# Big Data Searches and the Future of Criminal Procedure

Mary D. Fan*

*The vast volumes of our consumer data that companies retain to target advertising, train artificial intelligence products, and predict our preferences can also help solve crimes and identify unknown perpetrators. Two powerful strategies for cracking cases involving unknown perpetrators, keyword warrants and geofence warrants, direct businesses to disclose devices that performed incriminating keyword searches or that were present during a crime. The new digital search strategies drawing on corporately held big data are sparking conflicts and confusion in the courts because a suspect is not named, spurring originalism-influenced analogies to 1700s-era general warrants. Evaluating digital searches through the lens of a time before electric power existed—much less electronic data—makes no sense but remains alluring because of Romantic Luddism, a tradition of anxiety over technological change and nostalgia for the past. Advancing beyond Romantic Luddism in Fourth Amendment interpretation, this Article offers a new analytical lens for big data search strategies that are evolving with technology.*

*How crimes are perpetrated in the digital age has evolved. Our concept of the Fourth Amendment's requirements, including what constitutes probable cause and particularity in big data search warrants, must evolve as well. This Article frames the concepts of digital probable cause and collateral impact to address conflicts in the courts over big data searches using keyword and geofence warrants to identify unknown perpetrators. The Article draws on the analogy of John Doe DNA warrants to explain how advances in science and technology can give new grounds for probable cause and particularity when a perpetrator's identity is unknown. The Article also frames the concepts of collateral impact and collateral harm to evaluate overbreadth concerns and empathy disparities regarding the impact of searches on persons not involved with the crime. The Article's proposal enables controlled use of big data search strategies such as geofence and keyword warrants while forestalling abuses, such as mass surveillance of political protesters or hunting for abortion seekers.*

---

* Jack R. MacDonald Endowed Chair, University of Washington School of Law. Email: mdfan@uw.edu. Phone: (206) 685-4971. Thank you to Barry Friedman, Lauryn Gouldin, Sandy Mayson, Erin Murphy, Alexandra Natapoff, David Owens, Maria Ponomarenko, Chris Slobogin, and Seth Stoughton for valuable insights and advice and the organizers of the Law of the Police Conference at the University of Chicago Law School. Special thanks to Articles Editors Jack Wade and Anna Kate Benedict and the team at the *Texas Law Review* for outstanding editing and to Editor-in-Chief Mason Grist and Chief Articles Editor Thomasina H. Deering for excellent leadership and communication.

## Introduction

Arsonists set ablaze a home shared by three sleeping Senegalese immigrant families one early morning in a Denver neighborhood.[1] Five members of a family burned to death, including parents Djibril ("Djibby") and Adja Diol, their two-year-old daughter, Djibby's sister Hassan, and Hassan's infant daughter.[2] The unsolved murders haunted the region's Senegalese immigrant community with fears of potential hate crimes.[3]

A neighbor's security camera showed three masked figures in the targeted home's backyard pointing, then running away a few minutes before flames erupted and residents began screaming.[4] Said Senegalese community leader Papa Dia, "We don't know if they're out there plotting the next evil act[.] People are not eating properly and they are not sleeping properly because of that fear of the unknown of why they did this and who did this."[5]

Lingering unsolved for six months, the arson-murder cases grew cold.[6] Homicide detectives partnered with federal agents to try to crack the case.[7] The team pursued multiple investigative strategies drawing on electronic data trails.[8] We shed both location data, when our cell phones connect to cell sites for signal, and keyword data, when we search online for information, much like we shed DNA from hair and skin cells.[9] Big Tech companies store our consumer big data in massive vaults for profit-making purposes, such as

---

1. Response to Motion to Suppress Evidence Unlawfully Obtained (Home) at 2, People v. Seymour, No. 21CR20001 (Colo. Dist. Ct. Nov. 16, 2022) (on file with author) [hereinafter People's Response, Home, *Seymour*], *rule to show cause discharged*, 536 P.3d 1260 (Colo. 2023).

2. *Names, Photos Released of All 5 Victims in Green Valley Ranch Arson*, CBS COLO. (Aug. 13, 2020, 12:46 PM), https://www.cbsnews.com/colorado/news/victims-green-valley-ranch-arson-djibril-diol/ [https://perma.cc/UM3V-NB5P].

3. People's Reply to Defendant's Motions to Suppress at 1, *Seymour*, No. 21CR20001 (on file with author) [hereinafter People's Reply, *Seymour*].

4. Transcript of Oral Ruling on Motion to Suppress at 9, *Seymour*, No. 21CR20001 [hereinafter Oral Ruling, *Seymour*].

5. *Fears Grow for Denver's Senegalese Community as Reward Increases in Green Valley Ranch Fatal Fire Case*, CBS COLO. (Sept. 10, 2020, 6:06 AM), https://www.cbsnews.com/colorado/news/fears-denver-senegalese-community-reward-increases-green-valley-ranch-fatal-fire/ [https://perma.cc/Y4N2-MZS3].

6. Darren Whitehead, *Green Valley Ranch Murder Case: Google Evidence Will Be Allowed at Teen's Trial*, 9NEWS (Nov. 16, 2022, 2:53 PM), https://www.9news.com/article/news/crime/green-valley-ranch-arson-murder/73-b3e6f847-d510-4a2b-bec6-e9351352ffd5 [https://perma.cc/WFB8-YZ77].

7. Elizabeth Hernandez, *Denver Police Arrest 3 Teens in Arson Fire that Killed 5 Family Members in Green Valley Ranch Home*, DENVER POST (Jan. 27, 2021, 2:00 PM), https://www.denverpost.com/2021/01/27/green-valley-ranch-arson-djibril-diol-arrest/ [https://perma.cc/Q6KT-W4EU].

8. Oral Ruling, *Seymour*, *supra* note 4, at 10–11.

9. *See* Riley v. California, 573 U.S. 373, 385 (2014) (discussing the ubiquity of cell phones in modern life and how they would appear to a visitor from Mars to be part of the human anatomy); Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018) (discussing cell site location information).

facilitating targeted advertising, learning our preferences, and training artificial intelligence (AI) products.[10] Increasingly, law enforcement investigators are turning to these corporately held big data troves to crack cold cases via geofence warrants and keyword warrants.[11]

"Keyword warrants" direct the world's largest search engine providers, such as Google, Yahoo, and Microsoft (the maker of Bing), to search their data vaults for users who searched incriminating keywords during a relevant period.[12] Often secret and filed under seal, keyword warrants request businesses to disclose IP addresses identifying the devices of users who entered particular search keywords during a relevant time.[13] Investigators then narrow the list of potential suspect devices using location and other data, and then obtain the user account information identifying suspects winnowed from the pool.[14]

While keyword warrants draw on Big Tech's trove of search history data, "geofence warrants," also known as "reverse location search warrants," draw on the location data that companies amass about users to facilitate targeted advertising.[15] An especially alluring target for both keyword and geofence warrants is Google because of its dominant market share in internet and mobile search services and apps.[16] Google location data, stored in its Sensorvault and linked databases, is substantially more precise than cell site location data obtained via "tower dumps" seeking all cell phones connecting to a particular cell phone tower for signal in an area because Google draws on Wi-Fi access points, Bluetooth beacons, and GPS data.[17] The difference in precision can be between a multiple-block radius approximated from tower

10. *See, e.g.*, Mary D. Fan, *The Right to Benefit from Big Data as a Public Resource*, 96 N.Y.U. L. REV. 1438, 1440–41 (2021) (discussing the massive pool of consumer big data collected by companies).

11. *See infra* notes 19–22 and accompanying text; *see also infra* sections I(A)(1)–(2).

12. *E.g.*, Search Warrant Application Affidavit at 4, *In re* Search of Info. and Recs. Associated with Google Searches, No. 18-MJ-170 (W.D. Tex. Mar. 14, 2018) (filed under seal) (on file with author) [hereinafter Google Keyword Warrant 1, Pipe Bombings].

13. *See id.* at 4, 8 (requesting information on Google users who searched for the addresses of the sites of pipe bombings in the month before each site was bombed).

14. *See, e.g.*, People's Reply, *Seymour*, *supra* note 3, at 3 (explaining the geofence multi-step winnowing process).

