional warrant that requests details involving the identity of the anonymous users that they deemed "relevant to the investigation."[51] In essence, these RLSWs "suggest[] possible suspects and witnesses in the absence of other clues."[52]

Many law enforcement officers claim to utilize RLSWs only in situations where the police do not have any known leads or suspects of a crime.[53] Despite this intention, police are still casting a wide net—so wide that police are often receiving information on innocent individuals.[54]

---

[45] *Id.*

[46] *Id.*

[47] *Id.*; Jennifer Lynch, *Google's Sensorvault Can Tell Police Where You've Been*, ELEC. FRONTIER FOUND. (Apr. 18, 2019), https://www.eff.org/deeplinks/2019/04/googles-sensorvault-can-tell-police-where-youve-been [https://perma.cc/WL2N-CNJ7].

[48] Broderick, *supra* note 34.

[49] *Id.*

[50] *Id.*

[51] *Id.*; *see In re* Information Stored at Premises Controlled by Google, No. 20 M 297 *6 (N.D. Ill. July 8, 2020).

[52] *See* Valentino-DeVries, *supra* note 13.

[53] *See* Brandom, *supra* note 1.

[54] *Id.* The number of individuals caught within these nets varies depending on the geographic location of the warrant and the time range. If the RLSW was issued for a city, encompassing a popular street and commercial businesses, then it would most likely include a significant amount of people the larger the scope.

B. The Increasingly Contentious Five-Year History of RLSWs

The protests following the shooting of Jacob Blake[55] were not the first instances in which law enforcement utilized this relatively new investigative tool.[56] The first RLSW granted by a court was in 2016[57] and was not reported on until 2018.[58] Since then, there has been an exponential increase in police departments around the country requesting and using RLSWs,[59] including for investigations related to the George Floyd protests in Minneapolis in 2020.[60]

Law enforcement has employed RLSWs in other criminal investigations as well.[61] In one striking example, police utilized an RLSW in 2018 to identify Jorge Molina in a criminal investigation in Phoenix, Arizona.[62] To identify Molina, Arizona police used an RLSW that tracked his location and placed him in the area of the crime at the approximate time the crime took place.[63] From this information, the police focused on Molina as their prime suspect for a case that otherwise had no investigatory leads.[64] Molina was subsequently arrested and detained for a murder he did not commit.[65]

With the heightened publicity of RLSWs, law enforcement agencies have likewise been using them at increasing rates.[66] Google publishes a transparency report every six months displaying the number of subpoenas, search warrants, and other orders the

---

[55] *See supra* Part I (referencing the Kenosha protests).

[56] Brandom, *supra* note 1; Valentino-DeVries, *supra* note 13.

[57] Dukes, *supra* note 13; Valentino-DeVries, *supra* note 13.

[58] Dukes, *supra* note 13; Valentino-DeVries, *supra* note 13.

[59] Valentino-DeVries, *supra* note 13.

[60] Brandom, *supra* note 1.

[61] Valentino-DeVries, *supra* note 13; *In re* Information Stored at Premises Controlled by Google, No. 20 M 297 *1 (N.D. Ill. July 8, 2020).

[62] Valentino-DeVries, *supra* note 13.

[63] *Id.*

[64] *Id.*

[65] *Id.* Molina spent less than a week in jail due to the investigation illuminating the actual perpetrator but was harmed by the false allegations. *Id.* As a consequence of being falsely arrested, Molina's car was repossessed after it was impounded for investigation, and he was unable to find employment. *Id.*

[66] *Id.*

company receives from the government.[67] In all categories, the number of requests since 2016 has progressively gone up.[68] Specifically related to RLSWs, approximately 982 geofence warrants were served on Google in 2018; 8,396 were served in 2019; and, 11,554 were served in 2020.[69] By late 2019, Google stated it was receiving up to 180 RLSW requests per week—a 1500% increase between 2017 and 2018, and a 500% increase from 2018 to 2019.[70] No data suggests the number of requests of RLSWs will go down in the near future.[71]

Even with this significant increase in requests, Google maintains that the company has "a rigorous process designed to protect the privacy of [its] users while supporting the important work of law enforcement."[72] A part of this process is making sure the company complies with all applicable laws and that users are notified when

---

[67] *See Global Requests for User Information*, GOOGLE (last visited Oct. 13, 2021), https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts,compliance;authority:US;time:&lu=user_requests_report_period&legal_process_breakdown=expanded:5,4 [https://perma.cc/Z74Q-GBNN].

[68] *Id.*

[69] Zack Whittacker, *Google Says Geofence Warrants Make Up One-Quarter of All US Demands*, TECHCRUNCH (Aug. 19, 2021, 5:54 PM), https://techcrunch.com/2021/08/19/google-geofence-warrants/ [https://perma.cc/F7VQ-8KRT]; *see also Supplemental Information on Geofence Warrants in the United States*, GOOGLE (2021), https://s3.documentcloud.org/documents/21046081/google-geofence-warrants.pdf [https://perma.cc/7WPY-P9QW] [hereinafter *Supplemental Information*].

[70] Wendy Davis, *Law Enforcement Is Using Location Tracking on Mobile Devices to Identify Suspects, But Is It Unconstitutional*?, A.B.A. J. (Dec. 1, 2020, 1:50 AM), https://www.abajournal.com/magazine/article/law-enforcement-is-using-location-tracking-on-mobile-devices-to-identify-suspects-geofence [https://perma.cc/4BM8-LNJG].

[71] *Id.*; Whittacker, *supra* note 69; *Supplemental Information*, *supra* note 69.

