WHY IT'S TIME TO BAN GEOFENCE SEARCHES IN LIGHT OF *UNITED STATES V. CHATRIE*

Danny Drane[†]

TABLE OF CONTENTS

DOI: https://doi.org/10.15779/Z38VM42Z6N

† J.D. Candidate, University of California, Berkeley, School of Law, Class of 2024. Thank you to Professor Talha Syed for his mentorship, as well as the stellar editors at the *Berkeley Technology Law Journal*.

I. INTRODUCTION

On December 13, 2018, Jorge Molina was arrested for a murder he did not commit.[1] At roughly 9 a.m., four police officers approached Molina at a Macy's department store and told him that they needed to speak with him.[2] The officers put Molina in handcuffs, drove him to the jailhouse, and interrogated him about a murder.[3] In shock, Molina pleaded, "I didn't shoot anybody. I'm not that type of person."[4] Yet the officers confidently retorted that they "knew, one hundred percent, without a doubt, that his phone was at the shooting scene."[5] As it turned out, that was wrong.

The officers were confident Molina's phone was at the scene because they had issued a standard "geofence search warrant" to Google. In the week prior, police obtained surveillance footage of a car following the victim on the night he was killed.[6] The officers then sent a geofence search warrant to Google, asking the company to identify "any wireless communication device that passed through the same geographical locations that the suspect vehicle did" on that night.[7] Google complied with the request, sending back a list of four Google accounts that were in that area at the time.[8] Then, when police asked for more details on each account, Google identified a device that was logged into Jorge Molina's Google account.[9] Rather than pursue leads that would have uncovered the real culprit, police pinned this evidence on Molina, costing him his job, car, and reputation.[10] Police were "blinded by data."[11]

Since Molina's wrongful arrest, police use of geofence search warrants has skyrocketed nationwide. In 2020, the most recent year for which data is available, law enforcement issued over 11,000 geofence search warrants to

1. Meg O'Connor, *Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder*, PHX. NEW TIMES (Jan. 16, 2020), https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374.

2. *Id.*

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. *Id.*

8. *Id.*

9. *Id.*

10. *See id.* Had police investigated further, it would have been "clear" that the culprit was Molina's stepfather. *Id.* Police learned that Molina owned the suspect vehicle, yet two months prior, police impounded the same car after Molina's stepfather was arrested for driving it without a license, which had occurred multiple times prior. *Id.* And if police had sought additional data on Molina's Google Account, they would have learned that Molina himself was in a different part of the city that night. *Id.*

11. *Id.*

Google—a 37% increase from 2019.[12] This trend concerns privacy advocates because a single geofence search can sweep up over a thousand people.[13] Consequently, legal scholarship has dissected whether and when geofence search warrants violate the Fourth Amendment's privacy protections.[14]

Troublingly, legal scholarship has largely ignored the on-the-ground impact of geofence searches on political speech. Although court records typically shield the details of search warrants, activists have discovered that police departments have used geofence searches to solve crimes committed at or near Black Lives Matter protests.[15] This pattern suggests police are using geofence search warrants to target individuals who are expressing viewpoints with which police do not agree. But so far, legal scholarship on geofence search warrants is largely grounded in discussions on privacy, with very limited mentions of speech.[16] This Note seeks to fill this gap in legal scholarship, in part because geofence search could become a potent tool against protestors. Protests have a high density of people concentrated in one area, and geofence searches offer police the unique ability to identify and track anyone present at a particular place, time, and location.

This Note proposes a simple legislative solution to the threats posed by geofence search warrants: a blanket ban on all geofence searches. Part II explains what geofence search warrants are, Google's protocols for processing them, and how they threaten privacy and speech. Part III contends that, absent

12. Zack Whittaker, *Google Says Geofence Warrants Make Up One-Quarter of All US Demands*, TECHCRUNCH (Aug. 19, 2021), https://techcrunch.com/2021/08/19/google-geofence-warrants/.

13. Thomas Brewster, *Google Hands Fed 1,500 Phone Locations in Unprecedented 'Geofence' Search*, FORBES (Dec. 11, 2019), https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search/?sh=3220433827dc.

14. *See, e.g.*, Haley Amster & Brett Diehl, *Against Geofences*, 74 STAN. L. REV. 385 (2022); Esteban De La Torre, *Digital Dragnets: How the Fourth Amendment Should Be Interpreted and Applied to Geofence Search Warrants*, 31 S. CAL. INTERDISC. L. J. 329 (2022); Cassandra Zietlow, *Reverse Location Search Warrants: Law Enforcement's Transition to 'Big Brother,'* 23 N.C. J.L. & TECH. 669 (2022); Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508 (2021).

15. *See, e.g.*, Russell Brandom, *How Police Laid Down a Geofence Dragnet for Kenosha Protestors*, VERGE (Aug. 30, 2021), https://www.theverge.com/22644965/kenosha-protests-geofence-warrants-atf-android-data-police-jacob-blake; Zach Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protesters*, TECHCRUNCH (Feb. 6, 2021), https://techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant/.

16. *See, e.g.*, Amster & Diehl, *supra* note 14, at 396 (mentioning protests in only one sentence throughout the article); De La Torre, *supra* note 14, at 330 n.7, 330 n.8, 351 n.185 (citing three articles that mention protests in headlines but not stating "protest" or "speech" anywhere in the article); Zietlow, *supra* note 14, at 670–72, 678, 690 (mentioning the use of geofence searches against protestors several times without mentioning or contextualizing the accompanying threat to political speech).

Congressional legislation, courts will interpret the Fourth Amendment in ways that encourage, rather than limit, geofence searches' harms. To do so, Part III dissects the third-party doctrine, the Fourth Amendment's weak remedies, and how a recent case, *United States v. Chatrie*, epitomizes these doctrinal failures. Finally, Part IV criticizes alternative proposals to rely on courts and legislative reforms to showcase why a blanket ban is the most desirable solution.

II. GEOFENCE SEARCHES THREATEN PRIVACY AND SPEECH

A. UNDERSTANDING GEOFENCE SEARCHES

A geofence is a virtual perimeter that maps out a real-world geographic area during a specific timeframe. Geofences use GPS technology to identify digital devices that enter or exit the geofence boundaries. Law enforcement agencies conduct geofence searches to retroactively locate mobile devices that entered or exited the geofence.[17] This entails submitting a geofence search warrant. Geofence search warrants are requests to a third-party company such as Google, for information on mobile devices that are associated with the accounts.[18] Before requesting this information, law enforcement applies for a search warrant and describes the searches' terms to a magistrate judge.[19]

Take, for instance, the geofence search warrant ruled unconstitutional in *United States v. Chatrie*.[20] In response to a bank robbery, police in *Chatrie* issued a geofence search warrant to Google, compelling Google to identify every device that was within 17.5 acres of a bank between 4:20 p.m. and 5:20 p.m. on the day it was robbed.[21] Put another way, police sought to identify every phone in an area equal to 3.5 blocks in New York City.[22]

Geofence search warrants are primarily issued to Google, which processes warrants through a three-step protocol.[23] Google's specialists use data from Location History (LH), an opt-in feature on Google products and services.[24] In the first step, a specialist searches the entirety of Google's LH database and provides law enforcement with the requested information in an anonymized

17. Mark Harris, *A Peek Inside the FBI's Unprecedented January 6 Geofence Dragnet*, WIRED (Nov. 28, 2022), https://www.wired.com/story/fbi-google-geofence-warrant-january-6/.
18. *Id.*
19. *See Geofence Warrants and the Fourth Amendment*, *supra* note 14, at 2509, 2514.
20. 590 F. Supp. 3d 901 (E.D. Va. 2022).
21. *Id.* at 919.
22. *Id.* at 918 n.26.
23. *Id.*
24. *Id.* at 908–09.

format.[25] This data includes the time-stamped coordinates of, and Google accounts associated with, every device located within the geofence.[26] This data is ostensibly anonymous. However, at this point in the three-step protocol, without further information from Google, an officer can "observe each account's reported location, track each account to his or her home, and pinpoint each account's personal identity using publicly available resources."[27] At step two, law enforcement reviews the list to identify devices they deem worth investigating and requests additional location data from Google.[28] During step three, Google provides information that identifies the users of these devices, including their full name, username, email addresses, birthdate, account type, account number, phone numbers, and the device's make and model.[29]

This three-step process is done at Google's and law enforcement's discretion, largely without the input of a judge.[30] Aside from approving the initial warrant, a neutral judge is not involved at any subsequent step of the process.[31] There is also no requirement that officers narrow their request in step two.[32] In fact, police often broaden the scope of their requests without seeking additional approval from a judge.[33] And, of course, Google is generally free to amend its three-step protocol at any point, which reduces the power of judges to limit geofence search warrants under the Fourth Amendment.[34]

B. GEOFENCE SEARCHES THREATEN PRIVACY

Google's Location History data is retroactive, precise, and comprehensive. The LH feature is automatically available on nearly every Android smartphone and on the Google Maps apps installed on any smartphone.[35] Considering 130 million Americans use an Android smartphone,[36] and one-third of active

25. *Id.* at 914–15.
26. *Id.* at 915–16.
27. *Id.* at 931 n.39.
28. *Id.* at 916–17.
29. *Id.* at 919 n.27.
30. *See Geofence Warrants and the Fourth Amendment*, *supra* note 14, at 2508, 2514–16.
31. *Id.*
32. *Chatrie*, 590 F. Supp. 3d at 923 (explaining that Google "typically require[s]" law enforcement to narrow the request but "has no firm policy as to precisely *when* a Step 2 request is sufficiently narrow").
33. *Geofence Warrants and the Fourth Amendment*, *supra* note 14, at 2514–16.
34. *See* Amster & Diehl, *supra* note 14, at 437–44.
35. *Chatrie*, 590 F. Supp. 3d at 920 (quoting a law enforcement affidavit describing Google's LH feature).
36. *Number of Android Smartphone Users in the United States from 2014 to 2022*, STATISTA, https://www.statista.com/statistics/232786/ (last visited Nov. 1, 2023).

Google users have the LH feature enabled,[37] a back-of-the-napkin estimate of solely Android users suggests Google's databases contain the minute-by-minute locations of, at the very least, 40 million Americans. Google can even pinpoint a phone's location to within three meters.[38] Thus, with any geofence search aimed at finding a suspect, police have a good chance of finding detailed information, to say the least.

Geofence searches typically have wide margins of error and expansive geographic parameters. Google estimates that the data it provides to law enforcement fall within a 68% confidence interval, meaning there is only a 68% chance that the identified devices were within the given location.[39] And in step two of Google's process, police often expand searches by requesting information on devices "outside the search parameters but within a 'margin of error.'"[40] This means not only do police routinely identify people outside the scene of the relevant crime, but the information learned is often inaccurate.

These wide parameters raise distinct privacy concerns in urban areas. Urban police departments are more capable of deploying geofences than their rural counterparts due to superior staffing and resources.[41] And urban police face more pressure to deploy geofences because urban areas also have higher rates of unsolved crimes—the exact situations where geofences are most valuable.[42]

The urbanization of geofence searches is troubling for two reasons. First, the high population density of cities increases the number of innocent people swept up in searches.[43] Second, people of color are concentrated in urban

37. *Chatrie*, 590 F. Supp. 3d at 909.