15. *In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 69–70 (D.D.C. 2021); Zach Whittaker, *Google Says Geofence Warrants Make Up One-Quarter of All US Demands*, TECHCRUNCH (Aug. 19, 2021, 4:54 PM), https://techcrunch.com/2021/08/19/google-geofence-warrants/ [https://perma.cc/BWS5-6R2D].

16. Mohit Rathi, Comment, *Rethinking Reverse Location Search Warrants*, 111 J. CRIM. L. & CRIMINOLOGY 805, 808–12 (2021); Donna Lee Elm, *Geofence Warrants: Challenging Digital Dragnets*, CRIM. JUST., Summer 2020, at 7, 8–9.

17. Criminal Complaint attach. at 2, United States v. Rhine, No. 21-MJ-646 (D.D.C. Nov. 4, 2021).

dumps, compared to a few meters or even feet around a crime scene, from Google data.[18]

While keyword warrants are often secret and revelations regarding them rare,[19] Google is reporting a surging number of geofence warrant requests for user location information since 2018, growing to more than 11,554 geofence warrants in 2020.[20] For example, geofence warrants unmasked the identities of persons who staged an armed insurrection at the U.S. Capitol on January 6, 2021 to disrupt the presidential election certification and transition of power.[21] At least forty-five federal criminal cases against insurrectionists entail the use of a geofence warrant to identity the defendant.[22]

Trying to solve the Diol family murders, investigators turned to tower dumps and geofence warrants before a keyword warrant netted their suspects.[23] Geofence and tower dump nets may return empty if perpetrators are not carrying phones, shut down their phones, or put them in airplane mode to prevent connection with cell sites.[24] Conversely, if an area is densely populated, too many devices render the information useless to find a suspect amid the haystack of users in the area.[25] In the Diol murder-arson

18. Mark Harris, *How a Secret Google Geofence Warrant Helped Catch the Capitol Riot Mob*, WIRED (Sept. 30, 2021, 7:00 AM), https://www.wired.com/story/capitol-riot-google-geofence-warrant/ [https://perma.cc/Z4SN-SUWE]; Jennifer Lynch, *Google's Sensorvault Can Tell Police Where You've Been*, ELEC. FRONTIER FOUND. (Apr. 18, 2019), https://www.eff.org/deeplinks/2019/04/googles-sensorvault-can-tell-police-where-youve-been [https://perma.cc/N52P-FLEJ]; Brief of Amici Curiae Technology Law and Policy Clinic at New York University School of Law & Electronic Frontier Foundation in Support of Defendant–Appellant at 8, United States v. Chatrie, No. 22-4489 (4th Cir. Jan. 27, 2023).

19. Thomas Brewster, *Exclusive: Government Secretly Orders Google to Identify Anyone Who Searched a Sexual Assault Victim's Name, Address or Telephone Number*, FORBES (Oct. 4, 2021, 10:33 AM), https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users [https://perma.cc/4NP5-C6M6].

20. GOOGLE, SUPPLEMENTAL INFORMATION ON GEOFENCE WARRANTS IN THE UNITED STATES (2020), https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf [https://perma.cc/3B42-CUJE]; *In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 68 (D.D.C. 2021).

21. United States v. Rhine, 652 F. Supp. 3d 38, 68–70 (D.D.C. 2023).

22. Harris, *supra* note 18.

23. Motion to Suppress Evidence from a Keyword Warrant at 3–5, People v. Seymour, No. 21CR20001 (Colo. Dist. Ct. Nov. 16, 2022) (on file with author) [hereinafter Motion to Suppress, *Seymour*], *rule to show cause discharged*, 536 P.3d 1260 (Colo. 2023).

24. *See, e.g.*, Crystal Wilde, *How to Make Your Phone (Nearly) Impossible to Track—and Keep Personal Information Safe*, READER'S DIG. (Dec. 22, 2022), https://www.rd.com/article/how-to-make-your-phone-impossible-to-track/ [https://perma.cc/4TZM-KFV5] (noting that shutting down phones or putting them on airplane mode prevents location tracking).

25. *See* Motion to Suppress, *Seymour*, *supra* note 23, at 3–4 (describing the failure of tower dumps and geofence warrants to find a suspect because of the large number of users in the area).

investigation, the tower dumps and two geofence warrants failed to identify potential suspects because so many devices were in the residential area.[26]

So, the Diol investigators sought a keyword warrant directing Google to reveal the IP addresses of persons who had searched the targeted home address in the fifteen days before the fire.[27] To establish probable cause, a detective working the Diol murders attested that, based on how the arson was executed, the crime appeared personally targeted and there was a reasonable basis to believe the perpetrators searched for the address to find the home in the dense subdivision.[28] The multistep search procedure behind keyword warrants was so new to the homicide detective that it took three tries and communications with Google to determine how to frame the keyword warrant.[29]

Google's response to the keyword warrant cracked the cold case.[30] The warrant returned information regarding five accounts that searched for the targeted address within the fifteen-day period before the arson.[31] The return included the IP addresses, location, and associated email addresses of the five accounts.[32] One of the persons was a member of the Diol family.[33] The remaining accounts led investigators to the three persons ultimately charged with the murders and arson: Kevin Bui, Gavin Seymour, and a juvenile with name withheld.[34] Returns on subsequent search warrants yielded text messages between Bui and Seymour that revealed the alleged motive: revenge spurred by erroneous digital data.[35] Bui was buying a gun at a city park when someone robbed him, taking his cell phone.[36] Bui activated the Find My iPhone feature and mistakenly believed based on the digital trail that the phone was in the Diol home.[37]

---

26. *See* Oral Ruling, *Seymour*, *supra* note 4, at 11 (explaining the investigators' "starting point" was a geofence "which essentially fences in certain areas and tries to identify those folks coming in and out of that particular area" and how that strategy "didn't yield any productive results or any suspects").

27. People's Reply, *Seymour*, *supra* note 3, at 2; Response to Motion to Suppress Evidence Unlawfully Obtained (Cellphone Data) at 2, *Seymour*, No. 21CR20001 (on file with author) [hereinafter People's Response, Cell Phone Data, *Seymour*].

28. People's Reply, *Seymour*, *supra* note 3, at 2.

29. *Id.*

30. People's Response, Cell Phone Data, *Seymour*, *supra* note 27, at 2.

31. *Id.* at 2–3.

32. *Id.*

33. *Id.* at 2.

34. *Id.* at 3.

35. Whitehead, *supra* note 6; Transcript of Preliminary Hearing at 148–51, People v. Seymour, No. 21CR20001 (Colo. Dist. Ct. Nov. 16, 2022) [hereinafter Preliminary Hearing Transcript, *Seymour*], *rule to show cause discharged*, 536 P.3d 1260 (Colo. 2023).

36. Preliminary Hearing Transcript, *Seymour*, *supra* note 35, at 58.

37. *Id.* at 58–59.

The Diol arson-murders tragically show how digital data is transforming how crimes are perpetrated—and how perpetrators may be identified. The law is struggling to catch up. The law is unsettled regarding whether law enforcement officers may use digital forensic strategies. Courts are split on geofence warrants.[38] Judicial rulings on keyword warrants are so nascent that one of the main judicial decisions to date—in the Diol case—was an oral ruling with no written decision.[39] Ultimately, the Colorado Supreme Court upheld the Diol murder investigators' reliance on the keyword warrant.[40]

There is almost no scholarship on keyword warrants, save for a student comment that analogizes keyword warrants to the 1700s-era general warrants that prompted the Framers to draft the protections of the Fourth Amendment.[41] As for geofence warrants, with the rare exceptions of arguments that the warrant and probable cause requirements should not apply at all,[42] the emerging scholarship also tends to analogize geofence warrants to the historical abuse of general warrants and government rummaging in the 1700s.[43] The recurring references to eighteenth-century practices are alluring because of the long dominance of the originalist lens in constitutional

38. *Compare*, *e.g.*, United States v. Rhine, 652 F. Supp. 3d 38, 70, 90 (D.D.C. 2023) (affirming grant of geofence warrant that netted hundreds of January 6 insurrection suspects), *and In re* Search Warrant Application for Geofence Location Data Stored at Google, 497 F. Supp. 3d 345, 351, 364 (N.D. Ill. 2020) (authorizing geofence warrants revealing the location of persons at multiple locations), *with* United States v. Chatrie, 590 F. Supp. 3d 901, 921, 929–31, 941 (E.D. Va. 2022) (finding that geofence warrant that only revealed account user information for three devices lacked particularized probable cause), *and In re* Search of Info. Stored at Premises Controlled by Google, LLC, 542 F. Supp. 3d 1153, 1158–59 (D. Kan. 2021) (denying geofence warrant expressing concern that the location of innocent cell phone users may be revealed).