[72] A Google spokeswoman stated this when asked about the process that Google employs when it receives an RLSW. Andrea Vittorio, *Robbery Poses Legal Test for Police Use of Google Location Data*, BLOOMBERG L. (Sept. 14, 2021, 5:01 AM), https://www.bloomberglaw.com (log in to Bloomberg Law account, enter search query for "Robbery Poses Legal Test for Police Use of Google Location Data", sort results by "Relevance," and select the first search result) [https://perma.cc/97XK-X7MW].

their information will be shared with the government.[73] Google continually boasts its users' privacy policy, stating that the protection of its users' personal information is of the utmost importance and further claims the company is doing its best to safeguard this exceedingly important right to privacy.[74] However, the question is—does Google think users' personal information should be protected against access by governmental agencies and law enforcement? If so, there seems to be a significant amount of dissonance between the statements Google has made and the actions it has taken.[75]

C. Privacy Concerns of Geolocation Tracking

Many Americans might not care *per se* if their locations are shared with the government since they are not engaging in suspicious activities, much less activities that are illegal.[76] These Americans believe that "privacy is something that only criminals desire."[77] Although this perspective has been acknowledged as a general argument in favor of such forms of intrusive surveillance, that viewpoint still does not negate the fact that knowing an

---

[73] *See How Google Handles Government Requests for User Information*, GOOGLE (last visited Oct. 13, 2021), https://policies.google.com/terms/information-requests [https://perma.cc/9YBN-BG48].

[74] *See Sundar Pichai's Testimony Before the Senate Commerce Committee*, GOOGLE (Oct. 28, 2020), https://blog.google/outreach-initiatives/public-policy/sundar-pichai-testimony-senate-commerce-committee/ [https://perma.cc/R6HQ-GLRA] ("When it comes to privacy we are committed to keeping your information safe, treating it responsibly, and putting you in control.").

[75] *Compare id.*, *with* Aaron Mackey & Jennifer Lynch, *It's Time for Google to Resist Geofence Warrants and to Stand Up for Its Affected Users*, ELEC. FRONTIER FOUND. (Aug. 12, 2021), https://www.eff.org/deeplinks/2021/08/its-time-google-resist-geofence-warrants-and-stand-its-affected-users [https://perma.cc/9KF9-U7H5].

[76] *See* Alex Abdo, *You May Have 'Nothing to Hide' But You Still Have Something to Fear*, ACLU (Aug. 2, 2013, 10:17 AM), https://www.aclu.org/blog/national-security/secrecy/you-may-have-nothing-hide-you-still-have-something-fear [https://perma.cc/X3QC-V8YD].

[77] *Id.*

individual's location and being able to continuously access that information serves as an immense form of power.[78]

Having individuals' geolocations goes beyond merely being able to see their locations based upon their longitudinal and latitudinal coordinates—it "reflects a wealth of detail about [individuals'] familial, political, professional, religious, and sexual associations."[79] Additionally, these surveillance techniques "evade[] the ordinary checks that constrain abusive law enforcement practices."[80] Thus, knowing individuals' locations depicts more than their geographic placements at certain times; having access to this information can non-consensually invade every personal aspect of their lives.[81]

Although unrealistic, one solution to the privacy concerns associated with RLSWs is to simply not have a cellphone or electronic device that tracks one's geolocation. Without a cellphone, individuals' locations and the details of their activities would remain private from government intrusion. As modern society relies extensively on technology, this solution is implausible.[82] Cellphones and electronic devices are so heavily ingrained in modern society that a "proverbial visitor from Mars might conclude that they were an important feature of human anatomy."[83]

---

[78] *See id.*; *see also* Riley v. California, 573 U.S. 373, 396 (2014) ("[Location data] can reconstruct someone's specific movements down to the minute, not only around town but within a particular building.").

[79] United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

[80] *Id.*

[81] *See id.*

[82] *See Mobile Phones and Society – How Being Constantly Connected Impacts Our Lives*, S. UNIV. (Aug. 10, 2016), https://www.southuniversity.edu/news-and-blogs/2016/08/mobile-phones-and-society-how-being-constantly-connected-impacts-our-lives-137313 [https://perma.cc/CCQ8-EX7F] [hereinafter *Mobile Phones and Society*].

[83] *Riley*, 573 U.S. at 385; *see* Monica Torres, *This Simple Job Hiring Requirement Can Reinforce Poverty*, HUFFPOST (Jul. 11, 2019, 4:21 PM), https://www.huffpost.com/entry/phone-verification-barrier-get-a-job_l_5d1cfc59e4b0f312567e1316 [https://perma.cc/QM2K-QRDA]. Americans rely on this form of communication and the ability to constantly be connected to others. *Id.* A perfect example of the reliance on cellphones is depicted through the requirement of individuals to be 'reachable' for employment purposes. *Id.* In most situations, an individual must have a cellphone or a phone that they regularly use in order to

If this increased intrusion is generally accepted, then one could justifiably be concerned about the quintessential "slippery slope" scenario: It would be more difficult for lawmakers to define a limitation in the future regarding the government's access to individuals' location data. The concept of constant and nonstop surveillance depicted in Orwell's *1984* appeared to be unbelievable and was brushed off as fiction—government control at an extreme.[84] However, facilitated by RLSWs, the U.S. government seems to be heading towards Orwell's depiction of a problematic government engaging in too much surveillance.[85] With the lack of legal safeguards surrounding RLSWs, law enforcement is currently able to receive the geolocations of any individual the government desires (i.e., to obtain investigatory information regarding who was in a particular location at a particular time), including—most concerningly—those of innocent individuals.[86]

IV. THE INTERSECTION OF REVERSE LOCATION SEARCH WARRANTS WITH THE FOURTH AMENDMENT

In recent years, the Supreme Court has been forced to grapple with new technological advancements and ascertain how these technologies fit in with the Constitution and the fundamental rights afforded to all U.S. citizens, but the Court has not yet specifically addressed RLSWs—although it should.[87] Three reasons the Court should address RLSWs include: (a) RLSWs constitute a search under the Fourth Amendment and do not fall under the third-party doctrine; (b) RLSWs do not satisfy the particularity requirement necessary for issuance of a warrant; and, (c) judges and magistrates are incorrectly applying a broader version of the particularity requirement in the Fourth Amendment that allows for these warrants to be issued.