38. *Id.*; *see also In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 360 (N.D. Ill. 2020) ("One only needs to look at one's location in Google Maps to know that the location data is remarkably accurate.").

39. *Chatrie*, 590 F. Supp. 3d at 909. A confidence interval is a statistical measure that, in simple terms, shows the probability that a given number falls within a certain range.

40. *See, e.g.*, *In re* Search of: Information Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 745 (N.D. Ill. Aug. 24, 2020).

41. Lauren Weisner, H. Douglas Otto & Sharyn Adams, *Issues in Policing Rural Areas: A Review of the Literature*, ILL. CRIM. JUST. INFO. AUTHORITY (Mar. 18, 2020), https://icjia.illinois.gov/researchhub/articles/issues-in-policing-rural-areas-a-review-of-the-literature.

42. *See id.*; Maura Arnold, *Geofence Warrants: Useful Crime Solving Tool or Invasive Surveillance Tactic?*, J. HIGH TECH. L. BLOG. (Mar. 10, 2021), https://sites.suffolk.edu/jhtl/2021/03/10/geofence-warrants-useful-crime-solving-tool-or-invasive-surveillance-tactic/.

43. A. Reed McLeod, *Geofence Warrants: Geolocating the Fourth Amendment*, 30 WM. & MARY BILL RTS. J. 531, 557 (2021); *see also In re* Search of: Info. Stored at Premises Controlled by Google, No. 20 M 297, 2020 U.S. Dist. LEXIS 165185, at *1, *2 (N.D. Ill. July

areas.[44] There, racially disparate policing patterns are deeply rooted, well-documented, and typically reinforced when police acquire new tools and technology.[45] Given urban police departments are able and incentivized to use geofence searches, this tool will join a growing list of police technologies that perpetuate privacy invasions, structural racism, and mass incarceration.

C. GEOFENCE SEARCHES THREATEN POLITICAL SPEECH

Digital surveillance of protestors is not new. Since 2014, the FBI has used social media for long-term monitoring of Black Lives Matter activists.[46] Six federal agencies used facial recognition software to identify and criminally investigate people who protested the killing of George Floyd in 2020.[47] Customs and Border Patrol (CBP) used information collected from digital surveillance to curate dossiers of lawyers, activists, and journalists assisting migrants at the U.S.-Mexico border.[48] Federal, state, and local law enforcement agencies routinely share digital surveillance with each other through 80 federally funded "fusion centers."[49]

8, 2020) (highlighting that the requested geofence areas were within "a densely populated city" and captured individuals partaking in the "amenities associated with upscale urban living").

44. Kim Parker, Juliana Menasce Horowitz, Anna Brown, Richard Fry, D'Vera Cohn & Ruth Igielnik, *Demographic and Economic Trends in Urban, Suburban, and Rural Communities*, PEW RES. CTR. (May 22, 2018), https://www.pewresearch.org/social-trends/2018/05/22/demographic-and-economic-trends-in-urban-suburban-and-rural-communities/ (noting that 56% of the total population in urban counties are non-white).

45. *See, e.g.*, Michael Siegel, Rebecca Sherman, Cindy Li & Anita Knopov, *The Relationship Between Racial Residential Segregation and Black-White Disparities in Fatal Police Shootings at the City Level, 2013–2017*, 111 J. NAT'L MED. ASS'N. 580–87 (2019) (tracing racial disparities in policing and fatal shootings in cities to residential segregation); Will Douglas Heaven, *Predictive Policing Is Still Racist—Whatever Data It Uses*, MIT TECH. REV. (Feb. 5, 2021); https://www.technologyreview.com/2021/02/05/1017560/predictive-policing-racist-algorithmic-bias-data-crime-predpol/ (discussing the racial bias encoded in modern, data-driven predictive policing tools).

46. George Joseph & Murtaza Hussain, *FBI Tracked An Activist Involved With Black Lives Matter As They Traveled Across the U.S., Documents Show*, INTERCEPT (Mar. 19, 2018, 8:29 AM), https://theintercept.com/2018/03/19/black-lives-matter-fbi-surveillance/.

47. Radhamely De Leon, *Six Federal Agencies Used Facial Recognition on George Floyd Protestors*, VICE (June 30, 2021), https://www.vice.com/en/article/3aqpmj/six-federal-agencies-used-facial-recognition-on-george-floyd-protestors.

48. Tom Jones, Mari Payton & Bill Feather, *Source: Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates Through a Secret Database*, NBC SAN DIEGO (Jan. 10, 2020), https://www.nbcsandiego.com/news/local/source-leaked-documents-show-the-us-government-tracking-journalists-and-advocates-through-a-secret-database/3438/.

49. SARAH BRAYNE, PREDICT AND SURVEIL: DATA, DISCRETION, AND THE FUTURE OF POLICING 9 (2020); *see* Rachel Levinson-Waldman & Ángel Díaz, *How to Reform Police Monitoring*

Make no mistake: law enforcement uses digital surveillance to retaliate against protestors, even those who do not commit crimes at protests.[50] Immigration and Customs Enforcement (ICE), for instance, recently arrested and initiated deportation proceedings against several of its critics shortly after they participated in protests.[51] Sometimes police do not even wait for a protest to conclude. As Baltimore's protestors mourned the death of Freddie Gray in 2015, police, in their words, "stay[ed] one step ahead" by using "real-time, location-based social media monitoring" to identify protestors with outstanding warrants and "arrest them directly from the crowd."[52]

Police used geofence search warrants during Black Lives Matter protests in recent years. During protests over George Floyd's death at the hands of police, officers in Minneapolis asked Google to identify every device in an area with "dozens" of people to identify a person who broke the windows of an AutoZone store.[53] During protests in Kenosha, Wisconsin following the murder of Jacob Blake, federal agents issued six geofence search warrants that "stretch[ed] as long as two hours" and resembled a "dragnet[] spread over some of the [protests'] busiest times and locations."[54]

Geofence searches will have chilling effects on political expression, particularly when they complement other forms of digital surveillance. In 2019, the Manhattan District Attorney, for instance, combined facial recognition, social media monitoring, and a geofence search to try to identify "members" of Antifa for a separate prosecution of right-wing Proud Boys.[55] This prosecution is particularly telling. Antifa has no real "membership." It is an umbrella term that refers to small, loosely affiliated pockets of activists who are opposed to fascism.[56] Yet conservatives have warped "Antifa" into a catch-

of Social Media, BROOKINGS (July 9, 2020), https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.

50. Levinson-Waldman & Díaz, *supra* note 49.

51. Alice Speri & Maryam Saleh, *An Immigrant Journalist Faces Deportation as ICE Cracks Down on its Critics*, INTERCEPT (Nov. 28, 2018), https://theintercept.com/2018/11/28/ice-immigration-arrest-journalist-manuel-duran/.

52. AM. CIVIL LIBERTIES UNION N. CAL., CASE STUDY: BALTIMORE COUNTY PD (2016), http://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

53. Whittaker, *supra* note 15.

54. Brandom, *supra* note 15.

55. Colin Moynihan, *How Police Used Antifa to Investigate Far-Right Proud Boys*, N.Y. TIMES (Aug. 8, 2019), https://www.nytimes.com/2019/08/08/nyregion/proud-boys-antifa-trial.html.

56. Mark Bray, *Five Myths About Antifa*, WASH. POST (Sept. 11, 2020), https://www.washingtonpost.com/outlook/five-myths/five-myths-about-antifa/2020/09/11/527071ac-f37b-11ea-bc45-e5d48ab44b9f_story.html; Michael Kenney & Colin Clarke, *What Antifa Is, What it Isn't, and Why it Matters*, WAR ON ROCKS (June 23, 2020), https://warontherocks.com/2020/06/what-antifa-is-what-it-isnt-and-why-it-matters/.

all term for left-leaning protestors, and this prosecution showcases law enforcement's willingness to exploit this narrative to the detriment of Black Lives Matter protestors.[57] Thus, one lesson rings clear: law enforcement will use geofence searches to disrupt protests, leading people to self-censor and expend additional resources to engage in political activities. And given empirical research confirms that the mere perception of online surveillance is sufficient to stifle the expression of political views, chilling effects will occur even if people's fears of geofence-based surveillance are misplaced.[58]

Arguably, geofences pose greater risks than other forms of digital surveillance for two reasons. First, information revealed from a geofence search is more detailed than that of facial recognition and social media surveillance. After all, knowledge of a person's full name, usernames, birthdate, email address, and phone make and model is more likely to lead to arrests than, for example, a blurry photo put through facial recognition software.[59] Second, it is difficult to evade geofence surveillance. Through social media, for instance, police identify protestors largely because people voluntarily, and perhaps unwittingly, post photos and videos online. In response, activists have started warning protestors that "police can see your social media posts."[60] To evade surveillance and enable political speech, activists advise would-be protestors to communicate on encrypted platforms and refrain from posting another protestor's identifying information on social media.[61]

Whereas one can refrain from simply posting online, a protestor cannot as easily evade geofence-based location tracking. It would be counterproductive for a protestor to leave their phone at home because phones are invaluable for communication, coordination, and navigation to and from protests.[62]

57. *See* Tina Nguyen, *How 'Antifa' Became a Trump Catch-All*, POLITICO (June 2, 2020), https://www.politico.com/news/2020/06/02/how-antifa-became-a-trump-catch-all-297921.

58. *See* Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMM. Q. 296, 299–300 (2016).

59. *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. ON PRIVACY & TECH. (2019), https://www.law.georgetown.edu/privacy-technology-center/publications/garbage-in-garbage-out-face-recognition-on-flawed-data/ (noting that surveillance footage is often too low quality to identify suspects using facial recognition software).

60. *See* Corinne Purtill, *Before You Post That #Protest Selfie at the Inauguration Protests, Remember that Police Can See Your Social Media Posts*, QUARTZ (Jan. 20, 2017), https://qz.com/889696/before-you-post-that-protest-selfie-at-the-inauguration-protests-remember-that-police-can-see-your-social-media-posts/.

61. *See id.*

62. *See, e.g.*, Christina Neumayer & Gitte Stald, *The Mobile Phone in Street Protest: Texting, Tweeting, Tracking, and Tracing*, 2 MOBILE MEDIA & COMM. 117, 118 (2014) (highlighting that cell phones allow street protestors to coordinate in real time, to send short and functional text

Alternatively, disabling location features on one's phone is confusing, burdensome, and requires some degree of technical knowhow. As a Google employee once described the process of deleting one's location history, "[it feels] like it is designed to make things possible, yet difficult enough that people won't figure . . . [it] out."[63] Finally, buying a burner phone is cost-prohibitive, and its inconvenience is incompatible with the spontaneity of many protests.[64] As a result, protests are full of phones pinging their minute-by-minute locations to Google's vast database that police can access. As the Supreme Court recently put it, "a phone goes wherever its owner goes, conveying to the wireless carrier . . . a detailed chronicle of a person's physical presence."[65]

III. FOURTH AMENDMENT DOCTRINE ENCOURAGES TECH-SAVVY SURVEILLANCE

A. THE THIRD-PARTY DOCTRINE ENABLES MASS DIGITAL SURVEILLANCE

The Fourth Amendment protects people from "unreasonable searches" by requiring police obtain a warrant to search a person's "papers, houses, or effects."[66] A warrant is required only when the officer's conduct constitutes a "search," which occurs when police violate a person's "reasonable expectation of privacy"[67] or physically trespass on a person's property.[68]

---

messages, and to document the actions of protestors and police); Allison Gordon, *Black Lives Matter Makes its Mark on Map Apps*, CNN (June 10, 2020), https://www.cnn.com/2020/06/10/tech/map-protests-trnd/index.html (highlighting the value of Snapchat in broadcasting and finding protests).