39. Oral Ruling, *Seymour*, *supra* note 4, at 43–44, 48; *see also* Petition for Rule to Show Cause at 4, People v. Seymour, 536 P.3d 1260 (Colo. 2023) (No. 2023SA12) (noting that the district "did not enter any written orders regarding the Motion to Suppress").

40. People v. Seymour, 536 P.3d 1260, 1280 (Colo. 2023).

41. Chelsa Camille Edano, Comment, *Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants*, 97 WASH. L. REV. 977, 989–91, 995 (2022).

42. Christopher Slobogin, *Suspectless Searches*, 83 OHIO ST. L.J. 953, 957, 961 (2022); Reed Sawyers, *For Geofences: An Originalist Approach to the Fourth Amendment*, 29 GEO. MASON L. REV. 787, 812 (2022).

43. Haley Amster & Brett Diehl, Note, *Against Geofences*, 74 STAN. L. REV. 385, 434 (2022); Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2511 (2021); Esteban De La Torre, Note, *Digital Dragnets: How the Fourth Amendment Should Be Interpreted and Applied to Geofence Warrants*, 31 S. CAL. INTERDISC. L.J. 329, 339 (2022); Andrew Guthrie Ferguson, *Digital Rummaging*, 101 WASH. U. L. REV. (forthcoming 2024) (manuscript at 57–63) (on file with author); Brian L. Owsley, *The Best Offense Is a Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 HOFSTRA L. REV. 829, 863 (2022); *see also, e.g.*, Leonard W. Levy, *Origins of the Fourth Amendment*, 114 POL. SCI. QUARTERLY 79, 81–83 (1999) (discussing general warrants in the 1700s that prompted the Framers' concerns in drafting the Fourth Amendment).

interpretation, especially during the lengthy tenure of Justice Antonin Scalia on the Supreme Court.[44]

Analyzing digital forensic investigative techniques through the lens of a time before electric power, much less electronic data, is almost comically anachronistic.[45] Yet this regressive lens is alluringly rose-colored by Romantic Luddism, a combination of fear of technology and nostalgia for simpler times long gone.[46] The terms Luddite and Luddism arise from the anti-technology stance of English textile workers, who beginning in the early 1800s impeded industry efforts to innovate through technology by smashing new machines and staging uprisings.[47] The opposition to technological innovation grew far beyond the English textile worker revolts of the early 1800s, becoming a Romantic ideal of a simpler life predating technological change.[48] Though sometimes viewed as a pejorative for technophobes, Luddism has deeper philosophical offshoots throughout history, influencing diverse domains from science to literature, law, and policy.[49] Modern-day Luddites, sometimes proudly self-proclaiming to be neo-Luddites, continue a Romantic tradition of writers such as Jean-Jacques Rousseau in decrying the harms and risks of technological dependence.[50] Anxieties over technology are particularly resonant in modern-day fears of mass privacy intrusions and civil liberties violations against groups such as protesters and women seeking abortions.[51]

---

44. *See, e.g.*, David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739, 1762–64 (2000) (discussing the rise of "new Fourth Amendment originalism" in the Justice Scalia-era Supreme Court); Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1183–84 (2016) (discussing the rise of originalism as "an important mode of constitutional interpretation" since the late 1980s).

45. *See* THOMAS P. HUGHES, NETWORKS OF POWER: ELECTRIFICATION IN WESTERN SOCIETY, 1880–1930, at 2, 19 (1983) (discussing the development of electrical systems and lighting in the 1800s).

46. *See, e.g.*, STEVEN E. JONES, AGAINST TECHNOLOGY: FROM THE LUDDITES TO NEO-LUDDISM 45–48, 77–79 (2006) (discussing the Romantic philosophy of the Luddites); Thomas Pynchon, *Is It O.K. to Be a Luddite?*, N.Y. TIMES, Oct. 28, 1984 (discussing the nostalgia of Luddites).

47. Adrian J. Randall, *The Philosophy of Luddism: The Case of the West of England Woolen Workers, ca. 1790–1809*, 27 TECH. & CULTURE 1, 1–3 (1986).

48. JONES, *supra* note 46, at 45–48, 77–79.

49. NICOLS FOX, AGAINST THE MACHINE: THE HIDDEN LUDDITE TRADITION IN LITERATURE, ART, AND INDIVIDUAL LIVES xii, xvi–xvii, 257–59 (2002); VAL DUSEK, PHILOSOPHY OF TECHNOLOGY 182 (2006); David Edgerton, Comment, *In Praise of Luddism*, 471 NATURE 27, 28 (2011).

50. DUSEK, *supra* note 49, at 182.

51. *See, e.g.*, Matthew Guariglia, *Geofence Warrants and Reverse Keyword Warrants Are So Invasive, Even Big Tech Wants to Ban Them*, ELEC. 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 [https://perma.cc/58KP-H65H] (claiming that "[g]eofence and reverse keyword warrants are some of the most dangerous, civil-liberties-infringing" law

As advances in technology change how crime is committed and who perpetrators target, our conceptions of the Fourth Amendment's requirements of probable cause and particularity for searches of big data need updating. Filling a gap, this Article proposes new conceptual frameworks for evaluating the Fourth Amendment propriety of strategies such as geofence and keyword warrants that are evolving with technology.[52]

This Article frames the concept of digital probable cause to capture how advances in technology can generate probable cause to issue a search warrant for data even if perpetrators are unknown.[53] The Article unravels confusion in some judicial decisions that conflate the requirement of probable cause to arrest or search a physical person with probable cause to search a place for evidence, such as data.[54] Because an arrest warrant authorizes the seizure of a particular person, the identity must be particularized and probable cause against that individual specified.[55] Similarly, to search the body or clothes of a particular person, probable cause must be particularized to the physical person being searched as the site of evidence.[56] But a search warrant can extend to many other sites besides the limited context of a search of a physical person.[57] A search warrant is based on a fair probability that evidence of a crime is present in the place to be searched.[58] The place to be searched could belong to an innocent third party, such as a girlfriend or parent, whose house may be searched for a hidden weapon.[59] In executing a search warrant for the evidence specified, officers regularly must sift through

enforcement tactics posing threats to protesters and civil liberties); Bobby Allyn, *Privacy Advocates Fear Google Will Be Used to Prosecute Abortion Seekers*, NPR (July 11, 2022, 5:00 AM), https://www.npr.org/2022/07/11/1110391316/google-data-abortion-prosecutions [https://perma.cc/53JV-MLSQ] (expressing concerns about targeting abortion seekers).

52. *See infra* Part I.

53. *See infra* Parts II–III.

54. *See infra* text accompanying notes 356–59.

55. Ybarra v. Illinois, 444 U.S. 85, 91 (1979).

56. *See id.* at 90–91 (distinguishing the police's warrant based on probable cause to search the location that the person was in from any particularized probable cause to search that person).

57. *E.g.*, United States v. White, 863 F.3d 784, 785 (8th Cir. 2017) (search warrant for home of suspect's parents); United States v. McKenzie–Gude, 671 F.3d 452, 456–57 (4th Cir. 2011) (search warrant for home of suspect's friend); *cf., e.g.*, Anderson v. Creighton, 483 U.S. 635, 637, 641 (1987) (holding that officer should be permitted to argue that warrantless search of innocent third party's home for fugitive was reasonable based on exigent circumstances).

58. *See, e.g.*, Florida v. Harris, 568 U.S. 237, 243 (2013) (describing probable cause as only requiring "the kind of 'fair probability' on which 'reasonable and prudent [people,] not legal technicians, act,'" enough to "'warrant a [person] of reasonable caution in the belief' that contraband or evidence of a crime is present" (first quoting Illinois v. Gates, 462 U.S. 213, 231 (1983); then quoting Texas v. Brown, 460 U.S. 730, 742 (1983) (plurality opinion))).