---

be reached by current or potential employers. *Id.* The practical effect of such hiring policies and practices excludes a large portion of individuals without cellphones from being able to find stable employment. *Id.*

[84] *See* Orwell, *supra* note 18.

[85] *Id.*

[86] *See* Brandom, *supra* note 1.

[87] *See* U.S. v. Jones, 565 U.S. 400 (2012); Carpenter v. U.S., 138 S. Ct. 2206 (2018); Riley v. California, 573 U.S. 373, 385 (2014).

A. RLSWs and the Third-Party Doctrine

The third-party doctrine should not be applicable to geolocation data because individuals are not "voluntarily" disclosing their locations and internet searches to the public at large. In *Smith v. Maryland,*[88] the Supreme Court created an exception to the warrant requirement known as the third-party doctrine. Under this doctrine, "[b]y disclosing to a third party[,] the subject gives up all of his Fourth Amendment rights in the information revealed."[89] Simply stated, when an individual willingly shares information with a third party, that individual assumes the risk that the shared information could be further shared by the third party with others.[90] In *Smith*, the Court explained that the defendant had "assumed the risk" by "revealing" telephone numbers he had dialed to his telephone company (a third party); and therefore, those dialed telephone numbers could be turned over to law enforcement without a warrant.[91] The Court explained that the defendant "voluntarily" conveyed this information to the third party due to the defendant's knowledge of the phone company keeping these records for legitimate business purposes.[92] As such, the defendant's Fourth Amendment rights were not violated because the defendant did not have a subjective expectation of privacy, nor was such an expectation objectively one that society would recognize as reasonable.[93] Due to this voluntary sharing of information, the Court held that the government need not obtain a warrant to receive the information because obtaining and looking at the defendant's call records did not constitute an unreasonable search under the Fourth Amendment.[94] Rather, in sharing such information, a person or entity takes the risk that the third party is going to use the information however the party sees fit.[95]

---

[88] 442 U.S. 735 (1979).

[89] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009); *see Smith*, 442 U.S. at 743–744.

[90] *Id.*

[91] *Id.* at 735.

[92] *Id.* at 742–43.

[93] *Id.* at 743.

[94] *Id.*

[95] *Id.*

The third-party doctrine rests entirely on the concept that an individual assumes the risk that information voluntarily conveyed to another might be shared with others, including the government; and thus, there can be no reasonable expectation of privacy.[96] Although this doctrine makes the most sense when applied to government informants,[97] its application to modern technology, most notably to cellphones, deserves different treatment amongst courts. For there to be deemed an assumption of risk, there must be a choice made by the cellphone owner.[98] Moreover, this choice must be voluntary, meaning the information must be voluntarily and expressly given to a third party for a cellphone owner to have assumed the risk.[99] Currently, when it comes to cellphones and other electronic devices, individuals are likely not actively trying to convey their locations and internet searches to the public at large. However, service providers automatically collect this data, leaving the user at the ultimate mercy of cellphone companies and internet providers with respect to what information is obtained every time the user ventures into the public.[100]

As technology has progressed, it has become exceedingly more difficult for the Supreme Court to apply the third-party doctrine. Until *Carpenter v. United States*,[101] the circuits were split about whether cell-site location information ("CSLI"), which provides location points cataloguing the user's physical movements, fell within the third-party doctrine, thus allowing law enforcement to

---

[96] *Id.*

[97] U.S. v. White, 401 U.S. 745, 750–754 (1971) (differentiating between disclosing information to an informant because the individual is taking the risk that the person is not an undercover police officer or working as a confidential informant; the person is voluntarily sharing this information to another, they are not being forced to do so but actively engaging in the disclosure)

[98] Smith v. Maryland, 442 U.S. 735, 749–750 (1979) (Marshall, J., dissenting) ("Implicit in the concept of assumption of risk is some notion of choice . . . unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance.").

[99] *Id.*

[100] *See* Lynch*, supra* note 47.

[101] Carpenter v. U.S., 138 S. Ct. 2206 (2018).

receive such information without a warrant.[102] In *Carpenter*, the Court held that a warrant is required to receive an individual's CSLI.[103] The Court specifically maintained that the information transmitted through CSLI records is not "voluntarily provided" to the third party and thus does not fall under the third-party doctrine.[104]

Considering the similarities between CSLIs and RLSWs, the argument set forth in *Carpenter* can be applied to situations involving RLSWs. In relation to CSLIs, RLSWs gather location data in ways that are not "voluntarily" given.[105] An individual's geolocation, effectively the coordinates of that person's location, is not something that is being voluntarily given each time an individual's location point is catalogued.[106] Nevertheless, the geolocation points are tracked any time Google and other internet services "pick up" the location points through Bluetooth, cellular towers, and general use of any Google application.[107] More concerning, an individual does not even have to be actively using a Google application for it to track the individual's location.[108]

Some legal scholars support the application of the third-party doctrine to RLSWs. Specifically, these proponents argue that it is essential to our criminal justice system, especially considering the technological advancements that allow for individuals to hide their criminal activities through private transactions.[109] There is a worry

---

[102] *Compare In re* Application of U.S. for an Order Directing a Provider of Electronic Communications Services to Disclose Recs. To Gov't, 620 F.3d 304 (3d Cir. 2010), *with* U.S. v. Davis, 785 F.3d 498 (11th Cir. 2015).

