Journal of Criminal Law and Criminology

Volume 111 | Issue 3 Article 5

Summer 2021

Rethinking Reverse Location Search Warrants

Mohit Rathi

0091-4169/21/11103-0805
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 111, No. 3

Printed in U.S.A.

RETHINKING REVERSE LOCATION SEARCH WARRANTS

Mohit Rathi*

The conflict between personal liberty and collective security has challenged Americans throughout the ages. The reverse location search warrant, which provides police officers with the ability to access location information on every smartphone that passes within a certain radius around a crime scene, is the newest chapter in this conflict. This technology is relatively new, but it is slowly being adopted by technologically savvy police departments across the country. While the reverse location search warrant could help officers catch and prevent crimes, the technology comes at the cost of providing police departments with unprecedented access to the location information of individuals that might not have otherwise satisfied traditional probable cause as required by the Fourth Amendment.

This Comment first seeks to provide a high-level explanation of the reverse location search warrant, including the process by which this type of warrant is served to judges. It then discusses the role of Google, the primary provider of location information, in cooperating with law enforcement. Next, it outlines the technical and constitutional concerns created through the use of reverse location search warrants, specifically addressing concerns around the accuracy of Google's location information data, judges' ability to meaningfully review these warrants, and potential Fourth Amendment challenges that reverse location search warrants might face. It next discusses the benefits that reverse location search warrants might provide to police departments across the country, including connecting otherwise seemingly disparate crimes and providing defense attorneys with location information they can use to protect their clients. Finally, this Comment proposes that the judiciary create an emergency exception to the probable cause framework in order to analyze reverse location search warrants. This exception is necessary because these search warrants raise unique technological and

* Northwestern Pritzker School of Law, Class of 2021. Thank you to everyone who helped me write and review this note, and special thanks to Professor Ronald Allen and the whole editing team on the Journal of Criminal Law and Criminology.

constitutional issues that are difficult to analyze under the probable cause framework. Alternatively, this Comment provides three common-sense legislative solutions which, if adopted, would help limit the privacy impact that reverse location search warrants could have on citizens across the country.

INTRODUCTION

From Orwell to *The Hunger Games*, the concept of a dystopian world where every citizen's actions are monitored and reported has been a part of our society's subconscious for the past few decades. There is a growing sense of fear among many people that the same technological changes that have drastically improved our lifespan and productivity might also bring about the end of privacy as we know it.[1] This Comment examines one such technological change being adopted by local and federal law enforcement agencies across the country: the reverse location search warrant. This type of warrant allows police officers to request cell phone location information from any mobile device within a certain radius of a crime scene at the time the crime occurred.

This powerful new technology has the potential to make our lives safer by helping law enforcement catch dangerous criminals, but it also provides law enforcement with unprecedented discretion in accessing private location information. As is so often the case with crime-solving technology, the question is not *whether* reverse location search warrants will become more common, but *when* they will. In light of this new technology, it is important to consider what can be done to protect fundamental privacy concerns.

More specifically, the reverse location search warrant has the potential to erode the Fourth Amendment protection from warrants that lack probable cause. Currently, courts use the probable cause framework when analyzing warrants, but reverse location search warrants present unique technological and constitutional issues that are more difficult to analyze under traditional probable cause analysis. Accordingly, this Comment argues that courts should move away from the probable cause framework, at least within the context of reverse location search warrants, to ensure that they can adequately protect fundamental privacy concerns. If courts are unwilling to do so, then federal and state legislatures should adopt new laws and regulations to ensure that reverse location search warrants are defined

---

[1] *See, e.g.*, Lew McCreary, *What Was Privacy?*, HARV. BUS. REV. (Oct. 2008), https://hbr.org/2008/10/what-was-privacy [https://perma.cc/Q68T-YWX9]; Marc Groman, *As Technology Advances, What Will Happen With Online Privacy?*, FORBES (Jan. 15, 2019), https://www.forbes.com/sites/quora/2019/01/15/as-technology-advances-what-will-happen-with-online-privacy/#421c69af1c45 [https://perma.cc/XHS2-3LZW]; Charlie Warzel, Opinion, *We No Longer Expect Privacy. You Can Change That*, N.Y. TIMES (Dec. 3, 2019), https://www.nytimes.com/2019/12/03/opinion/privacy-tips.html [https://perma.cc/ULN8-YYEH].

narrowly and that judges have adequate information when deciding whether to approve these warrants.

Part I of this Comment provides background information on reverse location search warrants and the process police officers use to request them. It also analyzes the role of Google, the primary provider of detailed location information in the modern landscape, in cooperating with law enforcement agencies. Part II outlines technical concerns raised by reverse location search warrants, especially with regards to the judicial approval process, and discusses the potential societal benefits of adopting reverse location search warrant technology. Part III discusses Fourth Amendment "probable cause" jurisprudence broadly, as well as the constitutional challenges reverse-location search warrants are likely to face in coming years. Part IV proposes creating an exception to Fourth Amendment probable cause jurisprudence in the context of reverse location search warrants, before finally suggesting three common-sense legislative proposals that could collectively limit these warrants' impact on privacy rights.

I. REVERSE LOCATION SEARCH WARRANTS AND THE ROLE OF GOOGLE

The reverse location search warrant is a relatively new technology employed by police officers to catch criminals using the location information stored on criminals' phones. This Part of the Comment will provide background information on the reverse location search warrant, including a high-level description of the technology and how police officers use it. It will then describe the role of Google, the primary provider of location information for reverse location search warrants, in cooperating with law enforcement agencies across the country. Lastly, this Part will address Google's response to privacy concerns and its efforts to push back against overly broad requests from law enforcement.

A. HOW REVERSE LOCATION SEARCH WARRANTS WORK

Since at least 2017, law enforcement officers across the country have been using reverse location search warrants.[2] Rather than targeting a specific person, reverse location search warrants target location information pulled from mobile devices within a specified location.[3] This technology is gaining prominence partially due to the efforts of a corporation, ZetX, which travels

---

[2] Aaron Mak, *Close Enough: Police Departments Are Using "Reverse Location Search Warrants" to Force Google to Hand over Data on Anyone Near a Crime Scene*, SLATE: FUTURE TENSE (Feb. 19, 2019), https://slate.com/technology/2019/02/reverse-location-search-warrants-google-police.html [https://perma.cc/K7AW-AF9Y].

[3] *See id.*

around the country promoting its new software, Trax, to local law enforcement agencies.[4] Trax "recognizes cell phone data in any format from any provider and uses it to map the cell towers, create visuals of call information, [and] highlight callers' habits."[5] Once law enforcement installs this software, Trax can even automatically fill out search warrants: police officers simply select the area where the crime occurred on a map, and the longitudinal coordinates of the crime scene automatically populate directly into the warrant.[6] This technology, combined with corporations such as Google's extensive location tracking, makes it easier for law enforcement to request more reverse location search warrants.

Reverse location search warrants are typically split into two or three smaller warrant requests.[7] In the first warrant, law enforcement requests location data from a company—almost always Google.[8] That company provides location information from the smartphone of everyone who has come within a set distance of the crime scene.[9] This information is anonymous at first.[10] Once law enforcement officers narrow down the list of potential suspects based on the individual movement patterns revealed by the initial data, they request a second warrant to acquire more details, including the names and account information of any suspects.[11] The way Google obtains this information depends on the type of phone a suspect uses.[12] Google obtains this information from Android phones directly; for other smartphones, Google obtains this information through its applications, such

---

[4] *See* Merrin Overbeck, *Constitutionality of Cell Site Location Information Use*, UNIV. RICH. J. L. & TECH. (Sept. 9, 2019), https://jolt.richmond.edu/2019/09/09/constitutionality-of-cell-site-location-information-use/ [https://perma.cc/U5L5-48HE].

[5] *Id*.

[6] Melanie Basich, *Trax from Zetx: Visual Analysis*, POLICE MAG. (July 17, 2014), https://www.policemag.com/341174/trax-from-zetx-visual-analysis [https://perma.cc/T82E-SDPK].

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

[8] Google is the only company that has admitted to having the technological capability to perform these searches. *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/9BMZ-A8PX] [hereinafter Valentino-DeVries, *Tracking Phones*].

[9] Jennifer Valentino-DeVries, *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works.*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html [https://perma.cc/5T8H-395W] [hereinafter Valentino-DeVries, *Google's Sensorvault*].

[10] *Id*.

[11] *Id*.

[12] *See* Mak, *supra* note 2.

as Gmail, Chrome, or Google Maps.[13] Google derives location information from GPS tracking instead of cell-site location information (CSLI), which the Supreme Court has held requires a showing of probable cause to access.[14] GPS location tracking derives location information from mobile devices directly instead of triangulating their position based on cell phone towers; as such, it provides more accurate and detailed information than CSLI.[15]

The collected GPS information is then loaded into Google's platform for hosting location data, Sensorvault, which Google also uses for targeted advertising.[16] For instance, Google uses Sensorvault to check if a person physically entered a store he or she viewed advertisements for online and then reports back to the store about whether the advertisement they purchased was effective.[17] It is possible to opt out of sharing location information with Google in this way;[18] however, Google prompts users to re-enable Sensorvault when setting up applications such as Google Maps or even regular Google searches with location enabled.[19] Thus, it is difficult for Google users to avoid having their location information collected.