59. *See* Zurcher v. Stanford Daily, 436 U.S. 547, 556 (1978) ("The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific "things" to be searched for and seized are located on the property to which entry is sought.").

non-evidentiary property, such as entering a home and searching through bedrooms, drawers, and closets for a weapon hidden away.[60]

This Article frames the concepts of collateral impact and harms to assess claims of overbreadth.[61] "Collateral impact" refers to concerns about how investigative strategies affect persons who are not involved in the crime.[62] "Collateral harms" refers to impacts on uninvolved third parties that amount to injuries.[63] The Article contrasts the treatment of collateral harms in warrant execution doctrine—which is most likely to affect people with the least resources—with overbreadth concerns regarding keyword and geofence warrants, which are more likely to rouse the concerns of people with resources and power.[64] The Article argues against technological exceptionalism in the Fourth Amendment, drawing on theories of interest convergence and empathy deficits.[65]

Offering an analogic framework, this Article addresses confusion in the courts over the constitutionality of warrants seeking the identity of an unknown perpetrator particularized by digital search parameters.[66] The Article draws on the use of John Doe warrants based on DNA profiles to explain how probable cause and particularity for warrants do not always require knowing the identity of a discrete perpetrator.[67] Rather, advances in science and technology can give a reasonable basis to believe there is a fair probability that the individuals identified by technological and scientific means perpetrated the offense.[68]

Overly broad keyword or digital warrants that sweep up numerous plainly uninvolved persons or rove exploratorily through data without evidence of a known offense are insufficient for digital probable cause and particularity.[69] Rather, digital probable cause and particularity can be established by a tightly framed keyword or geofence warrant likely only to net persons for whom there is probable cause to believe perpetrated an unsolved crime.[70] This framework grounds a pragmatic approach that permits tailored geofence and keyword warrants to determine the perpetrators of

60. Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976); *In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 84 (D.D.C. 2021) (quoting *Andresen*, 427 U.S. at 482 n.11).

61. *See infra* Parts II–III.

62. *See infra* Part II.

63. *See infra* subpart II.

64. *See infra* subpart II(B).

65. *See infra* subpart II(B).

66. *See infra* Part III.

67. *See infra* Parts II–III.

68. *See infra* Part II.

69. *See infra* subpart III(A).

70. *See infra* subpart III(A).

known crimes like the Diol murders while forestalling abuses, such as mass surveillance of political protesters or hunting for women seeking abortions.[71]

This Article proceeds in three parts. Part I illuminates the nostalgic Luddism that influences Fourth Amendment jurisprudence and the challenges posed by evolving technologies to this dominant lens.[72] This Part explains the operation of geofence and keyword warrants and how their power to crack cold cases by unidentified perpetrators both tempt and terrify.[73] The confusion in the courts over the constitutionality of geofence and keyword warrants is emblematic of the larger challenges of the Romantic Luddism in Fourth Amendment originalism that has grown in influence over the decades.[74]

Part II frames and theorizes the concepts of collateral impact and collateral harm to analyze oft-expressed concerns that technological strategies may reveal the data of innocent persons. This Article uses the term collateral impact to refer to how persons who are not the targets of an investigative tactic or who are uninvolved in a crime are affected by the tactic.[75] The collateral impact can entail substantial collateral harm, such as being detained in handcuffs and asked about your immigration status by armed SWAT team members executing a search warrant on a housemate.[76] Collateral harm refers to injuries sustained by persons uninvolved in the crime.[77] Potentially disclosing the presence of an electronic device can entail far less collateral harm compared to other practices repeatedly upheld by the courts, such as detaining all persons onsite during a search warrant execution, or mistakenly searching incorrect persons or homes.[78] This Part illuminates the inequities of technological exceptionalism in overweighing collateral harms of incidental data disclosure compared to the collateral harms that are more likely to impact people with the least resources and power.[79]

Part III frames the concept of digital probable cause to address a major source of confusion in the courts over digital search warrants for unknown and thus unnamed perpetrators.[80] Data-based parameters that give rise to a

71. *See infra* subpart III(B); *see also, e.g.*, Allyn, *supra* note 51 (discussing fears over hunting abortion seekers); *Geofence Warrants and the Fourth Amendment*, *supra* note 43, at 2519–20 (discussing concerns over surveilling protesters).

72. *See infra* Part I.

73. *See infra* subpart I(A).

74. *See infra* subpart I(B).

75. *See infra* Part II.

76. Muehler v. Mena, 544 U.S. 93, 96, 98–99 (2005).

77. *See infra* Part II.

78. *See infra* Part II.

79. *See infra* subpart II(B).

80. *See infra* Part III.

fair probability that evidence of a crime can be found can support digital probable cause.[81] Parameters could be narrowly drawn geolocation coordinates for geofence warrants or keyword search parameters that only a perpetrator planning or executing the crime might use.[82] This Part draws on analogies from decades of practice and litigation over John Doe warrants, which illustrate how warrants can still be valid even if a perpetrator is unknown if particularity and probable cause arises from other parameters.[83] Finally, this Part offers three principles to protect against abuses of big data search warrants, such as hunting for protesters or abortion seekers.[84]

## I. Fourth Amendment Romantic Luddism and Evolving Technology

There is a bit of a Romantic Luddite in many of us (the author included).[85] The vision of Luddism is freedom of human flourishing without replacement by, or dependence on, technology and a critical interrogation of the impact of technology.[86] Nostalgically recalling simpler times before technological change, Romantic Luddites fear the seductive promises of technology to tempt us with shortcuts and alluring benefits only to addict us and diminish our human abilities to perform tasks taken over by machines.[87] We can turn off our own lights and up our music or thermostats—why do we need Siri, Google Voice, or Smart Home systems monitoring our utterances,

81. *See infra* Part III.

82. *See infra* subpart III(A).

83. *See infra* subpart III(A).

84. *See infra* subpart III(B).

85. *See* Brett Frischmann, *There's Nothing Wrong with Being a Luddite*, SCI. AM. (Sept. 20, 2018), https://blogs.scientificamerican.com/observations/theres-nothing-wrong-with-being-a-luddite/ [https://perma.cc/W69J-27BZ] (arguing that "some Luddism is important for society" because Luddism "enables critical reflection and evaluation" of how technology is impacting the world and our personhood); Jathan Sadowski, *I'm a Luddite. You Should Be One Too*, CONVERSATION (Aug. 9, 2021, 1:07 AM), https://theconversation.com/im-a-luddite-you-should-be-one-too-163172 [https://perma.cc/CGY2-WATX] (explaining that Luddism "treat[s] technology as a political and economic phenomenon that deserves to be critically scrutini[z]ed and democratically governed, rather than a grab bag of neat apps and gadgets" and that in this approach, Luddism has widespread appeal).

86. Darryl Coulthard & Susan Keller, *Technophilia, Neo-Luddism, eDependency, and the Judgement of Thamus*, 10 J. INFO. COMMC'N & ETHICS SOC'Y 262, 266 (2012); Frischmann, *supra* note 85; Sadowski, *supra* note 85.

87. JOACHIM DIEDERICH, THE PSYCHOLOGY OF ARTIFICIAL SUPERINTELLIGENCE 77–78 (2021); *see* Joel Mokyr, Chris Vickers & Nicholas L. Ziebarth, *The History of Technological Anxiety and the Future of Economic Growth: Is This Time Different?*, J. ECON. PERSPS., Summer 2015, at 31, 32–34 (discussing economists' views on the costs of technological advancement); *cf.* Kinga Piwowarska, *Contemporary Neo-Luddism in the Digital Transformation of Employment*, *in* ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS 354, 354–56, 359–60 (Laura Martín Miraut & Mariusz Zalucki, eds., 2021) (discussing how the increasing use of AI could lead to human rights violations).

habits, and preferences while performing these tasks for us?[88] Before navigation devices and apps, people used their brains and maps to navigate, knowing better than to obediently continue—and perhaps drive off a cliff—as directed by a computerized voice.[89] Before newfangled keyword warrants and geofence tactics, murders and arsons were solved by gumshoe detective work (though the homicide clearance rate has been astonishingly dismal since the 1960s, hovering at just above 60%).[90]

Fear and anxiety over how technology is changing our lives is a growing, important phenomenon, going by numerous terms in the literature, such as technophobia, digitalization anxiety, technology anxiety, and technostress.[91] There are many kinds of anxieties over technology, such as fears over learning and adapting to new technologies, disruption of familiar patterns of life, alienation of labor as machines substitute for humans, surveillance, and privacy erosion.[92] The rapid rate of technological change, concomitant mass cultural change, and growing public distrust in both governmental and private institutions exacerbate technology-related fears and anxieties.[93]

Consumer and research surveys show fear over adapting to new technologies, especially among older adults, but also a desire to reap the

88. *Cf.* Roberto Yus & Primal Pappachan, *Smart Devices Spy on You—2 Computer Scientists Explain How the Internet of Things Can Violate Your Privacy*, CONVERSATION (Mar. 14, 2022, 8:20 AM), https://theconversation.com/smart-devices-spy-on-you-2-computer-scientists-explain-how-the-internet-of-things-can-violate-your-privacy-174579 [https://perma.cc/D6YL-NPNT] (discussing the potential privacy and surveillance harms from Smart Homes and devices on the Internet of Things).