[103] *Carpenter*, 138 S. Ct. at 2220 ("Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection.").

[104] *Id.*

[105] *See* Brandom, *supra* note 1; Valentino-DeVries, *supra* note 13; Kate Cox, *Supreme Court Will Decide If Your Mobile Phone Location Data Is Private*, CONSUMER REPORTS (June 5, 2017), https://www.consumerreports.org/consumerist/supreme-court-will-decide-if-your-mobile-phone-location-data-is-private/ [https://perma.cc/TF6Z-EUFF] (noting that even with your GPS disabled, the approximate location of the device is set to the carrier based on signal towers).

[106] Brandom, *supra* note 1; Valentino-DeVries, *supra* note 13; Cox, *supra* note 105.

[107] Lynch, *supra* note 47.

[108] *Id.*

[109] Kerr, *supra* note 89, at 573.

that individuals "could use third parties to create a bubble of Fourth Amendment protection around the entirety of [their] criminal activity."[110] Although it is possible that certain illegal activities could go undetected by law enforcement if the third-party doctrine applies, this fear is immaterial to the use of RLSWs because law enforcement is already aware that a crime likely occurred and is therefore requesting RLSWs to create suspect lists.[111] To address these concerns of the Fourth Amendment being used to shield criminal activity, the Supreme Court has applied a balancing approach, noting that sometimes criminals could be shielded from liability because some circumstances might necessitate concluding a criminal is not liable, so as to not erode Fourth Amendment protections.[112]

The major argument in favor of using RLSWs is that police only receive information about an individual's location in a specific public area at a specific time, and police would have been able to get the same information if they were in that area at the time the crime occurred.[113] In order for police to have been able to observe this interaction without RLSWs, law enforcement would have to expend more resources by stationing more officers in public places at all times. With RLSWs, law enforcement avoids these resource limitations and gains valuable information without doing much work.[114] Even though RLSWs are currently used to obtain information about activities conducted in public spaces, RLSWs can still reflect the intricacies of someone's life and, concerningly, the government is able to maintain such a record.[115]

B. RLSWs Fail the Probable Cause and Particularity Requirements

RLSWs fulfil neither the probable cause nor the particularity prongs that are required for magistrates to issue warrants. As

---

[110] *Id.* at 576.

[111] Broderick, *supra* note 34.

[112] Arizona v. Hicks, 480 U.S. 321, 329 (1987) ("But there is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of us all.").

[113] *See* U.S. v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

[114] *Id.*

[115] *Id.*

mentioned above, in order to secure a warrant under the Fourth Amendment, law enforcement must have probable cause and particularly describe the person, place, or thing intended to be searched or seized.[116] Probable cause refers to law enforcement having a reasonable and objective belief that an individual committed a crime.[117] Probable cause has been described as a "fluid concept," which "turn[s] on the assessment of probabilities in particular factual contexts."[118] Accompanying this requirement for probable cause, the Fourth Amendment also requires that police have a particularized intention with which to search or seize.[119] These safeguards were implemented by the Framers of the Constitution to ensure that general searches or seizures would be illegal, so that the government would not be a threat to the Nation's democracy.[120] These general warrants gave "the widest discretion to petty officials" by allowing law enforcement to search places, people, or things without individualized suspicion.[121] Therefore, this requirement for individualized suspicion differentiates warrants that sought solely the information necessary for the government to continue its investigation from warrants that unduly invaded citizens' privacy—the general warrants that the Framers prohibited.[122]

As previously stated, the application for an RLSW requires a lesser degree of particularity than the application for a traditional search or arrest warrant.[123] Instead of providing any details of a crime, law enforcement substitutes establishing probable cause for stating the specific crime that was committed and uses a time range

---

[116] U.S. CONST. amend. VI.

[117] *See* Illinois v. Gates, 462 U.S. 213 (1983).

[118] *Id.* at 232.

[119] U.S. CONST. amend. VI.

[120] Carpenter v. U.S., 138 S. Ct. 2206, 2213 (2018) ("The Founding generation crafted the Fourth Amendment as a 'response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.'" (quoting Riley v. California, 573 U.S. 373, 403 (2014)); *see also* Osmond K. Fraenkel, *Concerning Searches and Seizures*, 34 HARV. L. REV. 361 (1921).

[121] Fraenkel, *supra* note 120, at 362; *see also Riley*, 573 U.S. at 403.

[122] Fraenkel, *supra* note 120, at 362.

[123] *Supra* Part II.

and location range to satisfy the particularity requirement.[124] Although there is the argument that receiving this location data might reasonably lead police to uncover evidence related to the crime (i.e. the identity of a suspect), this argument does not adequately satisfy the underlying principles of the Fourth Amendment.