Law enforcement has employed the reverse location search warrant in multiple jurisdictions.[20] Police departments in Raleigh, North Carolina; Orange County, California; and Minnesota have all used this technology in the last two years.[21] The reverse location search warrant's growing use raises serious Fourth Amendment concerns, as people can be searched through the first warrant[22] simply because they walked near a crime scene, which may not satisfy traditional probable cause analysis.[23] As explained further *infra*,[24] the reverse location search warrant arguably puts the cart before the horse

---

[13] *See id*.

[14] Carpenter v. United States, 138 S.Ct. 2206, 2221 (2018) (holding that the requirement for probable cause for a search warrant extended to warrants involving CSLI).

[15] *Id*. at 2219.

[16] Valentino-DeVries, *Google's Sensorvault*, *supra* note 9.

[17] *Id*.

[18] Samuel Gibbs, *How to Turn off Google's Location Tracking*, GUARDIAN (Aug. 14, 2018), https://www.theguardian.com/technology/2018/aug/14/how-to-turn-off-google-location-tracking [https://perma.cc/7CDJ-DQDQ].

[19] Valentino-DeVries, *Google's Sensorvault*, *supra* note 9.

[20] *See* Mak, *supra* note 2.

[21] *Id*.

[22] *See* George Joseph, *Manhattan DA Got Innocent People's Google Phone Data Through A 'Reverse Location' Search Warrant*, GOTHAMIST (Aug. 12, 2019), https://gothamist.com/news/manhattan-da-got-innocent-peoples-google-phone-data-through-a-reverse-location-search-warrant [https://perma.cc/T6LM-JX29].

[23] *See* Valentino-DeVries, *Tracking Phones*, *supra* note 8.

[24] *Infra* Part C.

through this first smaller warrant. While the second warrant in a reverse location search warrant might satisfy the probable cause framework, the first warrant has a much weaker justification because it is granted simply on the basis of an individual being near a crime scene.

B. GOOGLE'S COOPERATION WITH LAW ENFORCEMENT

Google can lawfully provide law enforcement officials with customer location information through the third-party doctrine, a common law principle which states that people who voluntarily give up their information to third parties have "no reasonable expectation of privacy."[25] In the case of reverse location search warrants, the third party is typically Google, which receives up to 180 requests for location information from law enforcement per week.[26] Under this doctrine, by agreeing to use location services, customers would likely be considered to have given up their location information to Google.[27] Thus, consumers who opt into Google's location services may have their information shared with the government.

Law enforcement officers also send these requests to other tech corporations that store customer location information.[28] One of Google's competitors, Apple, maintains that it currently lacks the capability to provide law enforcement officers with easily digestible location information.[29] At least outwardly, Apple's approach to sharing geolocation data seems more

---

[25] *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."). The Supreme Court has applied this doctrine in a variety of contexts. *See, e.g.*, Carpenter v. United States, 138 S.Ct. 2206, 2216 (2018); United States v. Jacobsen, 466 U.S. 109, 122–23 (1984).

[26] Valentino-DeVries, *Tracking Phones*, *supra* note 8.

[27] *See* Nathaniel Sobel, *Do Geofence Warrants Violate the Fourth Amendment?*, LAWFARE (Feb. 24, 2020), https://www.lawfareblog.com/do-geofence-warrants-violate-fourth-amendment [https://perma.cc/ZLE3-THY4] (discussing one recent case that might resolve this question).

[28] Charles Blain, *Police Could Get Your Location Data Without a Warrant. That Has to End*, WIRED (Feb. 2, 2017), https://www.wired.com/2017/02/police-get-location-data-without-warrant-end/ [https://perma.cc/YA5B-2V8H].

[29] Isobel Asher Hamilton, *Google Could Be Bankrupting Apple's Privacy Promises by Handing over iPhone Data to the Police*, BUS. INSIDER (Apr. 15, 2019), https://www.businessinsider.com/google-bankrupting-apple-privacy-promises-by-handing-data-to-police-2019-4 [https://perma.cc/5TYG-LEM2].

consumer privacy-forward than Google's.[30] Apple's public refusal to help the FBI break into the phone of Rizwan Farook, who, in 2015, carried out a shooting rampage that killed 14 people in San Bernadino, California, provides further support for this image.[31] Apple stated that helping the FBI investigate Farook would "set a dangerous precedent" for the future.[32] Apple appears to approve of the perception that it is more privacy-forward than Google, as it has released posters and advertisements mocking Google for its cooperation with law enforcement.[33]

The two companies' apparently differing stances on providing information to law enforcement might suggest that any needed change to location information sharing practices must come from individual corporations like Google. But despite its public persona, even Apple has provided the FBI with location data it possesses.[34] In fact, it's possible that the only reason Apple does not provide the same level of information to law enforcement as Google is because they lack the technological capability to do so.[35] Indeed, given tech companies' ever-increasing revenue from targeted advertisements,[36] it may be only a matter of time before most or even all tech

---

[30] Kate O'Flaherty, *Apple Issues New Blow to Facebook and Google with this Bold Privacy Move*, FORBES (Nov. 6, 2019), https://www.forbes.com/sites/kateoflahertyuk/2019/11/06/apple-issues-new-blow-to-facebook-and-google-with-this-privacy-move/#4fff26d1481d [https://perma.cc/UG8C-S5CL]. *But see* Ian Bogost, *Apple's Empty Grandstanding About Privacy*, ATLANTIC (Jan. 31, 2019), https://www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680/ [https://perma.cc/3VCP-NJUS].

[31] Laura Wagner, *The Apple-FBI Debate Over Encryption: FBI Says It May Be Able to Access Shooter's iPhone Without Apple's Help*, NPR (Mar. 21, 2016), https://www.npr.org/sections/thetwo-way/2016/03/21/471353161/fbi-says-it-may-be-able-to-access-shooters-iphone-without-apples-help [https://perma.cc/82SH-9SSQ].

[32] Hamilton, *supra* note 30.

[33] *Id.*

[34] Tim Cook, the CEO of Apple, has written that "[w]hen the FBI has requested data that's in our possession, we have provided it." *Id.*

[35] Valentino-DeVries, *Tracking Phones*, *supra* note 8 (investigators involved in using a reverse location search warrant told the New York Times that they had not sent other tech companies reverse location search warrant requests, and Apple said it did not have the capability to perform this kind of search).

[36] Megan Graham, *Digital Ad Revenue in the US Surpassed $100 Billion for the First Time in 2018*¸ CNBC (May 7, 2019), https://www.cnbc.com/2019/05/07/digital-ad-revenue-in-the-us-topped-100-billion-for-the-first-time.html [https://perma.cc/4ZF3-NW95] (explaining that digital advertising revenue recently hit an all-time high and continues to grow at double-digit rates).

companies begin storing detailed location information and providing this information to law enforcement agencies.[37]

C. GOOGLE'S RESPONSE TO PRIVACY CONCERNS

In response to growing privacy concerns, Google now elects to provide consumers with details on the kinds of requests it receives from law enforcement and the types of data consumers are at risk of disclosing to law enforcement agencies.[38] Google's Privacy and Terms policy states that the company receives government requests for information directly, and in criminal cases it requires search warrants before disclosing the content of email communications, documents, and photos.[39] Google also receives less extensive requests from law enforcement in the form of court orders.[40] Like search warrants, these court orders typically require judicial review and can provide officers with information such as IP addresses or non-content portions of emails such as headers or timestamps.[41] Google also states that in emergency cases, in order to prevent serious bodily harm or death, it voluntarily discloses user information to government agencies at its own discretion.[42]

According to Google, it has made at least some strides in protecting users' privacy from law enforcement. For example, Google has stated that it pushes back against overbroad requests from law enforcement by screening warrant requests for errors and by asking judges to amend warrants to be less broad in terms of both the time period and the applications law enforcement

---

[37] But *see* Note, *Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance*, 131 HARV. L. REV. 1722 (2018) (discussing reasons tech companies might support privacy laws, namely "their patriotism and desire to maintain positive relationships with their regulators – even in the absence of appropriate legal process."). *But see* Martin Kaste, *Google Explains How it Handles Police Requests for Users' Data*, NPR (Jan. 28, 2013), https://www.npr.org/2013/01/28/170428992/google-posts-how-it-handles-requests-for-users-data [https://perma.cc/2272-CJDM] (stating that "[m]ost of the industry thinks tougher privacy law would be good for business, especially on cloud-based services").

[38] *Legal Process for User Data Requests FAQs*, GOOGLE: TRANSPARENCY REP. HELP CTR., https://support.google.com/transparencyreport/answer/7381738?hl=en [https://perma.cc/M3SK-JVZR] (last visited Feb. 12, 2019).