89. *Cf.* Jennifer M. Bernstein, *Are We Literally Losing Our Way by Relying on GPS Devices?*, WASH. POST (Dec. 2, 2018, 8:00 AM), https://www.washingtonpost.com/national/health-science/by-relying-on-gps-devices-are-we-literally-losing-our-way/2018/11/30/dd9eb6ae-e9bd-11e8-bbdb-72fdbf9d4fed_story.html [https://perma.cc/9LAQ-YBWG] ("Research has established that mobile navigational devices, such as the GPS embedded in one's smartphone, make us less proficient wayfinders. . . . Handheld navigational devices have been linked to lower spatial cognition, poorer wayfinding skills and reduced environmental awareness."); *Man Follows Sat Nav to Cliff Edge*, BBC NEWS (Mar. 25, 2009, 8:47 PM), https://news.bbc.co.uk/2/hi/uk_news/england/bradford/7962212.stm [https://perma.cc/95E8-53GM] (reporting the case of a man who followed navigation device directions to the edge of a cliff, leaving his vehicle teetering over the edge).

90. Avdi S. Avdija, Christian Gallagher & DeVere D. Woods, *Homicide Clearance Rates in the United States, 1976–2017*, 37 VIOLENCE & VICTIMS 101, 102 (2022).

91. For an overview of the numerous terms, see, for example, Katharina F. Pfaffinger, Julia A.M. Reif, Andreas K. Huber, Vera M. Eger, Melina K. Dengler, Jan Philipp Czakert, Erika Spieß & Rita Berger, *Digitalisation Anxiety: Development and Validation of a New Scale*, DISCOVER MENTAL HEALTH, Nov. 29, 2021, at 1, 1–2, https://link.springer.com/content/pdf/10.1007/s44192-021-00003-w.pdf [https://perma.cc/AB3Y-Q5BE].

92. *See, e.g.*, Mokyr et al., *supra* note 87, at 32 (noting the different forms of anxiety and focusing on replacement of human labor, disruption, dehumanization, and technological stagnation).

93. CALESTOUS JUMA, INNOVATION AND ITS ENEMIES 5 (2016).

benefits of new technologies.[94] The nature of anxieties can vary with age, with persons aged eighteen to thirty-four concerned more about data disclosure than persons forty-five or older.[95] A survey by the Centre for International Governance Innovation, in collaboration with the United Nations Conference on Trade and Development and other organizations, found that more than half of respondents in twenty-five nations surveyed reported growing concern over online privacy.[96] Greater reliance on digital devices, such as during the pandemic, also heightens technology-related anxieties, showing the conflicting natures of technological fear and craving.[97]

Constitutional criminal procedure doctrine is also split by craving and fear of technological change and the opportunities that innovation opens.[98] This Part frames our conflicted present by discussing the struggle in constitutional criminal procedure over whether to allow investigative techniques to evolve with changing technology.[99] From DNA to digital forensics and beyond, technology-enabled tactics tempt with the potential to crack cold cases, address community fears, and provide some succor to survivors.[100] The tactics also terrify the technophobe in most of us about the risks of pervasive surveillance slipping beyond compelling use cases like solving cold cases.[101]

---

94. *E.g.*, Galit Nimrod, *Technophobia Among Older Internet Users*, 44 EDUC. GERONTOLOGY 148, 148–50 (2018); Mario Martínez-Córcoles, Mare Teichmann & Mart Murdvee, *Assessing Technophobia and Technophilia: Development and Validation of a Questionnaire*, 51 TECH. SOC'Y, 183, 183–86 (2017); Jason Bennett Thatcher, Misty L. Loughry, Jaejoo Lim & D. Harrison McKnight, *Internet Anxiety: An Empirical Study of the Effects of Personality, Beliefs, and Social Support*, 44 INFO. & MGMT. 353, 353–55 (2007); Candoo Tech, *Older Adults Admit High Anxiety and Fear About New Technology: Candoo Tech Surveys Shows 53% of Seniors Say Learning a New Device Is More Stressful than Going to the Dentist*, P.R. NEWSWIRE (Dec. 18, 2020, 8:49 AM), https://www.prnewswire.com/news-releases/older-adults-admit-high-anxiety-and-fear-about-new-technology-candoo-tech-surveys-shows-53-of-seniors-say-learning-a-new-device-is-more-stressful-than-going-to-the-dentist-301196011.html [https://perma.cc/Q7YF-YW77].

95. Press Release, Michael Curtis, Media Rels. & Soc. Media Leader, EY Glob., EY Survey: Digital Home Services Boom Fuels Anxiety Around Well-Being and Data Privacy (May 6, 2021), https://www.ey.com/en_gl/news/2021/05/ey-survey-digital-home-services-boom-fuels-anxiety-around-well-being-and-data-privacy [https://perma.cc/256Z-EZ8Z].

96. United Nations Conf. on Trade & Dev., *Data Privacy: New Global Survey Reveals Growing Internet Anxiety*, UNCTAD (Apr. 16, 2018), https://unctad.org/news/data-privacy-new-global-survey-reveals-growing-internet-anxiety [https://perma.cc/ST46-GGSJ].

97. Curtis, *supra* note 95; Brook Auxier & Paul H. Silverglate, *About One-Third of Consumers Report Feeling Overwhelmed by Tech Management During COVID-19*, DELOITTE (Aug. 19, 2021), https://www2.deloitte.com/xe/en/insights/industry/technology/digital-fatigue.html [https://perma.cc/M6Z3-JETP]; Galit Nimrod, *Not Good Days for Technophobes: Older Internet Users During the COVID-19 Pandemic*, 47 EDUC. GERONTOLOGY 160, 168 (2021).

98. *See infra* subpart I(A).

99. *See infra* subpart I(A).

100. *See infra* subpart I(A).

101. *See infra* subpart I(A).

The craving and fear over the power of geofence and keyword warrants is emblematic of the overarching technophobia in Fourth Amendment jurisprudence.[102] This Part explains the operation of geofence and keyword warrants, their powerful utility in cracking cold cases, and the new wave of litigation in the courts over the legality of such tactics.[103] The Part frames the contemporary challenges to geofence and keyword warrants in the context of the larger oscillation in constitutional criminal procedure between the nostalgia of originalism's Romantic Luddism and the need to adapt to the realities of technological evolution.[104]

### *A. The Allure and Terror of Keyword and Geofence Warrants*

Consider another investigation of multiple murders on a wintry night in a small college town so bucolic that there was not a single homicide for the preceding seven years.[105] Just over a week before the Thanksgiving break, in the early morning of November 13, 2022, someone entered a home shared by university students and stabbed to death four students barely in their twenties.[106]

The unsolved murders of students in their bedrooms rocked the college town, with numerous college students going home early or refusing to return from Thanksgiving break out of fear.[107] By December, some classrooms at the university were half-empty.[108] Even people who returned lived in fear of the unknown killer on the loose, buying doorbell cameras, installing locks, and fearing to walk home.[109]

---

102. *See infra* subpart I(B).

103. *See infra* subpart I(A).

104. *See infra* subpart I(B).

105. Mike Baker, Nicholas Bogel-Burroughs & Serge F. Kovaleski, *A Knife Sheath, Phone Pings and Trash: The Hunt for a Killer in Idaho*, N.Y. TIMES (Jan. 5, 2023), https://www.nytimes.com/2023/01/05/us/idaho-murders-suspect-kohberger-evidence.html [https://perma.cc/GXJ8-E8YR].