The information requested in RLSW applications does not meet the probable cause or particularity requirements—the safeguards integrated into the Fourth Amendment. Currently, law enforcement need only state that a crime occurred as their basis for probable cause and need not establish a probable cause for gathering the location data of hundreds—even thousands—of cellular devices that passed within the crime scene.[125] Law enforcement, however, does need to have an individualized suspicion about those believed to have committed the crime and cannot receive significant amounts of information about those determined to not be involved.[126]

Even with the knowledge that a crime occurred and the suspicion that the parties involved were able to be tracked through their geolocation, RLSWs do not comply with the particularity requirement. The warrants can have an exceedingly broad range that encompasses a significant amount of individuals' location data.[127] A warrant is not particularly described if most individuals identified through location data are not related at all to the criminal activity.[128] Through RLSWs, law enforcement is casting too wide of a net, encompassing innocent individuals, which could lead investigators to incriminate unsuspecting bystanders.[129] Based solely on the fact that RLSWs do not adhere to the safeguards of the Fourth Amendment, these applications for RLSWs must be effectively denied until law enforcement is able to include probable cause and particularly describe the area to be searched in a way that limits the innocent individuals searched.

---

[124] *See* Broderick, *supra* note 34.

[125] *Id.*

[126] In the Matter of the Search of: Information Stored at Premises Controlled by Google, No. 20 M 297 (N.D. Ill. July 8, 2020).

[127] *See id.* at *6.

[128] *Id.*

[129] *See* Valentino-DeVries, *supra* note 13.

C. Concerns About Magistrates Granting RLSWs

The decision to grant a warrant application is traditionally left to a "neutral and detached magistrate," who looks at the facts presented by the government and draws a conclusion as to whether the facts show that a warrant complies with the Fourth Amendment's requirements.[130] The Supreme Court has consistently relied on this concept of a judge that is disinterested and not "engaged in the often competitive enterprise of ferreting out crime."[131] Magistrates are deemed to be so outside the investigation and involvement of the crime that they do not have the same biased lens as law enforcement.[132] These neutral judges are tasked with issuing warrants in order to serve as a check against abusive government authority[133] and ensure that all constitutional requirements are followed accordingly.[134]

In RLSW applications, judges are accepting the fact that law enforcement has provided *any* form of particulars involving the time and location range as being enough to satisfy the particularity requirement.[135] This current approach in the context of RLSWs violates that prong of the Fourth Amendment. As required when assessing standard warrant applications, judges must consider information in a way that guarantees that there will be the minimum amount of intrusion upon the individual.[136] Instead of complying with this principle established by the Framers of the Constitution, judges are allowing the police to invade the private lives of individuals completely uninvolved in the crime under investigation.[137]

---

[130] Spinelli v. U.S., 393 U.S. 410, 415 (1969).
[131] *Id.*
[132] *See id.*
[133] *See id.*
[134] *See id.*
[135] *See generally Affidavit of Search Warrant*, *supra* note 30 (basing this assertion off how a judge signed off on the warrant, which contained no information outside of the specific geographic points and the time range about which the government was trying to receive information).
[136] *See* In the Matter of the Search of: Information Stored at Premises Controlled by Google, No. 20 M 297 (N.D. Ill. July 8, 2020).
[137] *Id.* at *6.

V. RECENT DEVELOPMENTS WITH AND RECOMMENDATIONS FOR JUDICIAL TREATMENT OF RLSWS

In recent years, American citizens have become more cognizant of the massive amounts of information cellphones gather and, more significantly, store about their daily lives.[138] This public awareness has led state legislatures in attempting to enact bills that protect the extensive data cellular devices store. Likewise, this recognition has not gone unnoticed in the judicial community as judges are beginning to understand the gravity of allowing the government to have access to cellular devices containing such intimate data.

A. Current State and Federal Legislative Trends

In many instances, courts have determined that the legislature should make decisions significantly affecting the lives of individuals, as the judiciary is not the branch of government elected to represent the interests of constituents.[139] Congress is the governmental body that is more closely tied to the people and is better able to discern what Americans want and need.[140] Within the context of technology, the Supreme Court has expressly supported this concept, meaning the legislature should be the body that defines the limitations of law enforcement's use of technology, such as RLSWs.[141]

In response to the recent protests for racial justice and police reform, legislatures at both the state and federal level have initiated action in trying to address law enforcements' increasing use of RLSWs. In New York, legislators proposed a bill that would outright ban RLSWs used by law enforcement in the State.[142]

---

[138] *See* Brenan & Stubbs, *supra* note 20.

[139] U.S. v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring) (citation omitted) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.").

[140] *Id.*

[141] *See id.*

[142] Issie Lapowsky, *New York Lawmakers Want to Outlaw Geofence Warrants as Protests Grow*, PROTOCOL (June 16, 2020), https://www.protocol.com/new-york-lawmakers-want-to-outlaw-geofence-warrants [https://perma.cc/3678-PVY4].

However, the New York Legislature has not yet enacted this law or a similar one.[143] The most notable bill introduced at the federal level was the Geolocation Privacy and Surveillance Act ("GPSA").[144] The GPSA would require law enforcement to obtain a warrant prior to receiving geolocation data and abide by stricter standards with which law enforcement would need to comply prior to a judge issuing a warrant.[145] These legislative proposals indicate that governments—at both the state and federal levels—have a genuine interest in keeping individuals' electronic information private; their constituents' data deserves protection, especially during law enforcement investigations.

Although there are ample public statements, political speeches, and proposed legislation to show that government representatives care about Americans' privacy interests amidst the increasing ability of technology to interfere with such interests, it is still difficult for representatives to fully execute this initiative politically. Recent attitudes about the scope of law enforcement's authority reflect a range of sentiments, such as a "tough-on-crime" attitude (the point of view that law enforcement should pursue any opportunity to "catch" those suspected of breaking the law, so long as law enforcement's general goal is to keep Americans safe by reducing the number of crimes occurring throughout the country).[146] Attitudes like this can inhibit, and even stop, legislators from advocating for their constituents' interests amidst law enforcements' ability to use technology, such as RLSWs, to assist in investigations by identifying suspects that otherwise would potentially endanger the public.