[39] *How Google Handles Government Requests for User Information*, GOOGLE: PRIVACY & TERMS, https://policies.google.com/terms/information-requests [https://perma.cc/86DK-424P] (last visited Mar. 20, 2021) (under "Requests for information made to Google LLC") [hereinafter GOOGLE: PRIVACY & TERMS].

[40] GOOGLE: TRANSPARENCY REP. HELP CTR., *supra* note 38.

[41] *Id*.

[42] *Id*.

officers can access.[43] Google also claims that it will notify any user whose information has been legally requested, unless such notifications are prohibited by law.[44] As a recent example, in January, 2020, Google's legal investigations team successfully notified a user in Gainesville, Florida that law enforcement had requested his location information.[45] The man had been flagged as suspicious by a reverse location search warrant because he passed the scene of a burglary three times while looping around his neighborhood on his bike.[46]

Law enforcement officials sometimes try to prevent companies from notifying users about these requests, arguing that these notifications might increase suspects' flight risk.[47] At law enforcement's request, courts can add a "gag order" under 18 U.S.C. § 2705(b) to these warrants.[48] In practice, gag orders bar Google and other tech companies from notifying customers when the government requests their data.[49] These gag orders can last indefinitely, and according to Mozilla's chief legal officer, "When requesting user data, these gag orders are sometimes issued without the government demonstrating why the gag order is necessary."[50] Though tech giants have been pushing back against government gag orders through both the court system[51] and creative technological solutions,[52] the apparent lack of accountability around

---

[43] Google, *Way of a Warrant*, YOUTUBE (Mar. 27, 2014), https://www.youtube.com/watch?v=MeKKHxcJfh0 [https://perma.cc/7K73-DYEA] (discussing the role of "producers," specialists who alongside Google's legal team examine warrants and work with investigators or judges to narrow down or amend overly broad warrants).

[44] GOOGLE: PRIVACY & TERMS, *supra* note 39.

[45] Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect*¸ MSNBC (Mar. 7, 2020), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/AG9R-AW3K].

[46] *Id.*

[47] John Ribeiro, *Google, Apple, Twitter, in Large Groups Backing Microsoft over 'Gag Orders'*, IT WORLD (Sept. 4, 2016), https://www.itworld.com/article/3116325/google-apple-twitter-in-large-group-backing-microsoft-over-gag-orders.html [https://perma.cc/DN7C-SVPV].

[48] *Id.*

[49] *Id*.

[50] *Id*. Requests for gag orders are made so frequently that challenging the orders would be prohibitively expensive for tech companies. As such, the government can obtain gag orders without proper explanations or any accountability. *See id.*

[51] Dave Lee, *Microsoft Sues US Government Over Secret Data Requests*, BBC (Apr. 14, 2016), https://www.bbc.com/news/technology-36050151 [https://perma.cc/V5XE-NZL9].

[52] Dan Gillmor, *Google Can't Tell You When the Government Wants Your Data. Here's a Sneaky Solution.*, SLATE TECH. (Jan. 29, 2015), https://slate.com/technology/2015/01/warrant-canaries-a-way-for-tech-companies-to-get-around-government-gag-orders.html [https://perma.cc/8TBY-W5TT] (explaining tech companies' use of the "warrant canary," a daily email

gag orders gives law enforcement wide discretion in applying 18 U.S.C. § 2705.[53]

Lastly, the Google Transparency Report lists the kinds of information Google typically discloses to law enforcement. The government can access email content, header information, sign-in IP addresses, and registration information through Gmail; sign-in IP addresses, registration information, video upload IP addresses, and private message content through YouTube; telephone records, billing information, registration information and IP addresses, stored text message content, and voicemails through Google Voice; and blog registration information, timestamps, IP addresses, and private comments through Blogger.[54] To some degree, this non-location information is protected from reverse location search warrant requests because it must be requested through a second warrant, and the initial warrant should have only given law enforcement access to anonymized location information. Still, as explained further below, this protection is not absolute. Reverse location search warrants can lead to the distribution of innocent persons' personal information to the police.

II. REVERSE LOCATION SEARCH WARRANTS: CHALLENGES AND BENEFITS

Like any new technology, reverse location search warrants present both challenges and benefits. This Part will address some of the technical challenges created by reverse location search warrants, including concerns related to the accuracy of Google's data and potential problems with how reverse location search warrants are served to judges. It will then lay out potential societal benefits created by the use of reverse location search warrants. These benefits include helping police officers catch criminals more efficiently and providing defense attorneys with a wealth of location information that they might then use to prevent wrongful convictions.

A. CHALLENGES POSED BY REVERSE LOCATION SEARCH WARRANTS

There are many technical concerns relating to the technology law enforcement uses to obtain reverse location search warrants. These concerns include the fact that GPS coordinates, rather than physical maps, are typically provided to the judges who review reverse location search warrants, that location information in these warrants may be inaccurate, and that innocent

service consumers can sign up for confirming that one's data has not been requested by law enforcement. The daily email does not arrive on days when law enforcement did actually request data).

[53] Ribeiro, *supra* note 47.

[54] GOOGLE: PRIVACY & TERMS, *supra* note 39 (under "What kinds of information do you disclose for different products?").

people's data can be at risk when these warrants are too broad. These concerns, while often technological in nature, always link back to the Fourth Amendment, which requires that all search warrants are supported by probable cause.[55]

1. How Reverse Location Search Warrants Are Served to Judges

One pressing concern is the way in which reverse location search warrant requests are served to judges. Specifically, reverse location search warrants often include complex GPS coordinates instead of a physical map displaying the area the warrant intends to surveil.[56] Police officers often map out the coordinates of the area they wish to survey within the Trax software (and related products such as Google Earth), but officers do not always provide these illustrations to judges, nor are they required to.[57] In the words of ACLU attorney Nathan Freed Wessler, "Most human beings can't interpret large strings of numbers and GPS coordinates without a map to illustrate them, and judges are no exception."[58] It seems unlikely that judges can accurately ascertain the size and physical features of the area they are authorizing for a search based on latitudinal and longitudinal coordinates alone, without a physical map to illustrate the buildings and general area covered by the reverse location search warrant. This is especially true in comparison to traditional search warrants, which typically authorize the search of a specific residence, computer, or person instead of an area generally.[59]

The volume of unsynthesized data presented by reverse location search warrants is especially problematic in light of the fast turnaround times for

---

[55] U.S. CONST. amend. IV.

[56] Tim Cushing, *Minnesota Judges Spent Only Minutes Approving Warrants Sweeping Up Thousands of Cellphone Users*, TECHDIRT (Feb. 12, 2019), https://www.techdirt.com/articles/20190211/08125241570/minnesota-judges-spent-only-minutes-approving-warrants-sweeping-up-thousands-cellphone-users.shtml [https://perma.cc/HNJ6-AYYN].

[57] Tony Webster, *How Did the Police Know You Were Near a Crime Scene? Google Told Them*, MINN. PUB. RADIO (Feb. 7, 2019), https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants [https://perma.cc/3LWR-Z9HV] (noting that only three of twenty-two warrants issued in Hennepin County, Minnesota included a map for the judges to visualize the area that the warrants encompassed).

[58] Yves Smith, *"Reverse Location Search Warrant": A New Personal Data Hoovering Exercise Brought to You by Google*, NAKED CAPITALISM (Feb. 12, 2019), https://www.nakedcapitalism.com/2019/02/reverse-location-search-warrant-a-new-personal-data-hoovering-exercise-brought-to-you-by-google.html [https://perma.cc/X8H6-ALTJ].

[59] FED. R. CRIM. P. 41(e)(2)(A).

search warrants in the modern era. A recent survey of public records[60] showed that most judges in Utah took less than three minutes to sign off on more than half of the warrants police had submitted over the period of a year.[61] The same study showed that judges spent about eight minutes on average reviewing a warrant and denied only two percent of proposed warrants.[62] Reviewing warrants so quickly can make meaningful review difficult, especially when complex technical information like longitudinal coordinates is involved. As one example, a judge in Edina, Minnesota reviewed a reverse location search warrant (which did not even include a map of the targeted area) for a maximum of four minutes before signing off on it.[63] Reviewing the warrant for such a short period of time makes it unlikely that the judge could analyze both the rationale behind the warrant and the scope of the area he or she was permitting the police to survey, especially without a map.[64] This concern is especially salient given that reverse location search warrants can cover a geographical area many times wider than traditional crime scenes, and a judge might have no idea that he or she signed off on a search of such a wide area.[65]

2. Concerns Related to Accuracy and Effectiveness

Reverse location search warrants also raise legitimate concerns related to the effectiveness and accuracy of location information. Research has shown that under some conditions, Google overestimates its own accuracy with regards to the exact location of a user ninety-three percent of the time.[66] Indeed, according to a 2018 forensic sciences study published by the U.S. National Library of Medicine, Google could only accurately ascertain that a device was somewhere within a fifty-two meter radius.[67] In tightly packed

---

[60] Conner Boyack, *Is the Warrant System Working Well?*, LIBERTAS INST. (June 6, 2019), https://libertasutah.org/justice-and-due-process/is-the-warrant-system-working-well/ [https://perma.cc/K8T2-J36Y].