106. Application for Search Warrant (Residence) [Redacted] exhibit A at 1–3, 5, *In re* Application for a Search Warrant, SW No. 12-29-2022A (Wash. Super. Ct. Jan. 17, 2023) (on file with author); Kevin Shalvey & Emily Shapiro, *4 Idaho College Students Killed in 'Targeted Attack,' No Suspects in Custody*, ABC NEWS (Nov. 16, 2022, 8:01 AM), https://abcnews.go.com/US/idaho-college-students-found-dead-apparent-homicide-officials/story?id=93247819 [https://perma.cc/BG9C-JGXK].

107. Nicholas Bogel-Burroughs, *Killings Left an Idaho College Town Shaken*, N.Y. TIMES (Jan. 5, 2023) [hereinafter Bogel-Burroughs, *Killings Left an Idaho College Town Shaken*], https://www.nytimes.com/2022/12/03/us/idaho-university-moscow-killings.html [https://perma.cc/GV6E-Y4CW]; Rachel Sun, Mike Baker & Nicholas Bogel-Burroughs, *'Targeted' Killings and No Arrest Bring Fear to University of Idaho*, N.Y. TIMES (Jan. 5, 2023) [hereinafter Sun et al., *Targeted Killings*], https://www.nytimes.com/2022/11/15/us/university-idaho-students-killings.html [https://perma.cc/5E7S-HWUL].

108. Bogel-Burroughs, *Killings Left an Idaho College Town Shaken*, *supra* note 107.

109. *Id.*

What ultimately cracked the case was a "video canvass" of the neighborhood around the slain students' home, asking for surveillance camera footage from neighbors and businesses.[110] Police were able to track the movements of a vehicle linked to Bryan Kohberger from the murder scene in Moscow, Idaho, where the slain students studied at the University of Idaho, to Washington State University, where Kohberger studied.[111]

But what happens when the increasingly expansive net of private video surveillance, traffic cameras, and campus security cameras does not fortuitously track and help identify a perpetrator from crime commission through getaway? In addition to canvassing the area around a crime to see if any private surveillance camera happened to record the perpetrator, police are increasingly canvassing the major technology companies that hold a massive vault of data on our movements and online search histories.[112] Two contested tactics are keyword warrants, also known as reverse keyword search warrants, and geofence warrants, also known as reverse location warrants.[113] Both digital forensic strategies are explained below as a prelude to delving into legal conflicts over the constitutionality of geofence and keyword warrants.

*1. Keyword Warrants and Crimes with Unknown Perpetrators.*— Though used for years, keyword warrants rarely come to light, sometimes only emerging by mistaken disclosure in violation of a seal order.[114] Keyword warrants are typically directed at the Big Tech companies that offer the most-used search engines: Google, Microsoft, and Yahoo.[115] The dominant leader in the search engine market ever since 1997, when first introduced, Google

110. Application for Search Warrant (Residence) [Redacted], *supra* note 106, exhibit A at 6; Gene Johnson & Manuel Valdes, *The White Sedan: How Police Found Suspect in Idaho Slayings*, ASSOCIATED PRESS (Jan. 6, 2023, 6:47 PM), https://apnews.com/article/washington-pennsylvania-idaho-5f5173a3af306701d5659f2fb61a9d44 [https://perma.cc/3B97-88US].

111. Application for Search Warrant (Residence) [Redacted], *supra* note 106, exhibit A at 7–8; Johnson & Valdes, *supra* note 110.

112. *See supra* notes 20–22 and accompanying text.

113. *See infra* sections I(A)(1)–(2).

114. Jessica Schladebeck, *Feds Issue Secret 'Keyword Warrants' for Google Search History*, GOVTECH (Oct. 7, 2021), https://www.govtech.com/security/feds-issue-secret-keyword-warrants-for-google-search-history [https://perma.cc/2SQ7-6QAA].

115. *E.g.*, Google Keyword Warrant 1, Pipe Bombings, *supra* note 12, at 4; Search Warrant Application Affidavit at 4, *In re* Search of Info. and Recs. Associated with Microsoft Searches, No. 18-MJ-171 (W.D. Tex. Mar. 14, 2018) (filed under seal) (on file with author) [hereinafter Microsoft Keyword Warrant, Pipe Bombings]; Search Warrant Application Affidavit at 4, *In re* Search of Info. and Recs. Associated with Yahoo Searches, No. 18-MJ-168 (W.D. Tex. Mar. 14, 2018) (filed under seal) [hereinafter Yahoo Keyword Warrant, Pipe Bombings].

commands 81.95% of the worldwide search engine market.[116] The runner-up, Microsoft's Bing, is not even close, holding just 10.51% of the global search market.[117] Third in market share, Yahoo, holds only 2.67% of the global search market.[118] Google is also a particularly alluring target for keyword warrants because in addition to Google Search, the company offers the popular apps Google Maps and Waze, which perpetrators might use to search for directions to targeted victim addresses.[119]

Keyword warrants direct the companies to reveal IP addresses, which identify the device that connected to the Internet, and account information of users who have searched for terms related to a crime during a relevant period.[120] Time periods for keyword warrant searches vary, usually consisting of dates preceding the offense when the crime was likely in planning stages, such as the two weeks preceding the arson-murders in the Diol case or a month preceding the serial pipe bombings in Austin, Texas.[121] Google, Microsoft, and Yahoo keep records of the IP addresses of computers on which users conduct searches, even if the user is not logged into a personally identifying account.[122]

In addition, if the user is logged onto her account, Google, Microsoft and Yahoo also may have personal details such as her name, associated email and device IP addresses, phone numbers, physical addresses, means and sources of payment, and other transactions associated with the account.[123] Google, Microsoft, and Yahoo also retain data regarding the times and durations of online sessions by the user, and other logs of account usage.[124] The widespread popularity of Gmail addresses also amplifies the power of geofence warrants directed at Google because account user information may

116. Tiago Bianchi, *Global Desktop Market Share of Search Engines 2015–2024*, STATISTA (Feb. 12, 2024), https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/ [https://perma.cc/D7NU-MYU7].

117. *Id.*

118. *Id.*

119. Google Keyword Warrant 1, Pipe Bombings, *supra* note 12, at 6.

120. *E.g.*, *id.* at 4, 7–8 (requesting information on Google users who searched for the addresses of the sites of pipe bombings in the month before each site was bombed).

121. People's Response, Cell Phone Data, *Seymour*, *supra* note 27, at 2; Google Keyword Warrant 1, Pipe Bombings, *supra* note 12, at 4, 9.

122. Google Keyword Warrant 1, Pipe Bombings, *supra* note 12, at 6; Microsoft Keyword Warrant, Pipe Bombings, *supra* note 115, at 6; Yahoo Keyword Warrant, Pipe Bombings, *supra* note 115, at 6.

123. Google Keyword Warrant 1, Pipe Bombings, *supra* note 12, at 6; Microsoft Keyword Warrant, Pipe Bombings, *supra* note 115, at 6–7; Yahoo Keyword Warrant, Pipe Bombings, *supra* note 115, at 6–7.

124. Google Keyword Warrant 1, Pipe Bombings, *supra* note 12, at 6–7; Microsoft Keyword Warrant, Pipe Bombings, *supra* note 115, at 7; Yahoo Keyword Warrant, Pipe Bombings, *supra* note 115, at 7.

include Gmail records of times, dates, and places of log-in, and also retains data that can link various accounts.[125]

The keyword warrants that have emerged into public view illustrate how law enforcement officials use the tactic as an entryway strategy to try to identify unknown perpetrators of unsolved crimes.[126] Consider one of the few examples to come to light besides the Diol arson-murder investigation and the serial pipe bombings discussed at the outset. Because of a mistake, the U.S. Department of Justice accidentally disclosed a sealed geofence warrant in the investigation of kidnapping, sexual abuse, and trafficking of a minor.[127] Viewed briefly by journalists, the temporarily unsealed warrant directed Google to reveal the IP address and account information for persons who searched the victim's name, her mother's name, or her address during a 16-day period.[128] The keyword warrant was quickly resealed, and whether any results were obtained in the ongoing investigation is also secret.[129]

Other examples of keyword warrants emerged in the investigation of serial or spree pipe bombings in Austin, Texas, in March 2018 that killed two people when they opened packages left on their porches, and injured several others.[130] All the people slain were from Austin's Black, Indigenous, and People of Color (BIPOC) communities, which feared the serial bombings and murders were hate crimes with more to come.[131] Racing to find the unknown perpetrator, FBI agents secured multiple keyword warrants directing the world's three largest search engine providers—Google, Microsoft (maker of Bing), and Yahoo—to search their data vaults for users who searched the targeted home addresses.[132] One of the keyword warrants also requested that

125. Search Warrant Application Affidavit at 7, *In re* Search of Info. and Recs. Associated with Google Searches, No. 18-MJ-189 (W.D. Tex. Mar. 19, 2018) (filed under seal) (on file with author) [hereinafter Google Keyword Warrant 2, Pipe Bombings].