63. *Chatrie*, 590 F. Supp. 3d at 913 (quoting an Associated Press article that described the user interface as of August 13, 2018). The interfaces of Google's location products can be so convoluted that they confuse Google's own software engineers. Okello Chatrie's lawyers introduced evidence of emails from Google employees expressing confusion about Google's various location products. *Id.* at 914 n.17.

64. *See* Neumayer & Stald, *supra* note 62, at 118 ("The immediacy, mobility, and constant access afforded by mobile phones make them especially useful in ad hoc demonstrations.").

65. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

66. U.S. CONST. amend. IV.

67. *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (explaining that a reasonable expectation of privacy requires both a subjective expectation of privacy, and that the expectation is one that society is prepared to recognize as reasonable).

68. United States v. Jones, 565 U.S. 400, 407 (2012) (establishing that either the reasonable expectation of privacy test or a physical intrusion onto a persons' constitutionally protected area is sufficient to constitute a search within the meaning of the Fourth Amendment).

Technology has shaped the Fourth Amendment's privacy protections. *Kyllo v. United States*, for instance, held that police need a warrant to use thermal imaging devices that compile images of the inside of a person's home based on the home's distribution of heat.[69] Writing for the majority, Justice Scalia reasoned that, although police do not physically enter a person's home, the use of thermal imaging devices risks inadvertently revealing "intimate" information that traditionally could only be revealed by entering the home.[70]

The third-party doctrine, however, has significantly undermined these protections. Under the third-party doctrine, police do not need a warrant to obtain information voluntarily given to a third party.[71] A person forfeits their expectation of privacy because they "assume[] the risk" that the information will be disclosed to police.[72] Since the person has no privacy expectation in disclosed information, an officer who obtains the information is not conducting a "search" for Fourth Amendment purposes and thus does not need a warrant. As such, the Supreme Court has held that police do not need a warrant to obtain a person's bank records,[73] or even the phone numbers of incoming and outgoing calls.[74] Effectively, the Fourth Amendment fails to protect Americans' digital information because virtually all digital information is shared with or stored by a third party.

The sole case where the Supreme Court declined to apply the third-party doctrine to digital information is *Carpenter v. United States*. There, police took advantage of the fact that cell phones send a signal to the nearest cell tower several times every minute.[75] Police obtained two sets of cell tower records without warrants: one retroactively traced the defendant's location over the course of 127 days, the other traced his location over two days.[76] The majority stressed that there was a significant privacy interest in "a person's physical presence compiled every day, every moment, over several years."[77]

69. 533 U.S. 27, 40 (2001).

70. *Id.* at 38 ("The [device] might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate'; and a much more sophisticated system might detect nothing more intimate than the fact that someone left a closet light on . . . . [And] no police officer would be able to know *in advance* whether his through-the-wall surveillance picks up 'intimate' details—and thus would be unable to know in advance whether it is constitutional.").

71. Smith v. Maryland, 442 U.S. 735, 744 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

72. *Smith*, 442 U.S. at 745.

73. *Miller*, 425 U.S. at 443.

74. *Smith*, 442 U.S. at 744.

75. *Carpenter*, 138 S. Ct. at 2211.

76. *Id.* at 2212.

77. *Id.* at 2220.

Additionally, since a phone shares its location "without any affirmative act" by the user, the person does not "*voluntarily* assume[] the risk" of disclosing their location "in [a] meaningful sense" for the purposes of the third-party doctrine.[78] Thus, the warrantless search of location information was unconstitutional.

In spite of *Carpenter*, however, lower courts still apply the third-party doctrine in countless scenarios where police collect intimate digital information about people. For instance, multiple circuit courts have held that police do not need a warrant to obtain basic subscriber information that customers must provide to use mobile applications, websites, and services like Google and Facebook.[79] This "basic" information usually includes IP addresses,[80] which are the identities of networks and devices on the internet, as well as a user's first and last name, home address, email address, profile pictures, birthdate, location information, and device information.[81]

Under the logic of the third-party doctrine, a frightening amount of digital information is provided "voluntarily" and thus does not necessitate a warrant to search. Consider a universal experience: someone visits a website or downloads an app, then agrees to a privacy policy or a pop-up notice with the word "cookies." Cookies are data that websites track, like a person's web browsing history or online shopping carts.[82] When a user agrees to or even ignores these terms, he or she consents to the website selling the user's information to third parties, which are usually advertisers and data brokers that make profiles of your online activity.[83] Users agree to these terms 95–99% of the time, even when given an option to opt-out that is explicitly titled "Do Not

78. *Id.* (quoting *Smith*, 442 U.S. at 745) (emphasis added).

79. *See, e.g.*, United States v. Rosenow, 33 F.4th 529, 548 (9th Cir. 2022); United States v. Ulbricht, 858 F.3d 71, 97 (2d Cir. 2017); United States v. Caira, 833 F.3d 803, 806 (7th Cir. 2016).

80. *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

81. LIZ WOOLERY, RYAN BUDISH & KEVIN BANKSTON, THE TRANSPARENCY REPORTING TOOLKIT: SURVEY & BEST PRACTICE MEMOS FOR REPORTING ON U.S. GOVERNMENT REQUESTS FOR USER INFORMATION, THE BERKMAN CTR. FOR INTERNET & SOC'Y AT HARV. UNIV. (Mar. 2016), https://cyber.harvard.edu/sites/cyber.harvard.edu/files/Final_Transparency.pdf. The messaging app Kik has a FAQ website for law enforcement that includes this information in its definition of "basic subscriber information." *See Kik FAQ*, LAW ENFORCEMENT HELP CTR., https://medialablawenforcementhelp.zendesk.com/hc/en-us/articles/4404983340187-What-s-included-in-Basic-Subscriber-Information- (last visited Nov. 1, 2023).

82. Jon Healey, *What Are Those Annoying Website Popups About Cookies? And What Should You Do About Them?*, L.A. TIMES (Sept. 1, 2021), https://www.latimes.com/business/technology/story/2021-09-01/what-are-website-cookies-how-do-they-impact-internet-data.

83. *Id.*

Sell My Personal Information."[84] In one experiment, 74% of people agreed to a website's privacy policy without reading it, and 93% agreed to a condition to give up their first-born child.[85]

This habit of doling out digital information has gifted police with endless opportunities for warrantless digital surveillance. Police are free to commercially purchase troves of data from online advertisers, and do not need a warrant or subpoena.[86] Thanks to this "constitutional loophole," law enforcement can simply "us[e] its checkbook to get around *Carpenter*."[87] Though advertisers' data is anonymized, its precision makes it easy to identify people.[88] For example, when given access to one digital advertising dataset, New York Times staffers were "quickly able to match more than 2,000 supposedly anonymous devices . . . with email addresses, birthdays, ethnicities, ages, and more."[89] It is no exaggeration to say the third-party doctrine "threatens to nullify the Fourth Amendment."[90]

B. FOURTH AMENDMENT REMEDIES ARE POOR DETERRENTS

1. The Exclusionary Rule

The primary remedy for Fourth Amendment violations is the Exclusionary Rule: evidence uncovered from an unconstitutional search cannot be admitted

84. INTERACTIVE ADVERTISING BUREAU, IAB CCPA BENCHMARK SURVEY SUMMARY 6 (Nov. 12, 2020), https://www.iab.com/insights/iab-ccpa-benchmark-survey/ (finding that opt-out rates were only 1–5%). This study examined, among other things, the rate at which website users opted out of websites selling third-party cookies after the passage of the California Consumer Privacy Act (CCPA). CAL. CIV. CODE §§ 1798.100–1798.198 (2018). The CCPA requires websites that sell data to provide a "clear and conspicuous link on the business's internet homepages, titled 'Do Not Sell or Share My Personal Information,' to an internet web page that enables a consumer . . . to opt out of the sale of the consumer's personal information." CAL. CIV. CODE § 1798.135(a)(1).

85. Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO., COMM., & SOC'Y 128 (2020).

86. Tim O'Brien, Suspicionless Search: Geofence Warrants and the Fourth Amendment 28 (Feb. 13, 2023) (unpublished manuscript), https://ssrn.com/abstract=3834623.

87. *See* Charles Levinson, *Through Apps, Not Warrants, 'Locate X' Allows Federal Law Enforcement to Track Phones*, PROTOCOL (Mar. 5, 2020), https://www.protocol.com/government-buying-location-data; Isabelle Canaan, *A Fourth Amendment Loophole?: An Exploration of Privacy and Protection through the Muslim Pro Case*, 6 HUM. RTS. L. REV. 95, 104 (2021).

88. Canaan, *supra* note 87, at 104.

89. Charlie Warzel & Stuart A. Thompson, *They Stormed the Capitol. Their Apps Tracked Them*, N.Y. TIMES (Feb. 5, 2021), https://www.nytimes.com/2021/02/05/opinion/capitol-attack-cellphone-data.html.

90. Gabriel Broshteyn, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1931 (2017).

against the defendant.[91] To those who believe that an effective remedy should make a person whole, excluding evidence hardly ameliorates the harms of pretrial detention, including disruptions in wages and employment,[92] housing stability,[93] familial relationships,[94] and mental[95] and physical health.[96] The Supreme Court has openly acknowledged the Exclusionary Rule's inability to

91. Weeks v. United States, 232 U.S. 383, 393 (1914).

92. *See* Will Dobbie & Crystal Yang, *The Economic Costs of Pretrial Detention*, BROOKINGS PAPERS ON ECON. ACTIVITY, Spring 2021, at 251, 260, https://www.brookings.edu/wp-content/uploads/2021/03/15872-BPEA-SP21_WEB_DobbieYang.pdf ("Even a short period of pretrial detention can be destabilizing . . . resulting in immediate job loss . . . ."). On average, pretrial detention reduces a person's earnings by $948 per year over the 3–4 years following detention. *Id.* at 13.

93. *See* GINA CLAYTON, ENDRIA RICHARDSON, LILY MANDLIN & BRITTANY FARR, ESSIE JUSTICE GRP., BECAUSE SHE'S POWERFUL: THE POLITICAL ISOLATION AND RESISTANCE OF WOMEN WITH INCARCERATED LOVED ONES 62 (2018), https://www.becauseshespowerful.org/wp-content/uploads/2018/05/Essie-Justice-Group_Because-Shes-Powerful-Report.pdf ("[Fifty percent] of women who have owed money to a bail bonds agency faced housing insecurity as a result.").