[61] Jessica Miller, *New Data Show Utah Judges Are Often Spending Less than Three Minutes Viewing Warrants Before Approval*, SALT LAKE TRIB. (July 9, 2018), https://www.sltrib.com/news/2018/01/14/warrants-approved-in-just-minutes-are-utah-judges-really-reading-them-before-signing-off/ [https://perma.cc/A78F-UBSR].

[62] *Id*.

[63] Cushing, *supra* note 56.

[64] *Id*.

[65] Webster, *supra* note 57.

[66] Smith, *supra* note 58.

[67] *Id.*; for the study, see Andrea Marcellus Rodriguez, Christian Tiberius, Roel van Bree, Zeno Geradst, *Google Timeline Accuracy Assessment and Error Prediction*, U.S. NAT'L LIBRARY OF MED. (Oct. 23, 2018), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6201806/ [https://perma.cc/55HG-EEFL].

urban environments such as metropolitan cities, fifty-two meters can mean the difference between being directly at the scene of a crime and at home asleep a few floors upstairs. And because judges may grant a second, more extensive, search warrant on the basis of suspicious location movements tracked during the first warrant,[68] inaccurate location information pulled in response to the first warrant could lead to innocent parties having their information shared with the police, raising significant privacy concerns.

Similarly problematic is the fact that, as the technology used to generate reverse location search warrants becomes more widely known, professional criminals might learn to opt out of location sharing services, leave their cellular devices at home during crimes, or stop using smart phones entirely. Google allows users to clear their Google Maps history,[69] and criminals might be more likely to use this feature because they have something to hide. On the other hand, innocent people, who have nothing to hide from law enforcement, might not adopt the same precautions. Thus, if professional criminals are able to effectively dodge reverse location search warrants, the use of these warrants could drive up the number of wrongful arrests in criminal cases and even result in wrongful convictions.

This risk of increasing wrongful convictions is sobering, especially given the United States' already high rate of wrongful convictions.[70] Moreover, wrongful convictions disproportionately victimize Black people.[71] Studies show, for example, that Black people wrongfully convicted of crimes like murder must wait longer to be exonerated compared to their white counterparts.[72] In this way, reverse location search warrants may have troubling implications for racial justice. To accurately ascertain whether the risk of wrongful convictions would increase over time because of reverse location search warrants, further research must be conducted.

---

[68] *See* Gelb, *supra* note 7, at 68.

[69] Andrew Martonik, *How to Clear Search and Location History in Google Maps on Android*, ANDROIDCENTRAL (July 26, 2019), https://www.androidcentral.com/how-clear-search-and-location-history-google-maps-android [https://perma.cc/93SF-8Y3J].

[70] Samuel Gross, *The Staggering Number of Wrongful Convictions in America*, WASH. POST (July 24, 2015), https://www.washingtonpost.com/opinions/the-cost-of-convicting-the-innocent/2015/07/24/260fc3a2-1aae-11e5-93b7-5eddc056ad8a_story.html_[https://perma.cc/FLM6-Y2VA] (citing studies that show up to 4.1% of defendants sentenced to death might be wrongfully convicted).

[71] Niraj Chokshi, *Black People More Likely to Be Wrongfully Convicted of Murder, Study Shows*, N.Y. TIMES (Mar. 17, 2017), https://www.nytimes.com/2017/03/07/us/wrongful-convictions-race-exoneration.html [https://perma.cc/XAN9-E7S9].

[72] *Id*.

3. The Collection of Innocent People's Data

Even if reverse location search warrants do not lead to an increase in wrongful convictions, at the very least, this technology could result in the collection of many innocent people's data. Police departments often request location information tracked hours before and after a crime and from areas much larger than the crime scene itself.[73] Once police close the case, the location data collected, as well as any other information brought up during the course of the second warrant, could become part of the case file whether accurate or not.[74] Case files become part of the public record, and for this reason, details about innocent individuals' locations could become subject to public scrutiny.[75]

Because Trax is so new, case files involving investigations where police have used this technology are still largely open and thus unavailable to the public.[76] Cause for concern is growing, however, as once these records become available to the public[77] or get leaked, the tracked location information could become subject to scrutiny from the press. This scenario is not unprecedented. An innocent man in Minnesota who drove a cab within 170 feet of a crime scene had his name released to a local journalist after it become part of the police record.[78] Furthermore, there is a risk of police officers themselves accessing location data once it becomes part of a criminal file. This access opens up the potential for abuse of power by malicious law enforcement officers who can find people's home addresses and daily schedules, among other information.[79]

---

[73] Smith, *supra* note 58 (stating that one query made by the federal government covered a total area of 45 hectares, or 111 acres).

[74] *Id*.

[75] *Contra* 5 U.S.C. § 552 (stating The Freedom of Information Act would protect against any requested location information which fell under the personal privacy exemption, but the location information would remain on police systems).

[76] Valentino-DeVries, *Tracking Phones*, *supra* note 8. For one example of a legal challenge against reverse location search warrants currently in the court system, see Tim Cushing, *Reverse Warrant Used in Robbery Investigation Being Challenged as Unconstitutional*, TECHDIRT (July 10, 2020), https://www.techdirt.com/articles/20200709/13185544875/reverse-warrant-used-robbery-investigation-being-challenged-as-unconstitutional.shtml [https://perma.cc/B9FS-XRJK]; *see also* Sobel, *supra* note 27.

[77] Paul Grabowicz, *Police Records*, BERKELEY GRADUATE SCH. OF JOURNALISM, ADVANCED MEDIA INST., https://multimedia.journalism.berkeley.edu/tutorials/police-records/ [https://perma.cc/ZTH2-PNR9] (discussing the process by which police records become available to the public or reporters and how it can vary state by state).

[78] Valentino-DeVries, *Tracking Phones*, *supra* note 8.

[79] Charles Blain, *Police Could Get Your Location Data Without a Warrant. That Has to End*, WIRED (Feb. 2, 2017), https://www.wired.com/2017/02/police-get-location-data-without-warrant-end [https://perma.cc/9FM7-HHDA].

A final privacy concern related to information collected by law enforcement is that it could be collected or hacked by malicious third parties. One recent data breach incident involving the Los Angeles Police Department resulted in "the personal information of at least 20,000 people" being shared with malicious hackers.[80] Despite law enforcement agencies' efforts to prevent leaks and abuse by officers, the sheer amount of data processed in reverse location search warrants makes the likelihood of error and serious harm to innocent people an ever-present danger.

B. SOCIETAL BENEFITS CREATED BY REVERSE LOCATION SEARCH WARRANTS

Despite these drawbacks, reverse location search warrants could also create benefits, both for law enforcement agencies and for the constituencies they police. By providing law enforcement officers with a visual representation of detailed location information for hundreds of people near a crime scene, reverse location search warrants can help law enforcement solve crimes and even connect otherwise seemingly disparate crimes. Location information in the hands of skilled defense attorneys also has the potential to exonerate innocent suspects and prevent wrongful convictions from occurring in the first place.

1. Solving Crimes

The primary benefit of the reverse location search warrant is its potential to solve crimes and catch criminals. The reverse location search warrant provides law enforcement agencies with detailed, anonymized location information for everyone who passes within a certain distance of the scene of a crime.[81] Police officers can use this wealth of information to find people with suspicious location histories. For example, they might discover a person who went to a local gun store the day before passing in front of the scene of a shooting. They can then in turn use this information to request a second warrant, gathering more detailed information on the potential suspect.[82]

Law enforcement agencies are already using these warrants to arrest suspects in certain jurisdictions. In Virginia, authorities arrested a suspect for

---

[80] Zak Doffman, *Cyberattack on LAPD Confirmed: Data Breach Impacts Thousands of Officers*, FORBES (July 30, 2019), https://www.forbes.com/sites/zakdoffman/2019/07/30/lapd-cyberattack-police-department-confirms-it-has-been-hacked/#55251e5a14be [https://perma.cc/K56K-YNPH] (discussing a data breach where the names, dates of birth, email addresses, passwords, and even the last four digits of social security numbers for over 17,500 police applicants and 2,500 police officers were collected by hackers and potentially put up for sale).

[81] Mak, *supra* note 2.