B. Denials of RLSWs by Judges and Magistrates

Significantly, the judicial tide appears to be turning towards a more burdensome threshold for law enforcement's RLSW

---

[143] *Id.*

[144] H.R. 3470, 115th Cong. (2017).

[145] *Id.*

[146] *See* Inimai M. Chettiar & Udi Ofer, *The 'Tough on Crime' Wave is Finally Cresting*, BRENNAN CTR. FOR JUST. (Jan. 16, 2018), https://www.brennancenter.org/our-work/analysis-opinion/tough-crime-wave-finally-cresting [https://perma.cc/2GUT-YHHT].

applications to be approved, as recent decisions by district court judges suggest denying RLSW applications is becoming more common.[147] Two judges in Chicago, Illinois[148] and one judge in Topeka, Kansas[149] denied requests for RLSWs, reasoning that the warrant applications did not comply with the Fourth Amendment.[150]

In *Matter of the Search of: Information Stored at Premises Controlled by Google*,[151] the government applied for RLSW to use in a criminal investigation of stolen pharmaceuticals that were subsequently sold.[152] This application for an RLSW was denied three separate times by three separate judges, even after amendments to the warrant were made.[153] Each request sought geolocation information from a single, forty-five-minute interval within a 100-meter radius of the same location for three separate days.[154] For each application, the judges found that the warrants for which law enforcement was applying were too broad and the items to be searched were not described with particularity.[155] As for the breadth of the RLSW application, one judge expressly acknowledged a

---

[147] *See* Jennifer Lynch & Nathaniel Sobel, *New Federal Court Rulings Find Geofence Warrants Unconstitutional*, ELEC. FRONTIER FOUND. (Aug. 31, 2020), https://www.eff.org/deeplinks/2020/08/new-federal-court-rulings-find-geofence-warrants-unconstitutional-0 [https://perma.cc/F99C-XDY4]; Thomas Brewster, *Google Geofence Warrants Endanger Privacy–Judges Now See The Threat*, FORBES (June 15, 2021, 10:38 AM), https://www.forbes.com/sites/thomasbrewster/2021/06/15/google-geofence-warrants-endanger-privacy-judges-now-see-the-threat/?sh=3afbbce5113a [https://perma.cc/4JVQ-T5DF].

[148] *In re* Information Stored at Premises Controlled by Google, No. 20 M 297 (N.D. Ill. July 8, 2020); *In re* Information Stored at Premises Controlled by Google, No. 20 M 392 (N.D. Ill. Aug. 24, 2020).

[149] *In re* Information that is Stored at the Premises Controlled by Google, LLC, No. 21-MJ-5064-ADM (K. June 4, 2021).

[150] *See In re* Information Stored at Premises Controlled by Google, No. 20 M 297, *6–7; *In re* Information Stored at Premises Controlled by Google, No. 20 M 392, *8–40; *In re* Information that is Stored at the Premises Controlled by Google, LLC, No. 21-MJ-5064-ADM, *7–9.

[151] No. 20 M 297.

[152] *Id.* at *1.

[153] Lynch & Sobel, *supra* note 147.

[154] *In re* Information Stored at Premises Controlled by Google, No. 20 M 297; *In re* Information Stored at Premises Controlled by Google, No. 20 M 392.

[155] *In re* Information Stored at Premises Controlled by Google, No. 20 M 297, at *6; *In re* Information Stored at Premises Controlled by Google, No. 20 M 392, at *27.

concern that the geographical location listed—an area in a city encompassing many commercial businesses and a busy road—would have dragged significant amounts of individuals not involved in the crime into the dragnet.[156] The judge held that a warrant "is not 'narrowly tailored' when the vast majority of cellular telephones likely to be identified" are not related to the crime.[157] Moreover, the judge found that the application failed the probable cause requirement because the agents were not restrained from obtaining information about every device tracked within the RLSW.[158] Therefore, without this objective measure satisfied, the RLSW application was "devoid of any meaningful limitation."[159]

In Kansas, a district court judge denied the government's application for an RLSW of a federal crime based upon the similar reasoning of overbreadth and lack of probable cause shown in several parts of the application.[160] First, the judge found that the government lacked probable cause to believe that the perpetrator had possession of a device at the time of the crime and thus be able to be tracked by obtaining the information requested in the RLSW.[161] Similarly, the judge found that the government had not shown why there was probable cause for the one-hour time range requested when the video surveillance showed the suspect for not even ten minutes.[162] Lastly, the judge stated that there was a lack of probable cause for the surrounding buildings and commercial spaces to be included in the RLSW, as there was no explanation for why the government needed to obtain the geolocation data of individuals within those areas.[163] With these denials of RLSWs being more publicly available, there is a possibility that judges and magistrates will increasingly look more closely at the unanswered questions within the RLSW applications.

---

[156] *In re* Information Stored at Premises Controlled by Google, No. 20 M 297, at *6.
[157] *Id.*
[158] *Id.* at *7.
[159] *Id.* at *6.
[160] *In re* Information that is Stored at the Premises Controlled by Google, LLC, No. 21-MJ-5064-ADM (K. June 4, 2021).
[161] *Id.* at *4–6.
[162] *Id.* at *8–9.
[163] *Id.* at *8.