94. *See* Sara Wakefield & Lars Højsgaard Andersen, *Pretrial Detention and the Costs of System Overreach for Employment and Family Life*, 7 SOCIO. SCI. 342 (2020) (finding that people detained pretrial but not convicted have a statistically higher risk of no longer living with their partner or child after release); *see also* CREASIE FINNEY HAIRSTON, ANNIE E. CASEY FOUND., KINSHIP CARE WHEN PARENTS ARE INCARCERATED: WHAT WE KNOW, WHAT WE CAN DO. A REVIEW OF THE RESEARCH AND RECOMMENDATIONS FOR ACTION (2009), https://eric.ed.gov/?id=ED507722 (documenting how incarcerated mothers seek care for their children by relying on their children's grandparents, extended family, and foster care).

95. *See, e.g.*, JENNIFER BRONSON, JESSICA STROOP, STEPHANIE ZIMMER & MARCUS BERZOFSKY, U.S. DEP'T OF JUSTICE, DRUG USE, DEPENDENCE, AND ABUSE AMONG STATE PRISONERS AND JAIL INMATES, 2007-2009, at 3 (2017), https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5966 (finding that two-thirds of jail inmate have a substance use disorder); Andrew P. Wilper, Steffie Woolhandler, J. Wesley Boyd, Karen E. Lasser, Danny McCormick, David H. Bor, & David U. Himmelstein, *The Health and Health Care of US Prisoners: Results of a Nationwide Survey*, 99 AM. J. PUB. HEALTH 666 (2009) (finding that half of all inmates who have previously been treated for a psychiatric condition receive no medical treatment while in jail).

96. *See, e.g.*, Amy Katzen, *African American Men's Health and Incarceration: Access to Care upon Reentry and Eliminating Invisible Punishments*, 26 BERKELEY J. GENDER, L. & JUST. 221, 228 (2011) (noting that poor ventilation and overcrowding in jails cause higher rates of tuberculosis); Shabbar I. Ranapurwala, Meghan E. Shanahan, Apostolos A. Alexandridis, Scott K. Proescholdbell, Rebecca B. Naumann, Daniel Edwards, Jr., & Stephen W. Marshall, *Opioid Overdose Mortality Among Former North Carolina Inmates: 2000–2015*, 108 AM. J. PUB. HEALTH 1207, 1208 (2018) (attributing an increase in mortality rates not to higher incarceration rates among substance users, but to the fact that one's tolerance for drugs decreases while behind bars, thereby increasing the risk of overdose upon release).

compensate for harms, having characterized the rule as simply a "deterrent" against violations of the Fourth Amendment.[97]

Yet the Court has carved out numerous exceptions that swallow the Exclusionary Rule's deterrent effect. For instance, evidence can only be excluded if the defendant proves that the officer intentionally or recklessly violated the Fourth Amendment.[98] Even if a defendant overcomes that hurdle, prosecutors can still use unlawfully gained evidence to impeach any witness, including the defendant,[99] against a different defendant whose Fourth Amendment rights were not violated,[100] and when the officer had a "good-faith" reason for not knowing that their search was illegal.[101] The inevitable discovery doctrine, too, is a "colossal loophole" that allows police to use illegally gained evidence if other practices would have otherwise yielded the evidence.[102] Additionally, unconstitutional searches typically yield topics for further investigation, including physical evidence and witness identifications. Under yet another exception, prosecutors can admit anything police learn from follow-up actions to an unconstitutional search so long as intervening circumstances render the evidence gained to be sufficiently "attenuated" from the initial constitutional violation.[103]

---

97. *See, e.g.*, United States v. Leon, 468 U.S. 897, 906 (1984) (quoting Stone v. Powell, 428 U.S. 465, 540 (White, J., dissenting)).

98. Herring v. United States, 555 U.S. 135, 144 (2009).

99. United States v. Havens, 446 U.S. 620, 628 (1980).

100. Rakas v. Illinois, 439 U.S. 128, 130 (1978).

101. *Leon*, 468 U.S. at 906–08.

102. Nix v. Williams, 467 U.S. 431, 432, 444 (1984) (announcing the inevitable discovery doctrine); *see generally* Tonja Jacobi & Elliot Louthen, *The Corrosive Effect of Inevitable Discovery on the Fourth Amendment*, 171 U. PA. L. REV. 1, 2 (2022) (charting the application of the inevitable discovery doctrine and arguing that tests adopted by many lower courts have devolved into a more relaxed standard than the one set out by the Supreme Court in *Nix v. Williams*).

103. Initially intended to allow for the admission of evidence gained as a result of unforeseeable intervening circumstances, the attenuation doctrine is a three-part test announced in *Brown v. Illinois*. 422 U.S. 590 (1975). To determine whether the admitted evidence is sufficiently attenuation from the officer's unconstitutional conduct, courts analyze the 1) temporal proximity between the officer's actions and the seizure of the evidence, 2) whether there are intervening circumstances, and 3) the flagrancy of the officer's conduct. *Id.* at 603–605. The Supreme Court vastly expanded the application of this test in *Utah v. Strieff*, concluding that evidence obtained by police during an unlawful stop is not subject to the exclusionary rule if the police discover that the person stopped has a warrant out for their arrest. 136 S. Ct. 2056, 2059–63 (2016). The majority reasoned that the discovery of this warrant, though merely minutes after the stop began, was sufficiently attenuated from the unlawful stop. *Id.* For a discussion of this flawed holding's likely impacts on the Fourth Amendment and officer misconduct, see Matthew E. Sweet, *Stretching the Attenuation Doctrine to Its Limits: How the Supreme Court Erred in* Utah v. Strieff *and What Can Be Done to Preserve the Doctrine*, 25 GEO. MASON. L. REV. 861, 871–880 (2018).

To illustrate how these broad, categorical exceptions have made the Exclusionary Rule "Swiss cheese,"[104] consider a hypothetical. Police illegally raid a person's home without a warrant and find nothing except a box of drugs owned by the homeowner's friend. Although the homeowner's Fourth Amendment rights were violated, this box is admissible evidence in a criminal prosecution against the friend because his home was not raided.[105] Let's add to this hypothetical. A label on the box contains the friend's phone number, so police find an unconstitutional way to intercept his outgoing texts that say, "I am currently at a large meeting of drug dealers." Police then contact each drug dealer at this meeting, and each dealer snitches on each other. At his trial, the friend testifies that he was not at this meeting, so the prosecutor reads these texts out loud for impeachment purposes.[106] In reality, the jury just heard a smoking gun confession disguised as an impeachment.[107] And in subsequent prosecutions, every drug dealer is out of luck because their confessions were "attenuated" from these Fourth Amendment violations. As this hypothetical showcases, "[w]hat ultimately matters to defendants is not where their constitutional rights begin and end, but rather the more pragmatic question of whether or not evidence is actually admitted."[108]

Thus, for the Court to call the Exclusionary Rule a "deterrent" ignores the obvious. For a deterrent to work, it must impose sufficient costs on bad actors. To borrow from economics literature on deterrence, an officer will violate a person's Fourth Amendment rights "if the expected benefits to the police officer exceed the expected costs."[109] The expected benefit to an officer would be a criminal conviction, or merely pretrial detention itself, which would allow police to confiscate contraband, interrogate the suspect, and perhaps temporarily prevent a crime.[110] An officer weighs these benefits against the

104. Christopher Slobogin, *Why Liberals Should Chuck the Exclusionary Rule*, 1999 U. ILL. L. REV. 363, 375.

105. *See* Rakas v. Illinois, 439 U.S. 128, 130 (1978).

106. *See generally* United States v. Havens, 446 U.S. 620, 628 (1980).

107. The exclusionary rule's exception for impeachment evidence has been rightfully criticized for its prejudicial impact on criminal defendants and the fact that it deters defendants from testifying at trial. *See, e.g.*, Richard D. Friedman, *Minimizing the Jury Over-Valuation Concern*, 2003 MICH. ST. L. REV. 967, 981 ("It is unlikely that jurors use [impeachment evidence] to assess the credibility of the accused . . . . Inevitably though, they are tempted to use the evidence for a purpose for which they are *not* supposed to consider it—in this case, determining that the accused is a bad person. This means that the impeachment evidence has a serious biasing effect—and because of that, the threat of such evidence often intimidates a defendant from exercising his fundamental right to testify in his own defense . . . .")

108. Jacobi & Louthen, *supra* note 102, at 1–2.

109. Michael Cicchini, *An Economics Perspective on the Exclusionary Rule and Deterrence*, 75 MO. L. REV. 459, 469 (2010).

110. *Id.*

probability that the Exclusionary Rule frees the criminal suspect.[111] Unfortunately, this probability is "near zero" given the frequency with which police lie at hearings, the pressure defendants face during plea negotiations, and the Exclusionary Rule's many exceptions.[112]

The Exclusionary Rule also imposes zero personal costs on officers. Deterrence generally requires that the targeted person perceive a sufficiently high probability and severity of punishment.[113] In economics terms, effective punishments cause officers to "internalize the harm" that they cause which incentivizes them to refrain from future misconduct.[114] Merely excluding evidence, however, does not affect officers personally because the outcomes of evidentiary hearings only affect defendants, and defendants lose 99% of the time.[115] In fact, court surveys of police demonstrate that officers twist the facts at evidentiary hearings so often that police coined a term for it: "testilying."[116] When officers "so widely, willingly, and cavalierly lie[] to courts about their Fourth Amendment actions," the Supreme Court is wrong to suggest that the Exclusionary Rule sufficiently deters officers from violating the Fourth Amendment.[117]

2. Civil Suits

There is also little deterrent value in lawsuits brought under 42 U.S.C. § 1983, which authorizes civil suits against state government officials who violate a person's constitutional rights.[118] To prevail and earn money damages

111. *See id.* at 470–81 (theorizing that the expected costs are the probability of evidence suppression, the cost of a lost conviction, and secondary sanctions against the officer such as "civil lawsuits, job-related sanctions, and public condemnation.").

112. *See id.* at 470–71 (quoting commentary on the Mollen Report, a survey of New York City police officers that documented a common practice of testifying untruthfully during suppression hearings); Jamie Fellner, *An Offer You Can't Refuse: How U.S. Federal Prosecutors Force Drug Defendants to Plead Guilty*, 26 FED. SENT'G REP. 276, 277–80 (2013) (discussing the effects of mandatory minimum sentencing provisions on plea negotiations of criminal defendants facing federal drug charges).

113. *Cf.* Nuno Garoupa, *The Theory of Optimal Law Enforcement*, 11 J. ECON. SURVEYS 267, 268 (1997) (referencing Gary Becker's seminal papers on the deterrence theory of criminal punishment); *see also* Cicchini, *supra* note 109, at 470–81 (theorizing that officers may face "secondary sanctions" such as job-related sanctions, civil lawsuits, and public condemnation).

114. Robert Cooter, *Three Effects of Social Norms on Law: Expression, Deterrence, and Internalization*, 79 OR. L. REV. 1, 16 (2000).

115. *See* Albert Alschuler, *Studying the Exclusionary Rule: An Empirical Classic*, 75 U. CHI. L. REV. 1365, 1375 (2008) (citing empirical studies finding that courts exclude evidence in, at most, 1.3 percent of criminal cases).

116. *Id.* at 1376–77.