126. *See, e.g.*, Google Keyword Warrant 1, Pipe Bombings, *supra* note 12, at 4 (applying for a warrant to "establish who searched for information about the . . . addresses" to "help law enforcement to identify persons who may have knowledge about the bombings.").

127. Brewster, *supra* note 19.

128. *Id.*

129. *Id.*

130. Josh Gaynor, *Inside the FBI's Race to Stop Austin, Texas, Bombing Spree*, CBS NEWS (Oct. 20, 2020, 11:02 PM), https://www.cbsnews.com/news/austin-serial-bomber-mark-conditt-fbi-declassified/ [https://perma.cc/Z9UF-YTBN].

131. Emmanuella Grinberg & Jason Morris, *These Austin Residents Fear that the Explosions May Be Racially Motivated*, CNN (Mar. 15, 2018, 10:58 PM), https://www.cnn.com/2018/03/15/us/austin-explosion-packages/index.html [https://perma.cc/M3B5-VBBT]; *ADC Statement on Austin Bombings Targeting Communities of Color*, AMERICAN-ARAB ANTI-DISCRIMINATION COMM. (Mar. 20, 2018), https://adc.org/adc-statement-on-austin-bombings-targeting-communities-of-color/ [https://perma.cc/HZ9Y-EYKN].

132. Google Keyword Warrant 1, Pipe Bombings, *supra* note 12, at 2, 4; Microsoft Keyword Warrant, Pipe Bombings, *supra* note 115, at 2, 4; Yahoo Keyword Warrant, Pipe Bombings, *supra* note 115, at 2, 4.

Google disclose any users who searched for one of the victim's addresses on Google Maps or Waze.[133] More breathtakingly broadly, another keyword warrant asked Google for users who searched for various combinations of bombing and bomb-making related terms such as "cardboard" or "package" and "bomb" or "pipe bomb" or "PVC bomb."[134]

As investigators were executing the keyword warrants, two more bombs detonated, one in a residential neighborhood on March 18, and one on March 20, injuring three more people.[135] Ultimately, investigators determined the bomber to be Mark Anthony Conditt, 23, who detonated a last pipe bomb, killing himself and injuring an officer, when police tried to stop him on the road.[136] The geofence warrants, initially sealed in the case and unknown to the public, were unsealed following Conditt's death.[137]

From the keyword warrants that have emerged, it appears that the keyword searches proceed through a multistep process similar to the protocol Google has asked law enforcement to pursue for geofence warrants, discussed *infra* section I(A)(2).[138] To induce law enforcement to pursue a procedure that tries to reduce the privacy harms to uninvolved third parties, Google has a policy of challenging requests that fail to follow its internal protocol for using deidentified data to narrow the scope of the search.[139] To avoid litigation that would delay the investigation, officers work with Google specialists to work the protocol into their warrant requests—as occurred in the Diol murder investigation, when the homicide investigator reframed the geofence warrant based on Google's input.[140]

---

133. Google Keyword Warrant 2, Pipe Bombings, *supra* note 125, at 2, 9.

134. Search Warrant Application Affidavit at 2, *In re* Search of Info. and Recs. Associated with Google Searches, No. 18-MJ-191 (W.D. Tex. Mar. 19, 2018) (filed under seal) (on file with author) [hereinafter Google Keyword Warrant 3, Pipe Bombings].

135. Gaynor, *supra* note 130; Paul J. Weber & Will Weissert, *New Blast Sends Bombing Investigators to Central Texas FedEx Center*, CBS AUSTIN (Mar. 20, 2018, 4:41 AM), https://cbsaustin.com/news/local/breaking-package-addressed-to-austin-explodes-at-fedex-facility-in-schertz [https://perma.cc/C35W-D3HH]. Another bomb was intercepted on March 20 before it was able to detonate. Gaynor, *supra* note 130.

136. Jason Hanna, Faith Karimi, Jason Morris & Steve Almasy, *Police: Austin Bomber Left 25-Minute Confession Video on Phone*, CNN (Aug. 31, 2018, 6:26 PM), https://www.cnn.com/2018/03/21/us/austin-explosions/index.html [https://perma.cc/5AFT-Y3JV]; Clint Van Zandt, *What Makes a Serial Bomber Tick?*, ATLANTIC (Mar. 30, 2018), https://www.theatlantic.com/health/archive/2018/03/what-makes-a-serial-bomber-tick/556922/ [https://perma.cc/5UDD-PE99].

137. Motion for Limited Unsealing for Multiple Search Warrant Affidavits, at 1–2, *In re* Search of Sources and Locations Related to the Austin Bombings of 2018, No. 18-MJ-168 (W.D. Tex. Jan. 10, 2019).

138. *See infra* text accompanying notes 194–208.

139. Response to Rule 17 Subpoena attach. B at 2, United States v. Chatrie, 590 F. Supp. 3d 901 (E.D. Va. 2022) (No. 19-CR-130) [hereinafter Google Legal Investigations Lead Declaration].

140. People's Reply, *Seymour*, *supra* note 3, at 2–3.

In this three-step process, Google first strips away identifying information on users and devices responsive to the keyword or geofence warrant and produces a list ordered by assigned numbers.[141] Investigators then review the list of anonymized devices and rule out devices that are unlikely suspects, for example because their IP address shows them to be in a different state at the time of the crime.[142] After the deidentified list of devices is thus narrowed to the main suspects, investigators can seek identifying information.[143]

Why are keyword warrants sealed? As illustrated by the few publicly available examples, keyword warrants typically contain the targeted victim's home address or name, as well as the names of relatives.[144] The utility of the keyword search is greatest when the victim is not a public figure or the address is not a public place so there would be little reason to search for the name or address besides planning for a crime.[145] Release of the victim's name and address can feel like a revictimization or continuing amplification of the harm of the crime.[146] The brief revelations of the minor's name in the sexual abuse and trafficking case is illustrative of the sensitive and potentially damaging nature of public disclosure.[147] The Austin serial pipe bombings also dramatically illustrate another reason for filing warrants under seal: to avoid jeopardizing a pending investigation.[148] For continuing crimes, investigators may be concerned that perpetrators may erase or conceal their digital trails if alerted to keyword search terms that investigators are monitoring or strategies that they are pursuing.[149]

---

141. *See* Google Legal Investigations Lead Declaration, *supra* note 139, attach B. at 2–3 (describing the first step of the three-step process used for geofence warrants).

142. People's Reply, *Seymour*, *supra* note 3, at 3.

143. *Id.*

144. *E.g.*, Google Keyword Warrant 1, Pipe Bombings, *supra* note 12, at 4 (keyword warrant application involving variations of the targeted homes' addresses); People's Response, Cell Phone Data, *Seymour*, *supra* note 27, at 2 (summarizing keyword warrant search terms for the Diol family address where arson-murders occurred); Brewster, *supra* note 19 (describing keyword warrant in sexual abuse and trafficking case that included the names of the minor victim and her mother).

145. *See, e.g.*, Microsoft Keyword Warrant, Pipe Bombings, *supra* note 115, at 10 (explaining that the pool of people searching for a residential address targeted is likely small because it is not a public place such as a business).

146. *See* Mary Fan, *Adversarial Justice's Casualties: Defending Victim-Witness Protection*, 55 B.C. L. REV. 775, 777–78, 785–86 (2014) (explaining how the adversarial process can aggravate harms suffered by victims).