[82] *Id.*

robbing a bank based on the results of a reverse location search warrant sent to Google.[83] Examples such as this show the crime-fighting potential of the tool. Prosecutors and police officers assert that the tool has also proved helpful in "solving crimes such as pattern burglaries, arsons, and sexual assaults."[84]

While the crime-solving potential of this technology is clear, it may be difficult for certain law enforcement agencies to reap the benefits of reverse location search warrants. Urban areas, in particular, provide law enforcement agencies using reverse location search warrants with a special challenge. This is because a warrant for even a relatively small area in a metropolitan center (e.g., Times Square) might collect a huge number of people' information, making it more difficult for law enforcement officials to home in on suspects.[85] On the other hand, police departments in urban areas also tend to be larger and better funded than police departments in rural areas.[86] Thus, they may be well-positioned to use reverse location search warrants effectively.[87] For instance, larger bureaucracy and support staff presence at urban police departments can provide police officers with better implementation and integration of crime-mapping software.[88] Furthermore, larger police departments might be more likely to involve crime analytics staff in the use of crime-mapping technology like reverse location search

---

[83] 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) https://www.abajournal.com/magazine/article/law-enforcement-is-using-location-tracking-on-mobile-devices-to-identify-suspects-geofence [https://perma.cc/S3F5-DKLS].

[84] *Id*. On the other hand, it is unclear exactly how helpful the tool is when compared when traditional policing methods.

[85] Andrew Perrin, *Digital Gap Between Rural and Nonrural America Persists*, PEW RSCH. CTR. (May 31, 2019), https://www.pewresearch.org/fact-tank/2019/05/31/digital-gap-between-rural-and-nonrural-america-persists/ [https://perma.cc/4N5F-6ZML].

[86] Shako Liu & Phil McClausland, *Rural Police Struggle to Recruit Amid Poor Pay and Public Perception*, NBC NEWS (Nov. 10, 2019) https://www.nbcnews.com/news/us-news/rural-police-struggle-recruit-amid-poor-pay-public-perception-n1078496 [https://perma.cc/3SJN-A2V9] (urban areas tend to pay police officers better and be better staffed compared to rural areas, which have difficulties "acquiring up-to-date law enforcement resources and technology as they grapple with budget shortfalls.").

[87] *See generally* KEVIN STROM, NAT. CRIM. JUST. REFERENCE SERV., RESEARCH ON THE IMPACT OF TECHNOLOGY ON POLICING STRATEGY IN THE 21ST CENTURY, FINAL REPORT SERVICE (Sept. 2017), https://www.ojp.gov/pdffiles1/nij/grants/251140.pdf [https://perma.cc/F2VN-FTQS] (discussing how technology might positively impact policing strategy in the coming years).

[88] *Id*. at 4–6.

warrants. This specialized staff is often tech savvy and in a better position to assess the accuracy of mapping results than patrolling officers.[89]

Currently, adequate research into the effectiveness of reverse location search warrants is lacking.[90] Still, other crime-mapping solutions such as "hot-spot policing" and "risk-terrain modeling" have been shown to produce measurable benefits in urban municipalities through crime reduction.[91] Reverse location search warrants could provide similar benefits by making it easier for police officers to connect and solve seemingly disparate crimes. And providing police officers with the technology to connect disparate crimes could increase public safety and welfare by increasing law enforcement's ability to catch repeat criminals.

2. Preventing Wrongful Convictions

As discussed above, reverse location search warrants could expose innocent people to criminal liability in certain circumstances. But location information could also exonerate innocent suspects by proving their location during the time of the crime.[92] Law enforcement's gathering of detailed location information through mobile devices around crime scenes could actually help defense attorneys, who could use location information collected during discovery to exonerate innocent suspects who might not otherwise be able to prove their location at the time of the crime. Indeed, ZetX's own management team at one point listed shareability of information with defense counsel during the discovery process as one of the benefits of Trax.[93]

One well-funded public defender's office in New York has already tested whether location information might be useful to its clients.[94] The office purchased a laboratory full of digital forensics equipment and then provided

---

[89] *Id*.

[90] *Id*. at 4–5.

[91] *Id*. "Hot-spot policing" is a reactive strategy that deploys police officers to areas where crime is already most concentrated. "Risk-terrain modeling," which is more forward thinking, uses risk modeling to make future deployment decisions. Examples of better outcomes include reduced numbers of reported incidents or and reduced instances of observed physical and social disorder.

[92] For example, one man in New Haven, Connecticut, was recently exonerated from a murder and robbery conviction on the basis of previously hidden cell-site location information. *See* Kathleen McWilliams, *New Haven Man Jailed For 17 Years Freed after Judge Vacates Murder, Robbery Convictions*, HARTFORD COURANT (Apr. 25, 2018), https://www.courant.com/breaking-news/hc-br-vernon-horn-released-wrongful-conviction-20180425-story.html [https://perma.cc/KZ7Y-BSKC].

[93] Basich, *supra* note 6.

[94] Kashmir Hill, *Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone.*, N.Y. TIMES (Nov. 22, 2019), https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html [https://perma.cc/3L5L-4P5D].

location information on one client's Google phone as an alibi.[95] This led to the assistant district attorney dismissing the case against that client.[96] Similarly, a defense attorney in Gainesville, Florida recently used Google's location data to vindicate a client investigated on the basis of a reverse location search warrant.[97] These examples show how location information can be used by defense counsel to prove the innocence of suspects.

However, at the moment, public defenders and other defense attorneys often lack access to location information and other resources used by government prosecutors because it can be so expensive to pull information from a suspect's phone.[98] Because location information is so expensive to capture, the discovery process for a case involving a reverse location search warrant could allow defense attorneys to determine their own client's location and movements at a much lower cost. Eventually, widespread adoption of the technology around reverse location search warrants could lead to lower prices and greater accessibility to personal location information, allowing defense lawyers to better protect their clients.

III. POTENTIAL FOURTH AMENDMENT CHALLENGES TO REVERSE LOCATION SEARCH WARRANTS

Reverse location search warrants are likely to face a multitude of legal challenges as they become a mainstream tool used by law enforcement agencies. A primary vehicle for these challenges will likely be the Fourth Amendment, which states that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be searched."[99] Specifically, opponents may argue that reverse location search warrants do not satisfy the Fourth Amendment's probable cause requirement as it is traditionally understood. This Part will outline the history of the Fourth Amendment and discuss reverse location search warrants' similarities to problematic "general" warrants. Next, it will review recent Supreme Court jurisprudence relating to the Fourth Amendment's probable cause requirement and discuss whether reverse location search warrants satisfy this requirement.

---

[95] *Id*.

[96] *Id*.

[97] Schuppe, *supra* note 45.

[98] Hill, *supra* note 94 (discussing how equipment that analyzes location information costs around $100,000 – "a fortune in a public defender's budget").

[99] U.S. CONST. amend. IV.

A. REVERSE LOCATION SEARCH WARRANTS AS "GENERAL WARRANTS"

One of the potential challenges reverse location search warrants might face is that they are strikingly similar to the overly broad English general warrants which the Fourth Amendment was drafted to ban.[100] These general warrants were authorized by either the King or the courts, and "lack[ed] particularity regarding the person or place to be searched, or the papers or records to be seized."[101] At the time, some English and American writers considered general warrants to be the height of tyranny because they gave officers an incredible amount of discretion in deciding where and whom to investigate.[102] General warrants went so far as to allow officers to enter a house without a warrant if they were searching for a felon, which would have been condemned under common law at the time.[103] The solution to these concerns was the Fourth Amendment, which requires that warrants satisfy a "probable cause" standard before a judge signs them.[104]

Reverse location search warrants might be analogized to general warrants because both lack specificity with regards to the person or place to be searched. By not requiring police officers to have probable cause against any of the individual people they are searching before requesting location information, reverse location search warrants arguably recreate the exact issue the Framers were trying to prevent. Thus, from an originalist perspective, reverse location search warrants might circumvent the Framers' intentions behind the Fourth Amendment.

B. LOCATION INFORMATION & PROBABLE CAUSE

While an originalist challenge against reverse location search warrants is possible, arguments against the constitutionality of this technology will likely focus more on whether it satisfies probable cause. In *Brinegar v. United States*, the Court stated that probable cause must be "more than bare

---

[100] Thomas Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 551 (1999); *see also* Stanford v. Texas, 379 U.S. 476, 481 (1965) ("Vivid in the memory of the newly independent Americans were those general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists.").

[101] *Id*.; *see also* 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/KUQ2-SPA2].

[102] Davies, *supra* note 100, at 689–91 (discussing writings of James Otis, who "denounced general writs of assistance as a violation of American liberties" and John Adams, who wrote an abstract of Otis's argument that "[r]eason and the constitution are both against this writ").

[103] *Id*. at 578.