117. David Harris, *How Accountability-Based Policing Can Reinforce–or Replace–the Fourth Amendment Exclusionary Rule*, 7 OHIO ST. J. CRIM. L. 149, 162, 162 n.53 (2009).

118. 42 U.S.C. § 1983.

under § 1983, plaintiffs must overcome the affirmative defense of qualified immunity.[119] This requires that the officer violated a "clearly established" right of which "every reasonable officer" under the circumstances would be aware.[120]

Rather than interpret constitutional rights at a high level of generality, courts distinguish the facts of qualified immunity cases at a granular level, leaving very few rights "clearly established" in the eyes of individual police officers.[121] In an article describing the extreme degree to which courts distinguish facts to favor police, Professor Mark Brown highlighted troubling precedent from the Eleventh Circuit: "[f]or qualified immunity to be surrendered, pre-existing law must dictate, that is, truly compel (not just suggest or allow to raise a question about), the conclusion for every like-situated, reasonable government agent that what [they are] doing violates federal law in the circumstances."[122] Indeed, "*minor* variations in some facts" including "an *arguably significant* fact . . . might be very important" from the perspective of an officer and therefore make a right not "clearly established."[123]

This tendency to overly distinguish cases is particularly harmful in Fourth Amendment doctrine, which entails highly fact-specific tests.[124] The Supreme Court requires parsing existing law "with [such] a high degree of specificity" that a search's constitutionality under the Fourth Amendment is "beyond debate."[125] Although technologies like geofence searches are too new to have many cases surrounding their use in general, qualified immunity is only overcome with "controlling authority" or "a robust consensus of cases of persuasive authority" that directly bear on the facts of a particular search.[126]

---

119. Harlow v. Fitzgerald, 457 U.S. 800, 815 (1982).

120. Ashcroft v. al-Kidd, 563 U.S. 731, 741 (2011) (internal citations omitted). *Al-Kidd* heightened the standard of qualified immunity to emphasize what "every" reasonable officer would know, as opposed to *Harlow*'s original phrasing: "a reasonable officer." 457 U.S. at 815.

121. John C. Jeffries Jr., *What's Wrong with Qualified Immunity*, 62 FLA. L. REV. 851, 854–65 (2010).

122. Mark R. Brown, *The Fall and Rise of Qualified Immunity: From Hope to Harris*, 9 NEV. L.J. 185, 198 (2008) (quoting Rowe v. City of Ford Lauderdale, 279 F.3d 1271, 1280 (11th Cir. 2002) (emphasis omitted)).

123. *Id.* at 198–99 (quoting Marsh v. Butler Cty., 268 F.3d 1014, 1032 (11th Cir. 2001) (emphasis added)).

124. Jeffries, *supra* note 121, at 859–60. The primary test for evaluating whether the Fourth Amendment has been violated is "totality of the circumstances." Illinois v. Gates, 462 U.S. 213, 230 (1983); Lange v. California, 141 S. Ct. 2011, 2018 (2021) (applying the totality of the circumstances test through the officer's perspective to evaluate whether the "exigent circumstances" exception to the warrant requirement applied).

125. District of Columbia v. Wesby, 138 S. Ct. 577, 589 (2018).

126. *Id.* at 589–90 (quoting Wilson v. Layne, 526 U.S. 603, 617 (1999)); *see also Chatrie*, 590 F. Supp. 3d at 936 (holding that a police officer conducted an unconstitutional geofence search

And ultimately, even if an innocent criminal suspect somehow overcomes qualified immunity, money damages are hard to square with the one-time violation of privacy from an unconstitutional search. One Justice Department study found that, out of 12,000 lawsuits against federal officers for alleged constitutional violations, plaintiffs were paid damages in only five cases.[127] It was unknown whether any of those cases involved Fourth Amendment searches.[128] The study attributed this, in part, to the fact that illegal searches generally "do[] not cause the kind of actual damages that our tort system compensates."[129] All of this is to say, the low prospect of money damages provides virtually no deterrent for police use of novel technology because qualified immunity offers police tremendous freedom to experiment with our Fourth Amendment rights.

Injunctive relief, the other § 1983 remedy to stop or deter unconstitutional police practices, is difficult to pursue due to *City of Los Angeles v. Lyons*.[130] In *Lyons*, the Supreme Court held that, when seeking injunctive relief, a plaintiff's case is moot[131] unless they demonstrate that they are likely to be injured *again*

---

in good-faith belief of its constitutionality given "rapidly advancing technology" and the lack of "judicial guidance" on employing geofences).

127. *See* Donald Dripps, *Beyond the Warren Court and Its Conservative Critics: Toward a Unified Theory of Constitutional Criminal Procedure*, 23 U. MICH. J.L. REFORM 591, 629 (1990) (internal citation omitted).

128. *Id.*

129. *Id.*; *see also* Sherry F. Colb, *Innocence, Privacy, and Targeting in Fourth Amendment Jurisprudence*, 96 COLUM. L. REV. 1456, 1521 n.173 (1996) ("Damages may be minimal in the ordinary case because there is little injury to a person or to property."). Another convincing explanation is that juries are unwilling to award damages to suspected criminals. *See* Tracey Maclin, *When the Cure for the Fourth Amendment is Worse than the Disease*, 68 S. CAL. L. REV. 1, 31 (1994) ("If the majority of the public is willing to sacrifice the Fourth Amendment to stop illegal drug use, why should anyone believe that jurors in civil damages cases will protect the Fourth Amendment rights of guilty drug couriers?").

130. 461 U.S. 95 (1983).

131. For background on mootness, federal courts may only hear cases that are "ripe," as opposed to "moot." That is, the injury must actively persist at the time of litigation such that resolution of the case would affect the plaintiff's rights. *See, e.g.*, DeFunis v. Odegaard, 416 U.S. 312, 316–19 (1974) (describing the Court's mootness doctrine, then explaining that the plaintiff, a law school applicant seeking an injunction to be admitted into a law school, had a moot case because they were ultimately admitted into the school after the litigation commenced). The relevant exception to mootness in *Lyons* was that federal courts will hear a moot case when the injury is capable of repetition, yet evading review. The "classic" example of this exception is that courts will hear cases where the injury is related to pregnancy. *See* Roe v. Wade, 410 U.S. 113, 125 (1973). To require a litigant be pregnant throughout a lawsuit would be unrealistic because litigation can be a lengthy endeavor. Thus, to dismiss pregnancy-related injuries as moot would allow defendants to repeatedly evade identical lawsuits solely due to the temporary nature of injuries they cause. Hence, courts created the "capable of repetition, yet evading review" exception to mootness doctrine.

by the practice alleged to be unconstitutional.[132] Thus, Lyons was unable to challenge the L.A. Police Department's use of chokeholds on Fourth Amendment grounds because he failed to show that he specifically would be choked again by L.A. police.[133] In the context of a novel technology, how could a person credibly predict that in the near future they will be captured in, say, a geofence search?[134] And given this new search method has largely evaded judicial scrutiny, how could courts craft injunctions to accommodate the Fourth Amendment's many exceptions? After all, the court would need to "answer a seemingly limitless set of hypothetical situations addressing a seemingly limitless set of possible exceptions[.]"[135]

Altogether, the Fourth Amendment's weak remedies provide overly broad discretion to police over people's privacy.[136] With new technology, privacy infringements are becoming even cheaper and more convenient. If the Fourth Amendment exists only as a subject on which police experiment, then our privacy protections "might as well be stricken from the Constitution."[137]

C. CHATRIE EPITOMIZES THE FOURTH AMENDMENT'S FAILURES

1. The Geofence Search Warrant in Chatrie

The story of Okello Chatrie's arrest and conviction in the Eastern District of Virginia is as follows. After a bank robbery in May of 2019, police in Midlothian, Virginia issued a geofence search warrant to Google, seeking to identify every cell phone within 17.5 acres of the bank between 4:20 p.m. and 5:20 p.m. on the day it was robbed.[138] The geofence initially had a diameter of 300 meters, which was "longer than three football fields" and included the bank, a church, and a nearby wooded area.[139]

In his application for the search warrant, the officer told a magistrate judge what information he planned to request from Google. In sum, this is what the

132. 461 U.S. at 110.

133. *Id.* at 111–12.

134. *See, e.g.*, Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) (holding that a plaintiff failed to establish an injury-in-fact for standing purposes by means of a probabilistic theory that the National Security Agency's foreign surveillance program was reasonably likely to intercept the plaintiff's communications).

135. Orin Kerr, *The Limits of Fourth Amendment Injunctions*, 7 J. ON TELECOMM. & HIGH TECH. L. 127, 134–35 (2009) (charting, by means of example, the inherent difficulties in crafting an injunction against a warrantless search of a home).

136. Slobogin, *supra* note 104, at 364.

137. Weeks v. United States, 232 U.S. 383, 393 (1914) (announcing the exclusionary rule, then characterizing it as a means of deterring unconstitutional conduct, thereby securing Fourth Amendment protections).

138. *Chatrie*, 590 F. Supp. 3d at 914–15.

139. *Id.* at 922–23.

officer said would occur during his search: at step one of Google's process, the officer planned to ask for anonymized information on devices within the geofence;[140] then, at step two, law enforcement promised to "attempt[] to narrow" this list and request additional "contextual data points" that illustrate each person's travel,[141] where these data points would expand the geofence's radius to 387 meters—"more than twice as large as the original geofence"—and add thirty minutes to the beginning and to the end of the initial timeframe;[142] and finally, at step three, Google would provide account-identifying information.[143]

The magistrate judge reviewed this information for, at most, fifteen-to-thirty minutes.[144] He had completed his magistrate training program only three months prior and did not have a law degree, which is allowed under Virginia law.[145] Predictably, the magistrate judge signed off on this search warrant's "sweeping and powerfully intrusive" terms.[146]

Then, the officer contradicted the terms approved by the magistrate judge as he executed the geofence search. In step one, the officer requested anonymized information on 19 individuals detected within the geofence.[147] In step two, however, the officer "did not 'attempt to narrow down'" his request despite making that exact promise to the magistrate judge days before.[148] Rather, "in contravention to Google's policy, and without consulting [the judge]," the officer repeatedly asked Google for the full names, usernames, email addresses, and other identifying information on all 19 people.[149] Not only that, the also officer doubled the geofence's time and location parameters in these subsequent requests without narrowing the initial list of suspects.[150] It was only after Google's specialist personally called the officer did the latter finally narrow his request.[151]

2. Chatrie is Not the Answer

On a motion to suppress evidence, the district court held that the geofence search warrant was invalid for two reasons, but nevertheless denied the

140. *Id.* at 919–20.
141. *Id.* at 919.
142. *Id.* at 922–23.
143. *Id.* at 919.
144. *Id.* at 939.
145. *Id.* (citing VA. CODE §§ 19.2-37).
146. *Id.*
147. *Id.* at 920.
148. *Id.* at 921.
149. *Id.*
150. *Id.*
151. *Id.* at 922–23.

motion. First, the third-party doctrine did not apply because the government could not point out when Chatrie enabled the feature that disclosed his location.[152] This, coupled with Google's confusing interfaces, showcased the government's failure to prove that Chatrie voluntarily shared his location to a third party.[153] Because the third-party doctrine did not apply under these facts, police needed a warrant to conduct the geofence search that identified Chatrie. Hence, the court proceeded to its second line of reasoning: the warrant was not "sufficiently particular" in outlining probable cause for the individuals to be searched or the information sought.[154]