VI. RECOMMENDATIONS FOR LIMITATIONS ON RLSWS

Although RLSWs are unconstitutional in their current form, they could be useful to law enforcement without infringing upon Fourth Amendment or citizens' privacy rights. This Article suggests that RLSWs could be effectively limited by: (A) narrowing the geographic area and time range associated with RLSWs; (B) imposing objective limitations on the number of devices captured through the warrants; (C) treating RLSWs as a last resort for law enforcement; and, (D) issuing RLSWs only in exigent or emergency circumstances.

A. Narrowing the Geographical Area and Time Range

As highlighted above, RLSWs can be extremely and unnecessarily intrusive; however, this type of warrant has the potential to serve as a valuable tool in criminal investigations, so long as the RLSW is limited in its scope and use.[164] For example, RLSWs could be adequately constrained by only gathering data of individuals that were particularly close to the crime at the time the crime occurred. This narrow standard would involve specific limitations on both the geographical location and time range that the warrant encompasses for judges to accept the application.

One of the primary reasons that judges have been reluctant to issue these types of warrants is that RLSWs incorporate such a wide area and time range and therefore could catch hundreds of thousands of cellphone users,[165] a majority of which were not involved in the crime.[166] As a means of combatting this expansive—and likely unnecessary—scope, law enforcement agencies should be restrained in their request to search a certain area and time. By enforcing this restriction, judges could decrease the number of individuals that might be caught in law enforcement's dragnet and thus effectuate

---

[164] *See generally In re* Information Stored at Premises Controlled by Google, No. 20 M 297 *6 (N.D. Ill. July 8, 2020) (referencing how the RLSW application was overbroad, and how limitations could improve to ensure that RLSWs are "narrowly tailored").

[165] *See id.*

[166] *See id.*; *In re* Information Stored at Premises Controlled by Google, No. 20 M 297, at *6.

the purpose of identifying the perpetrators of the crime using an RLSW without implicating innocent bystanders.[167]

Currently, there are no specific limitations for judges as to the geographical area or time range RLSWs can encompass; rather, the government need only show probable cause for these ranges.[168] These large geographical areas and time ranges can capture hundreds, even thousands, of individuals' information, despite being uninvolved in the crime under investigation. Thus, RLSWs, as they are currently used, effectively fail to serve their true purpose—to find the perpetrator of the crime.[169] In order to accurately determine the perpetrator, the requested location should be set as close to the crime scene as possible to make the information and location patterns more relevant to the search. Establishing an overly expansive location drags in unnecessary information, making the investigative process longer and less effective.[170] In most situations, limiting the time allowed for RLSWs would also decrease the number of individuals whose information is gathered by reducing the window of opportunity that individuals could have passed through the geofence.

As previously noted, New York is the only state to propose a bill that would entirely outlaw the use of RLSWs by law enforcement agencies;[171] however, this state action is too extreme because RLSWs do afford law enforcement a means to potentially obtain essential information to generate leads for investigations. Instead, state legislatures and Congress should pass laws that provide specific limitations on the time and location that can be requested and allotted in the warrant. These limitations should be further assessed to ensure they are the least intrusive means of acquiring the relevant information for the investigation, thereby greatly reducing

---

[167] *See generally In re* Information Stored at Premises Controlled by Google, No. 20 M 297 (asserting that reducing the radius of the geofence and time range would reduce the number of individuals caught in the net).

[168] *Compare id.*, *with In re* Information that is Stored at the Premises Controlled by Google, LLC, No. 21-MJ-5064-ADM (K. June 4, 2021).

[169] *See In re* Information Stored at Premises Controlled by Google, No. 20 M 297, at *6.

[170] *See In re* Information Stored at Premises Controlled by Google, No. 20 M 297.

[171] *See* Lapowsky, *supra* note 142.

the number of innocent bystanders swept into these RLSW dragnets. As always, the government must still show probable cause for the time and location ranges it is requesting, and the limited scope set forth by Congress would ensure that judges clearly stay within the bounds of the Fourth Amendment.[172]

B. Imposing Objective Limitations on the Amount of Information Obtained from Devices

The other significant problem of RLSWs is that they do not fit the particularity requirement of the Fourth Amendment. Rather, RLSWs give law enforcement agents discretion to identify any individual who was within the identified geofence.[173] To satisfy the particularity requirement, law enforcement must include an objective limitation that restricts the access of police to identifying information (e.g., gathering the information of only ten cellphones).[174]

As stated in *Matter of the Search of: Information Stored at Premises Controlled by Google*,[175] an RLSW application has no objective limitation if, by means of the warrant, the government would be able to effectively identify all individuals' devices that were picked up in the dragnet.[176] Although law enforcement has claimed that it will only identify devices "relevant to the investigation,"[177] this general assurance is not an objective limitation that would effectively constrain police. One of the judges that denied the government's application suggested that the RLSW could "contain objective limits as to which cellular telephones agents could seek additional information" or indicate that "a very limited number of cellular telephones would be identified."[178] To effectuate this standard, the RLSW could propose an exact number of devices to be identified and searched rather than—to the discretion of law

---

[172] *See supra* Part II.

[173] *See In re* Information Stored at Premises Controlled by Google, No. 20 M 297, at *6–7 (N.D. Ill. July 8, 2020).

[174] *See id.*

[175] No. 20 M 297.

[176] *Id.* at *7.

[177] *Id.* at *6.