[104] U.S. CONST. amend. IV.

suspicion."[105] Instead, probable cause exists when a reasonable person acting on reasonably trustworthy information would have believed that based on the facts and circumstances of the case, the offense had been committed.[106] This standard leaves breathing room for some law enforcement error through the "reasonable" qualifier. [107]

More recently, in *Carpenter v. United States*, the Supreme Court confirmed that one of the goals of the Framers was to "place obstacles in the way of a too permeating police surveillance."[108] The *Carpenter* Court explained that the preservation of the Fourth Amendment required protection from the encroachments of advancing technology, specifically cell-site location information.[109] As such, the Court held that the government must "obtain a warrant supported by probable cause before acquiring such records;" it could not simply request the information through a court order.[110] The Court further stated that probable cause typically requires some level of "individualized suspicion."[111] Accordingly, law enforcement needed more than a court order to request personal location information under the Fourth Amendment because the showing required to get a court order did not reach the level of probable cause.[112]

The Supreme Court decision in *Carpenter* specifically concerned whether or not a warrant was required in the context of cell-site location information (CSLI).[113] The case arose when the government requested CSLI for suspected accomplices to a robbery and used this information to prove that the suspects were at or near the crime scene during the time of the robbery.[114] The CSLI referred to in *Carpenter* is created through cell phones pinging nearby radio antennas, which are called cell sites.[115] While the Court made it clear that the government must generally show probable cause in

---

[105] Brinegar v. United States, 338 U.S. 160, 175–176 (1949) (holding that "[p]robable cause exists where 'the facts and circumstances within their (the officers') knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that' an offense has been or is being committed.") (quoting Carroll v. United States, 267 U.S. 132, 162 (1925)).

[106] *Id*.

[107] *Id*.

[108] Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

[109] *Id*. at 2223.

[110] *Id*. at 2221.

[111] *Id*.

[112] *Id*.

[113] *Id*. at 2208–09.

[114] *Id*. at 2212–13.

[115] *Id*. at 2208–09.

order to receive CSLI,[116] the Court has yet to indicate whether this reasoning extends to GPS location information.[117] However, Justice Sotomayor's concurrence in *United States v. Jones*, where the Court similarly considered location data, seems to at least suggest that law enforcement agencies would need warrants (and in turn, probable cause) in order to track the location information of a regular person through GPS technology.[118]

Furthermore, as the Court held in *Carpenter*, probable cause requires some level of individualized suspicion based on the facts.[119] In *In re Oakland*, one federal court expounded on this, holding that a warrant compelling "any individual," including non-suspects who were simply present at the scene covered by the warrant, to unlock their device through biometric measures was overbroad because the request was not limited to "a particular person nor a particular device."[120] Though the California court made this decision within the context of biometric technology, it acknowledged its duty under *Carpenter* to protect individuals' constitutional rights from technological encroachments.[121] Courts could apply similar reasoning to overturn reverse location search warrants, which can cover every phone in a specific area and similarly do not list every individual or device that they are targeting. Reverse location search warrants, like the warrant in *In re Oakland*, are problematic because of the way that they capture the location data of innocent people who were simply present at the time of a lawful arrest.[122]

C. PROBABLE CAUSE ANALYSIS AS APPLIED TO REVERSE LOCATION SEARCH WARRANTS

Based on the reasoning in *Carpenter* and *In re Oakland*, reverse location search warrants put the cart before the horse. The second warrant in a reverse location search warrant would likely satisfy the probable cause framework established by the Court due to its basis in suspicious location information

---

[116] *Id*.

[117] *Id*.

[118] United States v. Jones, 565 U.S. 400, 416–17 (2012) ("GPS monitoring—by making available at a relatively low cost such a substantial quantum of information about any person whom the Government, in its unfettered discretion, choose to track—may 'alter the relationship between citizen and government in a way that is inimical to a democratic society.'").

[119] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

[120] In re Oakland, 354 F. Supp. 3d 1010, 1014 (N.D. Cal. 2019).

[121] *Id*. ("The challenge facing the courts is technology is outpacing the law. In recognition of this reality, the United States Supreme Court recently instructed courts to adopt rules that 'take account of more sophisticated systems that are already in use or in development.'") (quoting *Carpenter*, 138 S. Ct. at 2218–19).

[122] *Id*.

trends brought to light through the first warrant. However, the first warrant has a much thinner justification. Essentially, to satisfy the test under *Carpenter*, law enforcement officials must make the argument that being near a crime scene puts one under enough individualized suspicion to satisfy the probable cause requirement even though proximity to a crime scene might have nothing to do with criminal activity.[123]

This argument is not as far-fetched as it might sound, especially when search warrants are narrowly defined. Evidence showing that a stranger's cell phone was inside an apartment within an hour of a murder or theft would certainly make many reasonable police officers suspicious about the activities of the cell phone's owner.[124] In this way, narrowly defined reverse location search warrants can be analogized to traditional warrants for individuals seen by eyewitnesses or caught on video camera near the crime scene. However, reverse location search warrants authorized for huge areas or vast periods of time are much harder to justify. As such, courts should push back against overly broad reverse location search warrants to ensure that law enforcement acts properly within the probable cause framework.

In addition to pushing back against broad reverse location search warrants, courts should also consider the fact that, perhaps unlike information provided in traditional warrants, the GPS information provided by law enforcement in reverse search warrants may not be particularly reliable.[125] As the Court stated in *Brinegar*, part of satisfying probable cause requires a judge to evaluate whether the warrant they are authorizing is based on "reasonably trustworthy" information.[126] The Court simplified this requirement in *Illinois v. Gates*, where it stated, "[t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth [. . .] there is a fair probability that contraband or evidence of a crime will be found in a particular place."[127] Reverse location search warrants make this analysis more complicated because unaided judges are often ill-suited to the task of evaluating the

---

[123] *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) ("The Court requires 'some quantum of individualized suspicion' before a search or seizure take place.").

[124] Ben Levitan, *How Cellphones Help Catch Criminals*, CRIME ONLINE (Dec. 29, 2016) https://www.crimeonline.com/2016/12/29/cellphones-and-criminals/ [https://perma.cc/HV2H-P2UP].

[125] Illinois v. Gates, 462 U.S. 213, 266 (1983) (concurring with the majority and stating that courts assume good faith in police officers and should eschew inquiries into the "subjective beliefs" of law enforcement); *see supra* notes 67–68.

[126] Brinegar v. United States, 338 U.S. 160, 175–176 (1949).

[127] *Gates*, 462 U.S. at 238.

accuracy of data provided by Google and other location information providers.[128]

As already explained, the accuracy of Google's information is far from perfect.[129] Thus, judges decide whether probable cause exists without adequate information about both the size of the targeted area and the accuracy of the GPS tracking data that is informing the warrant.[130] Additionally, the second warrant within a reverse location search warrant is based on the results of the first warrant.[131] This means that when judges authorize the second warrant, they are likely proceeding on the assumption that Google provided law enforcement with results accurate enough to be considered "reasonably trustworthy."[132] This assumption might be justified because the "reasonable" qualifier leaves police officers some room for error in requesting warrants.[133] Until the technology improves, however, legitimate concerns around the trustworthiness of warrants issued based on Google's location information will persist, even when judges find that the warrants satisfy probable cause.

In summary, Fourth Amendment challenges against reverse location search warrants are inevitable.[134] These challenges might come from an originalist perspective based on the similarity between reverse location search warrants and general warrants. However, they will likely be primarily based on the Supreme Court's decision in *Carpenter*, with litigants arguing that courts may not grant a request to search every mobile device in an area because such a request would not be based on individualized suspicion, and accordingly, it would not satisfy the Court's probable cause standard.[135] In fact, these challenges have already begun. A federal district court in Richmond, Virginia is currently preparing to rule on a Fourth Amendment challenge against a reverse location search warrant.[136] Both defense counsel and the government relied on the ruling in *Carpenter* in the case's briefing, which also included a neutral amicus from Google.[137] Defense counsel even compared reverse location search warrants and general warrants in their briefings, before arguing that the third-party doctrine should not apply to

---

128 Webster, *supra* note 57.

129 *See supra* Part B.

130 Webster, *supra* note 57.

131 Gelb, *supra* note 7 at 69.

132 Brinegar v. United States, 338 U.S. 160, 175–76 (1949).

133 *Id*. at 176.

134 Valentino-DeVries, *Tracking Phones*, *supra* note 8.

135 Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

136 Sobel, *supra* note 27.

137 *Id*.

Google's location information and stating that reverse location search warrants are "invalid ab initio," or void.[138] The outcome of this pending litigation will serve as a litmus test for the success of Fourth Amendment challenges against reverse location search warrants.

IV. PROPOSED JUDICIAL AND LEGISLATIVE SOLUTIONS

The traditional probable cause framework might have been appropriate at the time it was put forward. But in recent years, the weight of technological innovation and changing consumer privacy expectations may have pushed it to its limits.[139] Reverse location search warrants are especially problematic because judges might struggle to assess the probability that warrants will lead to evidence based on the information law enforcement provides, especially within the limited time judges spend reviewing warrants.[140] This Part will discuss two potential solutions to this challenge. First, courts can use an alternative framework when deciding whether to grant reverse location search warrants. Second, federal and state legislatures can adopt three legislative proposals that collectively would put judges in a better position to decide whether warrants satisfy probable cause.

A. ALTERNATIVE FRAMEWORKS: A NEW PROBABLE CAUSE EXCEPTION

Though the Fourth Amendment's language explicitly requires that warrants be supported by probable cause,[141] there are exceptions to this requirement.[142] Examples of these exceptions include exigent circumstances,[143] searches incidental to arrest,[144] and hot pursuit.[145] In this

---

[138] *See id.* In this context, *invalid ab initio* means void or having no legal effect.