First, the third-party doctrine did not apply. The district court held multiple evidentiary hearings on Google's various products and services. These hearings revealed that, at the time the geofence search was conducted in summer 2018, Google's interfaces made it difficult for users to learn the extent of Google's location tracking, let alone delete their location history data.[155] Due to the "messiness of the current record as to when Chatrie 'gave consent'" for a third party to track his location, the trial court did not find that Chatrie voluntarily forfeited his expectation of privacy under the third-party doctrine.[156]

Then, in what appears to be dicta, the district court cited *Carpenter* to argue that, more broadly, the third-party doctrine does not apply to geofences searches and thus a warrant is required. Prosecutors urged the opposite, distinguishing the two rationales given in *Carpenter* regarding cell-site location information. They argued that the geofence captured "just two hours" of Chatrie's location, which raises a smaller privacy interest than the days' worth of information revealed in *Carpenter*.[157] Second, they argued that a geofence search can only track those who enable Google's Location History feature, which is a voluntary, "affirmative step" to disclosing one's location, unlike the automatic pings to cell towers in *Carpenter*.[158]

The district court rejected the prosecutors' arguments by citing powerful language in *Carpenter*. First, the court stated that Chatrie did have a privacy interest in "just two hours" of location data because, "perhaps even more so than" the information in *Carpenter*, Chatrie's location was "detailed,

152. *Id.* at 935.
153. *Id.* at 935–36.
154. *Id.* at 927–33.
155. *See id.* at 913, 914 n.17 (quoting Google employees and engineers who called the process of deleting one's location history confusing).
156. *Id.* at 935.
157. *Id.*
158. *See id.* at 935–36.

encyclopedic, and effortlessly compiled."[159] Second, the trial court concluded that Chatrie did not voluntarily provide his location because Google provided users with "limited and partially hidden warnings" regarding the frequency and precision of its location tracking.[160] Consequently, whatever "affirmative steps" Chatrie took in enabling the Location History feature would not "constitute a full assumption of the attendant risk of permanently disclosing one's whereabouts during almost every minute of every hour of every day."[161] Indeed, "a user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting 'YES, I'M IN' at midnight while setting up [an app]."[162]

The *Chatrie* district court's reasoning, though persuasive, will not broadly question the application of the third-party doctrine to geofence search warrants challenged in future cases. The court's criticism rested primarily on the government's failure to prove consent under these particular facts, which hinged on Google's inaccessible interfaces. But both of these hurdles are fixable in future prosecutions. The court repeatedly noted that Google's interfaces were confusing and incomplete as of summer 2018.[163] Yet in the months following the search in *Chatrie*, Google introduced several "controls that made it easier for users to manage their data."[164] And today, Google automatically deletes location data after 18 months, gives the option of automatically deleting data every three months, and offers a "Privacy Checkup tool" that allows users to see and control all information that Google collects.[165] With Google's since-updated privacy policies, in the future

159. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2216).

160. *Id.* at 936 ("In the Google Assistant set-up process, the device likely provided Chatrie a single pop-up screen informing him that '[t]his data may be saved and used in any Google service where [he was] signed in to give [him] more personalized experiences,' and that he 'can see [his] data, delete it and change [his] settings at account.google.com.' . . . However, the consent flow did not detail, for example, how frequently Google would record Chatrie's location (every two to six minutes); the amount of data Location History collects (essentially *all* location information); that even if he 'stopped' location tracking it was only 'paused,' meaning Google retained in its Sensorvault all his past movements; or, how precise Location History can be (*i.e.*, down to twenty or so meters).").

161. *Id.*

162. *Id.*

163. *See id.* at 911, 914 n.17, 936.

164. *Id.* at 913–14.

165. Jessica Bursztynsky, *Google Just Announced It Will Automatically Delete Your Location History by Default*, CNBC (June 24, 2020), https://www.cnbc.com/2020/06/24/google-will-automatically-delete-location-history-by-default.html; Todd Haselton, *Google Collects Information About Many Things You Do Online—Here's How to Stop It*, CNBC (May 1, 2019), https://www.cnbc.com/2019/05/01/how-to-stop-google-from-collecting-your-private-information.html.

prosecutors can more credibly argue defendants "assume the risk" of disclosing their whereabouts to police. It bears repeating that if a court concludes that the third-party doctrine applies, whatever search law enforcement conducted is not a search within the meaning of the Fourth Amendment and no warrant is required.

The *Chatrie* court's conclusion that geofence search warrants lack sufficient particularity likewise cannot be used to broadly question future geofence searches. Search warrants must have probable cause, a "fair probability" that the search will reveal evidence of a crime based on the "totality of the circumstances."[166] The court in *Chatrie* emphasized that the requirement of particularity in warrants limits the officers' discretion while they conduct searches. To limit infringements on privacy to only what is necessary for law enforcement, "discretion must be confined to the signing magistrate, not to the executing officers or a third party."[167] Thus, the geofence search warrant in *Chatrie* was invalid because steps two and three of Google's protocol did not require police to narrow the list of identified devices. Accordingly, the warrant failed to meet the particularity requirement because it did not provide the officer with "clear standards from which he or she could reasonably . . . ascertain and identify . . . the place to be searched [or] the items to be seized."[168]

Crucially, the court in *Chatrie* emphasized that it was not ruling that all geofence search warrants would lack particularity. The court referenced a case from the Northern District of Illinois that upheld a search warrant with six geofences that contained smaller timeframes and locations where few bystanders were present.[169] The court then suggested it would be constitutional for police to begin with an initial search for anonymized information, then broaden the search over the course of several successive approvals from magistrate judges.[170] Yet in the same breath, the court acknowledged that

166. *Gates*, 462 U.S. at 233, 238.

167. *Chatrie*, 590 F. Supp. 3d at 935 (citing United States v. Chadwick, 433 U.S. 1, 9 (1977)).

168. *Id.* (quoting *In re* Search of: Information Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 754 (2020)); United States v. Blakeney, 949 F.3d 851, 861 (2022)).

169. *Id.* (citing *In re* Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 361–62 (N.D. Ill. 2020)). In this case, six interrelated geofences covered areas related to two strings of suspected arsons. The geofences pinged devices present at multiple timeframes near multiple commercial and residential parking lots and roadways that connect these locations, then conducted searches of the same areas months later. 497 F. Supp. 3d at 351–53.

170. *See Chatrie*, 590 F. Supp. 3d at 933 ("In certain situations, then, law enforcement likely *could* develop initial probable cause to acquire from Google *only* anonymous data from devices within a narrowly circumscribed geofence at Step 1 . . . . From there, officers likely could use

anonymized data can reveal shocking amounts of intimate information.[171] Thus, if the alternative approach laid out in *Chatrie* were adopted, police would not need to obtain additional judge approval to conduct follow-up searches because all the information they need—and much more—would already be at their fingertips.

In its final illustration of the Fourth Amendment's limited ability to restrict geofence search warrants, the court in *Chatrie* still admitted evidence gathered from the unconstitutional search. Unlawfully gained evidence can be admitted when an officer conducted the search in "good faith."[172] In *Chatrie*, the court reasoned that the officer had a good-faith belief that the geofence search warrant was constitutional, in part, because of "rapidly advancing technology and lack of judicial guidance on this novel investigatory technique."[173] Another way to prove an officer's good faith is to show that they "reasonably" relied on the fact that a magistrate judge approved the search warrant, even when the approval itself was a "sweeping and powerfully intrusive" constitutional error.[174] Because the officer in *Chatrie* "reasonably" relied on the fact that magistrates had previously approved three similarly broad geofence search warrants, the court held that the officer acted in good faith.[175]

Chatrie leaves unanswered an important question: why is it "reasonable" or in "good faith" for an officer to not follow protocol? Okello Chatrie spent time behind bars because this officer "reasonably" believed it was legal to use Google's inadequate protocol on three prior occasions. The Fourth Amendment did not allow the court in *Chatrie* to question the good faith of an officer who "inexplicably" told the judge he had already found nineteen suspects before he even spoke with Google.[176] Perhaps the officer did not narrow his "sweeping and powerfully intrusive" request because he knew, as

---

that narrow, anonymous information to develop probable cause particularized to specific users. Importantly, officers likely could then present that particularized information to a magistrate or magistrate judge to acquire successively broader and more invasive information.").

171. *See id.* at 931 n.39 ("The fact that data points obtained during Steps 1 and 2 are anonymized when Google reports them does not completely quell this Court's concerns about the invasiveness of this warrant. Even 'anonymized' location data—from innocent people—can reveal astonishing glimpses into individuals' private lives when the Government collects data across even a one or two hour period.").

172. *Leon*, 468 U.S. at 923.

173. *Chatrie*, 590 F. Supp. 3d at 936.

174. *Id.* at 939; *Leon*, 468 U.S. at 922–23.

175. *Chatrie*, 590 F. Supp. 3d at 937–38.

176. *Id.* at 920.

Chatrie showcases, that the judiciary fails to hold police accountable when they violate an individual's Fourth Amendment rights.[177]

Rather than provide a cause for celebration, *Chatrie* epitomizes the Fourth Amendment's failure to deter and remedy infringements of privacy and free speech when police use novel technology. Thus, privacy and speech advocates should not rely on courts to restrict geofence searches.

IV. THE IMPORTANCE OF A BLANKET BAN

A. WHY THE CONSTITUTION CANNOT REGULATE GEOFENCE SEARCHES

Existing literature on geofences primarily discusses the constitutionality of geofence searches. Just as the court in *Chatrie* did, many articles argue or assume that geofence searches require a warrant because of the holding in *Carpenter* that people have a privacy interest in their location data and because geofences often capture information on people in their homes.[178] But courts likely will not adopt a "bright-line rule" that warrantless geofence searches are unconstitutional.[179] That is because, as *Chatrie* and other cases exhibit, the constitutionality of any search warrant turns on its degree of particularity and the "totality of the circumstances."[180] And every hole in our "Swiss cheese" Fourth Amendment weakens the promise of that already deprived test.

In fact, there are at least five justices on the Supreme Court who could rule that geofence searches categorically do not require a warrant. Justices Alito and Thomas are obvious candidates. Both justices dissented in *Carpenter*, that Carpenter had no privacy interest in any amount of location data—even data with "GPS-level precision"—because customers have no property rights over cell phone records.[181] A third candidate is Justice Gorsuch, who separately dissented in *Carpenter* on originalist, property-based grounds, under which one scholar has argued geofence searches would not require a warrant.[182] Fourth, Chief Justice Roberts, who authored *Carpenter*, could plausibly distinguish the

177. *See id.* at 921.

178. *See* De La Torre, *supra* note 14, at 329–30.

179. *See id.*

180. *Id.*; *Gates*, 462 U.S. at 230; *Chatrie*, 590 F. Supp. 3d at 927; *In re* Search of: Information Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 740–41 (2020).

181. *Carpenter*, 138 S. Ct. at 2224.