[178] *Id.* at *7.

enforcement—all those devices "relevant" to the investigation.[179] Government officers would accordingly have limited access to the amount of information available to them but at least access to enough information to effectuate the purpose of the RLSW—to find the perpetrator of the crime under investigation. Additionally, the RLSW should separately state that law enforcement will not be gathering more than a set number of identifications, with a stricter limit if they have no evidence of co-conspirators or other individuals that were involved in the criminal activity. This reduced scope of accessibility would potentially satisfy the particularity requirement as it would restrain law enforcement in the number of individuals that can be identified in the RLSW, as well as the devices that would be seized.[180]

C. Treating RLSWs as a Last Resort

The degree of restraint on how law enforcement can use RLSWs is the paramount concern, as these warrants have consistently been overbroad since their inception.[181] Due to the extensive amount of information gathered through Google and other internet providers, this information should only be available to law enforcement upon a sufficient showing that the information is needed. Thus, judges should only issue an RLSW when law enforcement has demonstrated that they have exhausted all leads and their investigation is unable to proceed without the RLSW. If this standard is not followed, then it would have a detrimental effect as law enforcement would rely on these warrants and potentially avoid following proper procedure before resorting to this intrusive investigative tool.[182]

Judges and magistrates serve as the neutral individuals that law enforcement must convince to grant this warrant for a lawful search or seizure.[183] Thus, judges and magistrates should require a showing

---

[179] *Id.*
[180] *Id.*
[181] *See supra* notes 154–57.
[182] *See generally* U.S. v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (referencing how police are using intrusive technology to evade the regular constraints of law enforcement of limited resources).
[183] Spinelli v. U.S., 393 U.S. 410, 415 (1969).

of necessity and exhaustion of all other means and resources for the crime under investigation. This showing of necessity should include evidence that depicts law enforcement has neither leads on the crime nor any potential for furthering the investigation without an RLSW.[184] Examples of sufficient evidence could include proof of no witnesses, extensive interviews of neighbors, individuals close to the scene who have already been identified, friends and family of the victim(s), and other video surveillance that could have been utilized. This evidence should be presented along with the RLSW to prove that law enforcement has pursued all investigative leads and is therefore left with no alternative but to request to obtain information via an RLSW.[185] With the obscene amount of information that can be divulged through these warrants, judges and magistrates should be required to follow this standard before granting law enforcement an RLSW in order to protect Americans' constitutional right to privacy.

D. Issuing RLSWs Only in Exigent or Extreme Circumstances

Considering the incredible amount of information that RLSWs encompass, these warrants should be utilized only when circumstances call for such an intrusion, such as in extreme circumstances or for crimes that pose a significant public safety threat.[186] As previously referenced, RLSWs have been used in a variety of criminal investigations, ranging from homicide to arson and burglary.[187] Allowing this widespread use makes RLSWs more accessible for law enforcement to employ in everyday activities, evidenced by Google receiving up to 180 requests per week.[188] Confining the instances for which RLSWs can be requested will likely decrease this demand and ensure that the potential

---

[184] *See* Brandom, *supra* note 1 (explaining how RLSWs are used when law enforcement has hit a dead-end and are not able to gather useful evidence by any other means).

[185] *Id.*

[186] *See supra* Part II (referencing how location data is a huge intrusion on an individual's privacy).

[187] *See In re* Information Stored at Premises Controlled by Google, No. 20 M 297 (N.D. Ill. July 8, 2020); Valentino-DeVries, *supra* note 13; Dukes, *supra* note 13.

[188] Valentino-DeVries, *supra* note 13.

information law enforcement can obtain does not become a guaranteed, easily requested commodity.

Most importantly, in determining when obtaining an RLSW is entirely necessary, the necessity should be weighed appropriately against the level of intrusion on individuals' private information. For instance, receiving the location pattern of individuals, especially those who appear to be unrelated to the crime, should receive a high level of protection, thus the application must establish a strong reason for requiring the RLSWs.[189] As such, were an unarmed burglary at a convenience store to occur, that should not weigh heavily enough to gather the private locational data of individuals within a two-mile area within an hour of the burglary. Instead, RLSWs should be used only in extreme cases that involve a threat to public safety if the perpetrator of the crime is not detained. If RLSWs become accessible for even minor legal offenses, then balancing access to information and protection of location information would be inconsequential. In effect, the threshold for obtaining an RLSW would be incredibly low, whereby law enforcement would solely be required to provide minimal evidence in order to establish a need to obtain information that could potentially infringe on the privacy of many individuals and—even worse—could potentially incriminate innocent bystanders.

VII. CONCLUSION

As currently used, RLSWs afford law enforcement the ability to obtain intimate information about individuals' lives without satisfying the procedural requirements of the Fourth Amendment. These investigative tools, although beneficial to law enforcement, invade individuals' privacy rights and should solely be approved in limited circumstances to avoid collecting location data of individuals not involved in the crime. In order to reduce law enforcement's access to innocent individual's information, state legislatures and Congress should enact laws that limit the

[189] *See supra* Part II. *See generally* Emergency Searches, 16A West's Pa. Prac., Criminal Practice § 19:30 (referencing the balancing of the needs of law enforcement against individual liberties and the "heavy burden" the police have to bear when demonstrating the urgency of acting without a warrant).

geographical and time ranges that can be issued in RLSWs. Judges should only approve RLSWs that have an objective limitation on the amount of identifying information that they will be able to obtain from internet service providers, such as Google. Similarly, judges should require law enforcement to treat RLSWs as a last resort for when officers have exhausted all other investigative avenues. Lastly, to reduce the influx and requests for RLSWs, these warrants should only be issued in situations in which the public safety threat would significantly outweigh the privacy interests of those individuals encompassed by the reach of the RLSW. Without these limitations, there appears to be no end to what the government can observe of its citizens, and Americans gets one step closer to the feared, dystopian society depicted by Orwell.