[139] Riley v. California, 573 U.S. 373 (2014); *see also Carpenter*, 138 S. Ct. 2206. In both cases, the Supreme Court elected to create unique carve outs from established doctrine partially because of the immense capacities of modern technology, such as cell phones, to store users' personal information.

[140] Cushing, *supra* note 56.

[141] U.S. CONST. amend. IV.

[142] Clifford Fishman, *Searching Cell Phones After Arrest: Exceptions to the Warrant and Probable Cause Requirements*, 65 RUTGERS L. REV. 995, 1003 (2013).

[143] Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (holding that warrants are required to search a home unless there are exigent circumstances, such as needing to enter a home in order to fight fire or prevent the destruction of evidence).

[144] *Riley*, 573 U.S. at 383 (holding that searches incidental to arrest are lawful even without a warrant).

[145] United States v. Santana, 427 U.S. 38, 43 (1976) (holding that police could make a warrantless entry when following a suspect who retreated into her house in order to avoid arrest).

vein, courts could create a new exception to the probable cause requirement to address the unique problems presented by reverse location search warrants. Similar to exigent circumstances cases, the court would essentially be acknowledging that while reverse location search warrants do not satisfy traditional probable cause analysis, in some emergency circumstances they might be needed in order to prevent a greater tragedy. One example of a situation where the government might argue that their interest in national security outweighs constitutional concerns would be in the context of terrorist threats.[146]

To determine whether the exception applies, courts could perform a balancing test for reverse location search warrants. Under this balancing test, courts would weigh the government's need for information in specific, emergency circumstances against the risk of violating people's Fourth Amendment rights. This alternative framework follows reasoning similar to that used in cases involving "exigent circumstances."[147] The exigent circumstances[148] exception allows officers to take certain actions, such as conducting warrantless searches, that would otherwise be legally suspect, in order to protect or preserve lives.[149] Google's policy of providing information without a warrant in emergency circumstances shows that even large corporations agree that when human life is at imminent risk, privacy concerns can become secondary.[150] Courts must be cautious in considering whether a particular request falls within the exigent circumstances exception in light of the constitutional concerns related to warrantless searches.[151] They would need to be similarly judicious in granting reverse location search warrants for this emergency balancing test solution to work. For example, courts would need to carefully consider the area surveyed and the context of the warrant as well as how pressing law enforcement's need for information is.

---

[146] Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google, and Others*, GUARDIAN (June 7, 2013, 3:23 PM), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/B9ZG-3X3U] (discussing the U.S. Government's PRISM program, where, in order to combat terrorist threats, the NSA directly accessed information held by tech corporations like Google and Facebook to surveil American citizens).

[147] Payton v. New York, 445 U.S. 573, 583 (1980) (holding that in certain emergencies, or "exigent circumstances," police could enter a home without a warrant).

[148] Exigent circumstances refer to "emergency or dangerous situations," not just day-to-day policing matters such as petty theft. *Id*.

[149] Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

[150] GOOGLE: TRANSPARENCY REP. HELP CTR., *supra* note 38.

[151] Welsh v. Wisconsin, 466 U.S. 740, 750 (1984) (stating that due to the "sanctity of the home," judges should not allow warrantless arrests for minor offenses).

This proposed balancing test framework would allow judges to take the purpose of a reverse location search warrant into account when deciding the whether to grant it. Law enforcement agencies, however, may not support this new approach since it may prevent them from using a valuable tool in their arsenal in some circumstances, and courts tend to give great deference to law enforcement agencies.[152] Courts might also hesitate to propose a balancing test because of the additional strain on judicial resources any speed bump in the warrant approval process could create.[153] Judges must always be on call in order to approve warrants, and law enforcement may call in at odd hours as needed.[154] Indeed, as judges already seem to lack the time or resources necessary to spend more than several seconds to review a warrant,[155] they may be especially reluctant to add a balancing test. Given the limitations of a judicial solution, a better solution would be for state and federal legislatures to write laws ensuring that reverse location search warrants satisfy traditional probable cause analysis.

B. LEGISLATIVE SOLUTIONS

While some state lawmakers may prefer to ban reverse location search warrants entirely, as some have already proposed,[156] others will likely aim to regulate them more closely. For the jurisdictions focused on regulation, there are a few common-sense legislative solutions that could significantly minimize the reverse location search warrant's impact on privacy and also have a good chance of passing. In today's polarized political environment, cooperation between both parties in state and federal legislatures might seem quixotic at best, but consumer privacy expectations are a bipartisan

---

[152] Anna Lvovsky, *The Judicial Presumption of Police Expertise*, 130 HARV. L. REV. 1995, 2052 (2017).

[153] Jonathan R. Nash, *Aiming for Simplicity, the Supreme Court Makes Things More Complicated*, HILL (July 13, 2016, 9:43 AM), https://thehill.com/blogs/pundits-blog/the-judiciary/287520-aiming-for-simplicity-supreme-court-opts-for-complexity [https://perma.cc/QEB7-3PX7].

[154] Dale Harris, *A Judges View: Warrants Can't Wait, so a Judge Always is on Call*, DULUTH NEWS TRIB. (Jan. 6, 2016, 3:00 PM), https://www.duluthnewstribune.com/opinion/3918552-judges-view-warrants-cant-wait-so-judge-always-call [https://perma.cc/4BD9-NRA5].

[155] Miller, *supra* note 61.

[156] In New York, Senator Zellnor Myrie and Assembly Member Dan Quart are pushing for the protection of constitutional rights by banning reverse location search warrants entirely in their proposed "Reverse Location Search Prohibition Act." Nicolette J. Zulli, *Scaling the (Geo)Fence: New York Lawmakers Push to Outlaw Geofence Warrants amid Ongoing National Debate for Police Reform*, LEXOLOGY (June 19, 2020), https://www.lexology.com/library/detail.aspx?g=3414b576-479a-4ebe-81c9-787ac220767b [https://perma.cc/DS5R-S5M5].

concern.[157] Both Republicans and Democrats in Congress continue to draft privacy bills addressing the distribution of personal information and the role of corporations in protecting consumer privacy.[158] In 2019 alone, over 150 pieces of legislation on data privacy were considered by state legislatures in both blue and red states.[159]

Thus, it seems possible that some of these legislatures might consider including regulations on reverse location search warrants as part of their comprehensive data privacy reform bills.[160] Furthermore, passing legislation, especially at the federal level, would ensure more uniform compliance across jurisdictions. This Comment proposes three specific laws that would cumulatively limit the reverse location search warrant's impact on privacy: a printed maps requirement, a mandated anonymization process for information gained via the first warrant, and a requirement that law enforcement erases unnecessary data collected by reverse location search warrants.[161]

1. Printed Maps Requirement

The first and simplest legislative proposal would require that all reverse location search warrants contain a printed map of the area in question alongside GPS coordinates. In order to satisfy a probable cause analysis, the warrant must present an area that judges can actually visualize. GPS coordinates or written descriptions might be helpful, but they do not provide judges with a full picture of the area to which they are granting police access. For example, a warrant might say "between the Hilton hotel and the intersection on Chicago Avenue" but fail to make note of the large residential apartment complex in between those two places. This would be problematic because the judge might unknowingly authorize the search of thousands of extra mobile devices belonging to people simply going about their day-to-day lives. A current map printed from Google Earth or any equivalent

---

[157] Charlie Warzel, *Will Congress Actually Pass a Privacy Bill?*¸ N.Y. TIMES (Dec. 10, 2019), https://www.nytimes.com/2019/12/10/opinion/congress-privacy-bill.html [https://perma.cc/Q2KX-JXJW] (discussing two similar privacy bills brought forward by both parties which are currently being negotiated on the Senate floor).

[158] *Id*.

[159] Michael Beckerman, *Americans Will Pay a Price for State Data Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html [https://perma.cc/YQ97-BJZF].

[160] *Id*.

[161] These solutions are simply a first step towards solving the problem of reverse location search warrants. As the technology becomes more widely adopted, I recommend further studies testing the accuracy of GPS location information and the effectiveness of reverse location search warrants in combatting crime.

software could help prevent this problem and lead to fewer people having their information needlessly shared with law enforcement.

Implementing this kind of legislation should be relatively inexpensive, as the Trax software used by law enforcement to create reverse location warrants already has the capability to create maps using Google Earth.[162] In fact, law enforcement officers already use the Trax software to map the area they are targeting before sending coordinates.[163] Law enforcement officials would only need to attach a copy of the map they created to the warrant before sending it to a judge. This simple legislative measure would allow judges to more thoroughly analyze whether a reverse location search warrant satisfies probable cause and could prevent police officers from casting too wide a net.[164]

2. Mandated Anonymization Process for the First Warrant

A second legislative proposal would require the initial reverse location search warrant to be protected by some anonymization process so that law enforcement would be unable to trace the location information back to individuals without getting judicial approval for a second warrant. Currently, Google uses a system of anonymized numbers in place of names when providing information in the initial reverse location warrants, which leads to a relatively higher degree of privacy for individuals whose sensitive location information is shared with law enforcement.[165] More detailed account information, including the people's names, is withheld from law enforcement officers until they narrow down the list of suspects and request a second warrant based on suspicious location history and trends.[166] As other tech companies expand their ability to collect location information, state and federal legislatures should codify Google's anonymization process to ensure that individuals' location information is adequately protected.