182. *See id.* at 2261–72 (Gorsuch, J., dissenting); Reed Sawyers, *For Geofences: An Originalist Approach to the Fourth Amendment*, 29 GEO. MASON L. REV. 787, 796–809 (2021) (appraising Justice Gorsuch's originalist framework and, in part, analogizing geofence search warrants to compelled subpoenas from early American history).

privacy interest and voluntariness of geofence search data from that of cell towers like the prosecutors in *Chatrie* did.

Either Justice Kavanaugh or Justice Barrett could be a fifth vote. Although Justices Kavanaugh and Barrett have not yet ruled on a Fourth Amendment case, neither one is a reliable vote for privacy. Professor Orin Kerr pegged Kavanaugh's likely Fourth Amendment jurisprudence as "somewhere in the ballpark" of Justice Kennedy, who wrote the primary *Carpenter* dissent, or Chief Justice Rehnquist, who voted to weaken the Fourth Amendment dozens of times.[183] Neither hypothesis is promising if the Supreme Court hears a geofence challenge. On the D.C. Circuit, then-Judge Kavanaugh wrote that the National Security Agency's bulk collection of metadata was "entirely consistent with the Fourth Amendment"—a position that has troubled digital privacy advocates.[184] On the Seventh Circuit, then-Judge Barrett twice ruled to exclude evidence, but neither case involved the search of a cell phone.[185] In her sole case that involved digital privacy interests, she ruled to admit evidence obtained from a warrantless border search of a traveler's cell phone.[186] Again, this holding is not promising if the Court decides to hear a challenge to geofence searches, particularly when Justice Barrett is a self-avowed originalist like Justices Gorsuch and Thomas.

Even when geofence searches require a warrant, this requirement itself does not adequately protect speech. Setting aside the numerous relevant exceptions to the warrant requirement,[187] the Fourth Amendment is not

183. Orin Kerr, *Judge Kavanaugh on the Fourth Amendment*, SCOTUSBLOG (July 20, 2018), https://www.scotusblog.com/2018/07/judge-kavanaugh-on-the-fourth-amendment/ (analyzing five of Justice Kavanaugh's rulings on the D.C. Circuit Court of Appeals); Craig M. Bradley, *Rehnquist's Fourth Amendment: Be Reasonable*, 82 MISS. L.J. 259, 260, 268 (2013) (noting that in over thirty years on the bench, there was only one non-unanimous Fourth Amendment case where Chief Justice Rehnquist voted for the defendant).

184. Klayman v. Obama, 805 F.3d 1148, 1148–49 (D.C. Cir. 2015) (Kavanaugh J., concurring). One expert wrote that Kavanaugh's opinion foreshadowed his "unwillingness to consider how technological changes have affected rights afforded by the Fourth Amendment." Susan Landau, *Brett Kavanaugh's Failure to Acknowledge the Changes in Communications Technology: The Implications for Privacy*, LAWFARE (Aug. 3, 2018), https://www.lawfareblog.com/brett-kavanaughs-failure-acknowledge-changes-communications-technology-implications-privacy.

185. *Amy Coney Barrett and Privacy*, ELECTRONIC PRIVACY INFO. CTR., https://archive.epic.org/privacy/barrett/ (last visited Nov. 8, 2023) (dissecting then-Judge Barrett's opinions on the Seventh Circuit).

186. *Id.*

187. One exception is when the facts facing the officer present "exigent circumstances." *See, e.g.*, Brigham City v. Stuart, 547 U.S. 398, 400–01 (2006) (holding that the safety of an occupant inside a home creates exigent circumstances, then finding this safety threatened when police overheard a fist fight inside a person's home); Kentucky v. King, 563 U.S. 452, 470 (2011) (holding that it does not violate the Fourth Amendment for police to deliberately create exigent circumstances).

equipped to address speech concerns. The Supreme Court effectively ruled as much when it held that police may raid a newsroom as long as there is a fair probability that that doing so will reveal evidence of a crime.[188] The fact that raiding a newsroom would have harmed the free flow of information, a core tenet of the First Amendment, did not change the Court's analysis because the warrant requirement's raison d'être is to limit invasions of privacy, not speech.[189]

Frankly, merely requiring a warrant is not a panacea for privacy concerns, either. The heart of the Fourth Amendment's warrant requirement is the notion that police simply need to ask permission before they violate your privacy or enter your home. Thus, if a cop and a judge suspect you have committed a crime, you no longer have an expectation of privacy over your personal information when that information is relevant to a crime. If one's priority is effective law enforcement, that makes sense. But the scope of criminal law has become so broad that it extends to the act of protesting itself,[190] activities that occur near or during protests,[191] and even people who attend protests with outstanding arrest warrants.[192] So long as our overly broad criminal law remains the filter through which the Fourth Amendment's warrant requirement operates, courts will allow geofence searches to the detriment of people, privacy, and speech.

That is, unless Congress acts. If courts will not offer meaningful, much-needed restrictions on geofence searches in the coming years, then privacy advocates must seek a different avenue. Legislative action is thus necessary.

B. WHY PROPOSED LEGISLATION WILL NOT PROTECT SPEECH AND PRIVACY

Generally, legislative proposals argue that geofence search warrants should have greater detail than a typical search warrant. For instance, one scholar

188. Zurcher v. Stanford Daily, 436 U.S. 547, 553 (1978).

189. *See generally id.*

190. *See, e.g.*, *US Protest Law Tracker*, INT'L CTR. FOR NOT-FOR-PROFIT L., https://www.icnl.org/usprotestlawtracker/ (last visited Nov. 8, 2023) (documenting the 18 states that have criminalized protests against oil and gas infrastructure since 2017); Kaylana Mueller-Hsia, *Anti-Protest Laws Threaten Indigenous and Climate Movements*, BRENNAN CTR. FOR JUST. (Mar. 17, 2021), https://www.brennancenter.org/our-work/analysis-opinion/anti-protest-laws-threaten-indigenous-and-climate-movements ("The combination of overly broad language and steep penalties in critical infrastructure laws make it likely that future activists and supporting organizations will be discouraged from exercising their First Amendment-protected protest rights.").

191. *See, e.g.*, Whittaker, *supra* note 12; Brandom, *supra* note 15.

192. *See* AM. CIVIL LIBERTIES UNION N. CAL., *supra* note 52 (noting that police used real-time social media monitoring to identify protesters and "directly" arrest them from the crowd).

proposes that all geofence search warrants should have a printed map that illustrates the geofence's parameters.[193] This scholar contends that this would educate magistrate judges on privacy concerns before they approve warrants.[194]

This proposal touches on, yet does not fully grasp the implications of, a wealth of evidence that magistrate judges are weak checks against police. One landmark study revealed that judges, on average, takes less than three minutes to review and approve a warrant.[195] It is common for police to go "shopping" for magistrates who tend to favor police.[196] Highly technical information in search warrants is systematically reduced to boilerplate explanations and surface-level descriptions like "cellular phone analysis."[197] Yet as police request tens of thousands of geofence search warrants per year, continuing education programs for magistrate judges did not have a single class with the word "geofence" in 2021.[198] Worse, as *Chatrie* showcased, magistrate judges do not need a law degree to authorize geofence search warrants.[199] To the extent that magistrates understand the Fourth Amendment, police deference is practically hardwired into its doctrine. All of this, coupled with informational asymmetries between police and magistrates, causes the latter to routinely defer to the former.[200]

In the face of these enormous structural problems, it is improbable to think that reforms like the inclusion of a printed map in a geofence search warrant application would sway a magistrate judge. Consider the photo below in Figure 1, which was contained in the geofence search warrant application in *Chatrie*.[201] To put it mildly, nothing about the photo illustrates the privacy and speech interests at play because the photo is blurry, black and white, and wholly non-descriptive as to what the captured buildings are and who may be inside them.

193. Mohit Rathi, *Rethinking Reverse Location Search Warrants*, 111 J. CRIM. L. & CRIMINOLOGY 805, 832 (2021).

194. *Id.* at 832–33.

195. RICHARD VAN DUIZEND, L. PAUL SUTTON & CHARLOTTE A. CARTER-YAMAUCHI, THE SEARCH WARRANT PROCESS: PRECONCEPTIONS, PERCEPTIONS, AND PRACTICES 31(1985).

196. *Id.* at 23–26.

197. *Id.*; O'Brien, *supra* note 86, at 24.

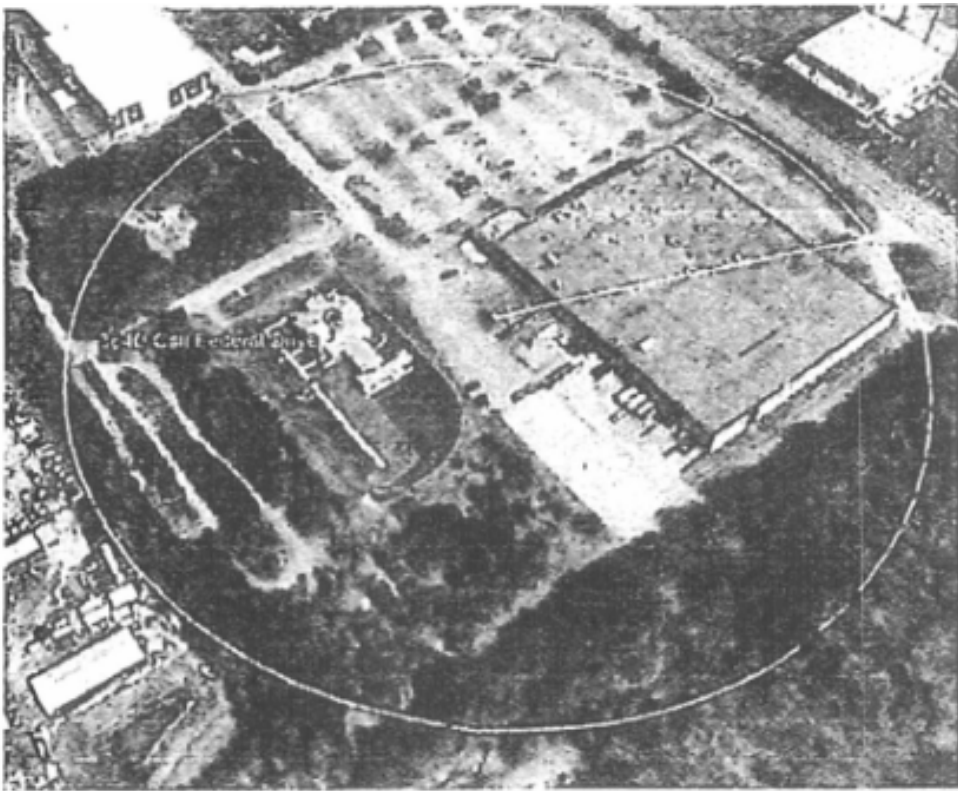
198. O'Brien, *supra* note 86, at 24–25.

199. *Chatrie*, 590 F. Supp. 3d at 939.

200. *See generally* O'Brien, *supra* note 86.

201. *Chatrie*, 590 F. Supp. 3d at 919.

Figure 1. The Parameters of *Chatrie*'s Geofence Search[202]



Another set of legislative reforms calls on Congress to regulate Google's process for evaluating warrants. Among these proposals is the requirement that Google provide step-one information in a de-identified format.[203] Echoing the *Chatrie* court's suggestion, another idea proposes that law enforcement must seek further judge approval after some—or all—steps in Google's protocol.[204] And police must narrow requests at step two or three of Google's protocol, rather than give police discretion over this decision.[205]

But legislation that focuses solely on the process of seeking search warrants will be ineffective. Recall what the court in *Chatrie* concluded: using Google's anonymous data, police could "observe each account's reported location, track each account to his or her home, and pinpoint each account's personal identity

202. *Id.*
203. Rathi, *supra* note 193, at 833.
204. *Chatrie*, 590 F. Supp. 3d at 933.
205. Rathi, *supra* note 193, at 834–35.

using publicly available resources."[206] These resources include the Data Broker Loophole.[207] Using anonymized data, one can identify the names, addresses, consumption habits, ethnicities, and ages of hundreds of people.[208] When Americans have exposed so much of their private lives in the digital era, simply tinkering with the warrant-seeking process will not protect privacy. The mere existence of geofence searches weaponizes our ubiquitous internet footprints.

A similar category of legislative proposals are restrictions on the circumstances under which geofence searches can be sought. One scholar suggested they only be approved in "exigent circumstances."[209] Under this proposal, Congress would require police to demonstrate geofence searches are "a last resort."[210] Judges would engage in an explicit balancing inquiry, approving warrants only when "the public safety threat would significantly outweigh the privacy [risks]."[211]

There are two primary problems with this proposal. First, as a practical matter, police could easily manipulate the statutory language. Second, exceptions will do little to quell the perception of surveillance, which inhibits speech.

First, case law shows just how easily police and courts would manipulate the language in the proposed restriction. Consider the phrase "public safety threat." In a criminal procedure ruling, the Supreme Court referred to a suspect who was disarmed, already in handcuffs, and in an empty supermarket in the middle of the night as a "threat to the public safety" that "outweigh[ed]" his Fifth Amendment rights.[212] In an evidence case, a drug-deal shooting that occurred twenty-five minutes prior with no follow-up activity was an "ongoing emergency."[213] The Court also interprets phrases "last resort" and "exigent circumstances" broadly. In Fourth Amendment cases, the term "exigent circumstances" describes situations where there is "no time to secure a

206. *Chatrie*, 590 F. Supp. 3d at 931 n.39.

207. *See id.* (quoting an American Bar Association report that discussed the power of anonymized data); *supra* Section III.A.

208. Warzel & Thompson, *supra* note 89.

209. Cassandra Zietlow, *Reverse Location Search Warrants: Law Enforcement's Transition to 'Big Brother,'* 23 N.C. J.L. & TECH. 669, 698 (2022).

210. *Id.* at 697.

211. *Id.* at 700.

212. New York v. Quarles, 467 U.S. 649, 651–52, 58 (1984).

213. Michigan v. Bryant; 562 U.S. 344, 351–52 (2011); *see also Quarles*, 467 U.S. at 879–85 (Scalia, J., dissenting).

warrant,"[214] which lower courts construed to include testing a person's urine[215] and smelling marijuana then hearing people moving inside an apartment.[216] With this in mind, legislators must ask whether they can trust courts and police to interpret even strongly worded limitations in a way that protects people, privacy, and speech.

Second, carving out piecemeal exceptions for geofence searches cannot ameliorate the harms to political speech. Empirical evidence shows that disruptions in political speech flow from the mere perception of surveillance.[217] In response to perceived surveillance, people self-censor, expend additional resources to organize political activities, and refrain from protests.[218] A proposal that does not ban all geofence searches will prove ineffective because the public will continue to correctly perceive that police can exploit the law's vagueness to use geofence searches as a surveillance tactic.

C. WHY A BLANKET BAN IS THE ANSWER

A blanket ban is the most effective way to address the impending harm of geofence searches. Regulated or not, geofence searches will inevitably lead to harassment of peaceful activists, intrusions on privacy, and unwarranted incarceration. The best avenue would be an act of Congress because federal legislation affects not just state and local police, but federal officers as well. Preventing federal officers from using geofence search warrants is crucial because the vast reach and resources of federal agencies like ICE make them uniquely able to maintain the worst harms of our surveillance state.[219]

In September 2021, New York introduced legislation to ban geofence searches. Congress should follow suit. Under Assembly Bill A84A, "no court shall issue a reverse location court order" and "no government entity shall seek, from any court, a reverse location court order."[220] "Reverse location court order" is the bill's term for a court-issued geofence search warrant.[221] If

214. *See, e.g.*, *Lange*, 141 S. Ct. at 2018; Missouri v. McNeely, 133 S. Ct. 1552, 1559 (2013); Michigan v. Tyler, 436 U.S. 499, 509 (1978).

215. State v. Hanson; 588 N.W.2d 885, 889 (S.D. 1999); *see also* Emily J. Sovell, State v. Hanson*: Has the Exigent Circumstances Exception to the Warrant Requirement Swallowed the Rule?*, 45 S.D. L. REV. 163, 179–185 (2000) (criticizing the *Hanson* decision).

216. Kentucky v. King, 563 U.S. 452, 470 (2011).

217. *See generally* Stoycheff, *supra* note 58, at 299–300.

218. *Id.*

219. *See* Speri & Saleh, *supra* note 51.

220. Assemb. B. A84A, 2021–2022 Leg., Reg. Sess. §§ 695.10, 695.20(2) (N.Y. 2021).

221. *Id.* § 695.00(3) ("'Reverse location court order' means any court order, including a search warrant, compelling the disclosure of records or information pertaining to electronic devices or their users or owners, whose scope extends to an unknown number of electronic devices present in a given geographic area at a given time as measured via global positioning

the bill is passed, criminal defendants may make a motion to exclude evidence gained from geofence searches.[222] To ensure deterrence and compliance with the law, the bill authorizes civil suits by "any individual whose records were obtained by any government entity" in violation of its terms.[223] Google, Microsoft, and Yahoo all support the bill.[224]

A common counterargument to a blanket ban is one that reifies our carceral state: banning geofence searches is "too extreme" because it would hurt law enforcement.[225] Yet the value that geofence searches add is, at best, indeterminate. Recent statistics suggest 11,000 geofence search warrants were executed in 2020.[226] There is no data on how many convictions these 11,000 searches led to, or even a breakdown of the crimes that were investigated.[227] It is also unclear how often geofences prove necessary; police have plenty of other cheap, effective, and less racially disparate investigative tools at their disposal.[228]

And broadly speaking, whatever benefit of solving crimes occurs is linked to over-policing and mass incarceration, largely against Black and Brown communities.[229] This has immense human and social costs.[230] Not only is

---

system coordinates, cell tower connectivity, Wi-Fi data, and/or any other form of location detention.").

222. *Id.* § 695.30.

223. *Id.* § 695.40.

224. Zack Whittaker, *Google, Microsoft, and Yahoo Back New York Ban on Controversial Search Warrants*, TECHCRUNCH (May 10, 2022), https://techcrunch.com/2022/05/10/google-new-york-geofence-keyword-warrant/; Matthew Guariglia, *Geofence Warrants and Reverse Keyword Warrants are So Invasive, Even Big Tech Wants to Ban Them*, ELECTRONIC FRONTIER FOUND. (May 13, 2022), https://www.eff.org/deeplinks/2022/05/geofence-warrants-and-reverse-keyword-warrants-are-so-invasive-even-big-tech-wants.

225. Zietlow, *supra* note 14, at 695; *cf.* A. Spencer Davies, *A Californian Algorithm: Amendment Assembly Bill 2261 to Regulate Law Enforcement's Use of Facial Recognition Technology in Post Hoc Criminal Investigations*, 26 BERKELEY J. CRIM. L. 27, 68 (2021) (noting this argument against a ban on law enforcement's use of facial recognition technology).

226. Whittaker, *supra* note 12.

227. *See id.*

228. *See* Nadine Deslauriers-Varin & Francis Fortin, *Improving Efficiency and Understanding of Criminal Investigations: Toward an Evidence-Based Approach*, 36 J. OF POLICE & CRIM. PSYCH. 635, 635 (2021) ("In recent years, we are, however, witnessing a growth of empirical studies that aim at providing support to police forces and specialized investigation units, and improving the efficiency of their practices using a proactive and evidence-based approach. This [is] particularly true for sexual crimes and homicides[.]"); *see also generally id.* at 636 (previewing a special issue of the *Journal of Police and Criminal Psychology* that contains 11 articles related to "innovative" investigative techniques, processes, and decision-making strategies).

229. *See supra* Section II.B (discussing how the urbanization of geofence searches will disproportionately affect racial minorities).

230. *See, e.g.*, Michael McLaughlin, Carrie Pettus-Davis, Derek Brown, Chris Veeh & Tanya Reen, *The Economic Burden of Incarceration in the United States* 4–5, (Inst. for Justice Research

incarceration's human toll important in its own right, but it is counterproductive because it aggravates the root causes of crime, thereby creating a revolving door of release, recidivism, and reincarceration.[231] For every person that a geofence search puts behind bars, there is a family and a community made less whole.

The premise of a blanket ban is that a small number of crimes may go unsolved if doing so safeguards people, privacy, and speech consistent with the values enshrined in the Constitution and Bill of Rights. Although this argument is not fully reflected in Fourth Amendment doctrine, Congress can and should enact a law with this principle in mind.

V. CONCLUSION

Geofence searches pose tremendous privacy and speech risks that neither Fourth Amendment nor legislative reforms will meaningfully mitigate. And *United States v. Chatrie*, despite its celebrated reasoning, showcased the failures of the Fourth Amendment to deal with these pending risks. Accordingly, Congress must enact a blanket ban on their use.

The harms of geofence searches are similar, and will add to, those of other forms of digital surveillance. The failures of the third-party doctrine and the Fourth Amendment's remedies to address these types of surveillance should give us pause as well. Going forward, legislators should consider whether the arguments fleshed out above justify blanket prohibitions on police use of commercial data, social media surveillance, facial recognition technology, and so much more. Without further action by Congress, the First and Fourth Amendments' promises will remain just that, promises.

& Development, Working Paper No. IJRD-072016, 2016) (finding that the aggregate economic impact of incarceration is $1 trillion in losses to income, health, and other measures); *see also supra* notes 92–96 and accompanying text (documenting, in great detail, the individual harms of pretrial detention, including disruptions in "wages and employment, housing stability, familial relationships, and mental and physical health").

231. Criminology literature offers several theories for why incarceration may reduce crime, including deterrence of crime and incapacitating people from committing crimes. For a thorough critique of this literature on theoretical, methodological, and empirical grounds, see David Roodman, The Impacts of Incarceration on Crime (July 9, 2020) (unpublished manuscript), https://ssrn.com/abstract=3635864; *see* Alexi Jones, *Reforms Without Results: Why States Should Stop Excluding Violent Offenses From Criminal Justice Reforms*, PRISON POL'Y INITIATIVE (Apr. 2020), https://www.prisonpolicy.org/reports/violence.html (summarizing Roodman's findings aptly: "incarceration can be counterproductive: While a prison sentence can incapacitate people in the short term, it actually increases the risk that someone will commit a crime after their release.").