Limiting police access to personal information could go a long way towards curtailing abuses by police officers and information leaks to the press. This proposed legislation would also provide a baseline privacy standard for smartphone consumers. This concern may become even more important as tech companies ramp up their use of location tracking services

---

[162] Basich, *supra* note 6.

[163] *Id*.

[164] Additional information disclaiming the accuracy of GPS information (perhaps based on current weather conditions) could also help judges make probable cause decisions. It is worth exploring this topic further when there is more data around reverse location search warrants and GPS accuracy.

[165] Valentino-DeVries, *Google's Sensorvault*, *supra* note 9.

[166] Valentino-DeVries, *Tracking Phones*, *supra* note 8.

in response to the Covid-19 pandemic and the need for contact tracing.[167] This legislation would also help hold Google accountable if consumer privacy becomes less valuable[168] to the company in the future.[169] Finally, keeping personal information anonymous during the initial warrant would also help ensure that reverse location search warrants satisfy probable cause analysis. This is because with anonymization, the initial warrant would only authorize a very limited release of data to law enforcement on the basis of being near a crime scene.

3. Erasing Unnecessary Data Collected by Reverse Location Search Warrants

A third and final legislative proposal would require that police departments dispose of unneeded information (location-related or otherwise) derived from reverse location search warrants after the investigation is considered closed. Currently, police departments nationwide may keep data pulled from sources such as reverse location search warrants in their archives indefinitely.[170] This practice may make sense for information derived from traditional search warrants because everyone implicated in those warrants likely at least satisfied the probable cause analysis. Reverse location search warrants, however, can contain the location information of many more innocent people than traditional warrants, especially in metropolitan areas.[171] This information is not easily accessible to the public through Freedom of Information Act requests,[172] but information held by law enforcement could

---

[167] Kif Leswing, *As Workplaces Slowly Reopen, Tech Companies Smell a New Multibillion-Dollar Opportunity: Helping Businesses Trace Coronavirus*, CNBC (May 10, 2020, 2:13 PM), https://www.cnbc.com/2020/05/10/coronavirus-tracing-for-workplaces-could-become-new-tech-opportunity.html [https://perma.cc/EK4P-NRED].

[168] Angela Moon & Paresh Dave, *Exclusive: Fearing Data Privacy Issues, Google Cuts some Android Phone Data for Wireless Carriers*, REUTERS (Aug. 19, 2019, 5:04 AM), https://www.reuters.com/article/us-alphabet-data-exclusive/exclusive-fearing-data-privacy-issues-google-cuts-some-android-phone-data-for-wireless-carriers-idUSKCN1V90SQ [https://perma.cc/55PY-CYWP] (discussing one example where Google removed a valuable service because of new data privacy concerns).

[169] More research must be done regarding the cost of implementing such measures. Using Google as a test case could help in deriving this information, although smaller companies may struggle to comply with the proposed regulation more than a massive corporation such as Google.

[170] Valentino-DeVries, *Tracking Phones*, *supra* note 8.

[171] *Id*.

[172] 5 U.S.C. § 552 (describing limits on information accessible to the public under the Freedom of Information Act (FOIA), including that information can be withheld if providing it would "constitute a clearly unwarranted invasion of personal privacy").

be leaked to the media,[173] collected by hackers,[174] or used by nefarious police officers[175] despite arguably having been collected without probable cause.

Law enforcement agencies will likely push back against regulations that require them to destroy location information.[176] They might argue that compiling large amounts of data across different agencies can help police officers better solve crimes as their departments' data analytics capabilities grow more powerful.[177] Indeed, law enforcement officials have successfully made similar arguments regarding DNA databases.[178] Though courts have been willing to consider privacy concerns in the DNA context, they have historically given great deference to the state's public interest in catching criminals.[179]

Unlike DNA databases, however, reverse location search warrants provide law enforcement agencies with location information about innocent citizens that officers can immediately use without needing to send anything to a lab. This information could include a person's name, workplace, or home address. Malicious police officers or any third party could more easily abuse location information in comparison to DNA evidence because they can use location information to easily identify an individual and find where they live. On the other hand, while DNA provides very sensitive information, it requires translation by scientists in order for a lay person to understand.

---

[173] Rafael Olmeda, *Sunrise Cop Charged with Leaking Secrets to the Press*, S. FLA. SUN SENTINEL (Sept. 18, 2020), https://www.sun-sentinel.com/local/broward/sunrise/fl-ne-roger-krege-charges-20200918-tfwrofwdprazrdjyomhnrc3gi4-story.html [https://perma.cc/9C5L-X3ZZ].

[174] Andy Greenberg, *Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents*, WIRED (June 22, 2020, 12:48 PM), https://www.wired.com/story/blueleaks-anonymous-law-enforcement-hack/ [https://perma.cc/MR56-WEBK].

[175] Sadie Gurman, *Across US, Police Officers Abuse Confidential Databases*, ASSOCIATED PRESS (Sept. 27, 2016), https://apnews.com/article/699236946e3140659fff8a2362e16f43 [https://perma.cc/9HUM-X444].

[176] For one example of police groups pushing back against technology regulations, see Melissa Hellman, *Tech, Police Groups Push Back Against Facial Recognition Bans*, GOV'T TECH. (Sept. 30, 2019), https://www.govtech.com/products/Tech-Police-Groups-Push-Back-Against-Facial-Recognition-Bans.html [https://perma.cc/MH8E-X62N].

[177] Emily Buder, *The Algorithm That Catches Serial Killers*, ATLANTIC (Nov. 28, 2017), https://www.theatlantic.com/video/index/546893/serial-killer-algorithm/ [https://perma.cc/UQH4-XFU7] (for one example of how police officers can use data troves to solve crimes).

[178] Kristen V. Brown, *No One Is Safeguarding Your DNA*, BLOOMBERG BUSINESSWEEK (Feb. 26, 2019, 5:00 AM), https://www.bloomberg.com/news/articles/2019-02-26/law-enforcement-can-do-whatever-it-likes-with-consumer-dna-data [https://perma.cc/7XDW-NGPN]; *see also* Maryland v. King, 569 U.S. 435, 436 (2013).

[179] *King*, 569 U.S. at 436 (stating that "great weight is given to both the significant government interest at stake in the identification of arrestees and DNA identification's unmatched potential to serve that interest").

Law enforcement officials might also argue that requiring the careful deletion of location information might be logistically difficult and expensive. For example, even after the case is officially closed, it may prove challenging for law enforcement agencies to draw the line between truly unnecessary information and slightly suspicious information that has potential relevance in case the investigation is reopened. Furthermore, it might be cost prohibitive for government officers to audit how often law enforcement officers are deleting extraneous information collected by reverse location search warrants. That being said, requiring police officers to delete unnecessary information collected by the first warrant in a reverse location search warrant would go a long way towards assuaging some of the fundamental privacy concerns citizens might have with the technology. Taken together, all three legislative measures proposed by this Comment would help combat the potential dangers to privacy presented by the widespread adoption of reverse location search warrants.

CONCLUSION

The reverse location search warrant is a powerful new technology capable of both making our lives safer and pushing us further towards all-pervasive government surveillance. As local police departments continue to adopt and refine this new tool and tech companies expand their capabilities for storing consumer location information, citizens' Fourth Amendment right to be free from searches without probable cause requires further protections. These protections could come at least in part from the courts, which have strained to adapt the probable cause framework to new technological developments. In lieu of judicial action, however, federal and state legislatures must create new laws to help judges better analyze whether warrants satisfy probable cause in order to protect innocent people from having their location information shared with police officers or even with the public at large.

The three laws proposed by this paper simply represent a starting point for protecting American citizens from reverse location search warrants. They would help assuage some of the practical and constitutional difficulties that these new warrants present. However, as more data is collected around the accuracy and effectiveness of reverse location search warrants, legislators will likely need to consider more specific laws and regulations in order to protect fundamental privacy concerns. These more technologically sophisticated solutions might include mandated support staff for police departments opting to use reverse location search warrants or proof of accuracy benchmarks before tech companies may provide police officers with location information in criminal cases. As a society, we seem to be

inching closer and closer towards a surveillance state. Still, reverse location search warrants are likely a necessary evil to help law enforcement officials keep in lockstep with tech-savvy criminals. Through the use of alternate legal frameworks, common-sense legislative protections, and careful approval of warrants, however, we can curtail the privacy impact of the reverse location search warrant.