147. *See* Brewster, *supra* note 19 (discussing concerns that the mistaken disclosure revealed the minor's name in the kidnapping, sexual abuse, and trafficking investigation).

148. *See, e.g.*, Brendan J. Lyons, *Search Warrants Are Rarely Unsealed. Here's Why*, TIMES UNION (Aug. 12, 2022, 3:09 PM), https://www.timesunion.com/state/article/Why-search-warrants-rarely-unsealed-17369233.php [https://perma.cc/XH7V-JUMU] (explaining that warrants are rarely unsealed while an investigation is pending).

149. *See, e.g.*, *In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 67 n.1 (D.D.C. 2021) ("The Court granted the government's request to seal the warrant

There are troubling costs to secrecy, however. Privacy advocates and defense attorneys are deeply concerned that the secretive nature of keyword warrants prevents effective challenge and regulation.[150] Keyword warrants vary dramatically in the breadth of their requests.[151] For example, a keyword warrant seeking a nonpublic victim's address targeted in a pipe bombing is much narrower in scope than a keyword warrant seeking any users who searched for various combinations of words relating to pipe bombs and packages.[152] To effectively analyze and challenge law enforcement requests, it is important to know what exactly investigators are seeking. To evaluate the potential costs and benefits of an investigative tactic, it is important to know how many people's search histories are revealed in a keyword warrant and what results investigators obtain—including whether serial bombers, murderers, or child sex traffickers were apprehended because of a keyword warrant. The dearth of data is troubling in a democratic society where there should be public deliberation over whether the benefits of police tactics are worth their costs, including the potential privacy impact on uninvolved third parties.[153]

*2. The Rise of Geofence Warrants.*—Do you sometimes go somewhere even your parents and best friends do not know? Even if your closest loved ones do not know your movements, at least one major tech company likely has your trail. Because of the widespread popularity of Google services and products, Big Tech company Google is the motherlode of location data, among other information.[154] Google amasses location information in its Sensorvault and linked databases when you use Google apps, perform a mobile search using Google, or use a device running the Android operating

application because the criminal investigation is not public and revealing the existence of the warrant could adversely impact the government's investigation, including by causing the subjects of the investigation to flee or destroy evidence.").

150. *E.g.*, *Geofence Warrants and the Fourth Amendment*, *supra* note 43, at 2514; Schladebeck, *supra* note 114 (quoting Jennifer Granick, surveillance and cybersecurity counsel at the American Civil Liberties Union).

151. *See infra* subpart II(A).

152. *Compare* Google Keyword Warrant 2, Pipe Bombings, *supra* note 125, at 2 (keyword warrant for targeted addresses), *with* Google Keyword Warrant 3, Pipe Bombings, *supra* note 134, at 2 (keyword warrant for terms related to pipe bombs).

153. *See, e.g.*, Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1846 (2015) (discussing the need for democratic deliberation over rules governing policing); David Alan Sklansky, *Police and Democracy*, 103 MICH. L. REV. 1699, 1802 (2005) (discussing the need for greater attention to structures of democratic oversight over policing).

154. United States v. Chatrie, 590 F. Supp. 3d 901, 907–11 (E.D. Va. 2022); *In re* Search Warrant Application for Geofence Location Data Stored at Google, 497 F. Supp. 3d 345, 350–51 (N.D. Ill. 2020).

system.[155] About 97% of the smartphones in the world either use Google applications, or the Android operating system, or both.[156] Three Google apps—Gmail, Google search, and Google Maps—are among the top five most used smartphone apps in the United States as of June 2023.[157] Google held 94.92% of the market for searches via mobile phones in April 2023.[158] Nearly half of U.S. smartphones—about 45.8% in July 2023—run on the Android operating system by Google.[159]

Google maintains that users must opt in to location history and location reporting for location data to be stored.[160] Yet investigative reports, confirmed by Princeton researchers, found that some Google apps, such as Google Maps, store your time-stamped location information even without your opting into sharing the data.[161] A consumer protection lawsuit by the Arizona Attorney General alleges that Google gathers location information to help sell ads through settings such as Web & App Activity even when the location history settings are set to off.[162] A private company knows way more about your personal preferences, movements, and even potentially intimate behaviors than the government.[163]

Google's location data is significantly more precise than cell site location information obtained from telecommunications companies such as AT&T, Verizon, or T-Mobile.[164] Cell site location information data is

155. *Chatrie*, 590 F. Supp. 3d at 907–10; United States v. Smith, No. 21-CR-107, 2023 WL 1930747, at *2 (N.D. Miss. Feb. 10, 2023).

156. *In re* Search of Info. Stored at Premises Controlled by Google, No. 20 M 297, 2020 WL 5491763, at *3 (N.D. Ill. July 8, 2020).

157. L. Ceci, *Mobile Audience Reach of Leading Smartphone Apps in the United States in June 2023*, STATISTA (August 29, 2023), https://www.statista.com/statistics/281605/reach-of-leading-us-smartphone-apps/ [https://perma.cc/W9RW-NDQ2].

158. Tiago Bianchi, *Market Share of the Leading Mobile Search Engines in the United States from January 2018 to April 2023*, STATISTA (May 22, 2023), https://www.statista.com/statistics/511358/market-share-mobile-search-usa/ [https://perma.cc/4VGH-UXWH].

159. Statista Rsch. Dep't, *Subscriber Share Held by Smartphone Operating Systems in the United States from 2012 to 2023*, STATISTA (Oct. 4, 2023), https://www.statista.com/statistics/266572/market-share-held-by-smartphone-platforms-in-the-united-states/ [https://perma.cc/9ZJR-NW27].

160. Brief of Amicus Curiae Google LLC in Support of Neither Party at 7–8, *Chatrie*, 590 F. Supp. 3d 901 (No. 19-CR-130) [hereinafter Google's *Chatrie* Amicus Brief].

161. Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, ASSOCIATED PRESS (Aug. 13, 2018, 10:15 PM), https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb [https://perma.cc/4SAF-E9MQ].

162. Complaint for Injunctive and Other Relief at 2, State *ex rel.* Brnovich v. Google LLC, No. CV2020-006219 (Ariz. Super. Ct. May 27, 2020).

163. *See* Fan, *supra* note 10, at 1440–41 (discussing the massive pool of consumer data collected by companies).

164. *In re* Search Warrant Application for Geofence Location Data Stored at Google, 497 F. Supp. 3d 345, 360 (N.D. Ill. 2020); Harris, *supra* note 18.

generated when cell phones ping nearby cell towers to obtain signal from the company's wireless network.[165] A person's location can be triangulated from the cell towers that the phone pings, but the accuracy is approximated to within three-quarters of a mile—thousands of meters or multiple city blocks.[166] In contrast, Google's location history function estimates a user's location using Wi-Fi access points, Bluetooth beacons, and GPS data and can be accurate to within a few meters or even square feet, depending on the location.[167]

Even assuming, as Google maintains, that a user must have location history enabled and sign into a Google account on the device,[168] about one-third of users have location history enabled to use services such as real-time traffic updates to find time-saving routes.[169] According to disclosures made in litigation, there were 592 million location history users in 2018.[170] For at least fourteen years, Google has collected and stored a gold mine of user location data to enable targeted advertising—including geofence-based marketing that advertises based on location—which generates billions in revenue annually.[171]

In the rapid evolution of digital forensic strategies to trace suspects using data rather than labor-intensive physical stakeouts, geofence warrants are eclipsing the allure of cell site location information.[172] The term geofence refers to the perimeter drawn around an area of interest using geolocation coordinates.[173] Companies use geofences to send targeted advertising as part of a $32 billion industry.[174] Law enforcement officers use geofences to define the area around a crime inside which suspects were likely to be at the time of

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

166. Harris, *supra* note 18; Brief of Amici Curiae Technology Law and Policy Clinic at New York University School of Law & Electronic Frontier Foundation in Support of Defendant–Appellant at 8, United States v. Chatrie, No. 22-4489 (4th Cir. Jan. 27, 2023).

167. Criminal Complaint attach. at 2, United States v. Rhine, No. 21-MJ-646 (D.D.C. Nov. 4, 2021); Doug Austin, *Google Geofence Data Identified 5,723 Devices Near January 6th US Capitol Attack: Data Privacy Trends*, EDISCOVERY TODAY (Dec. 2, 2022), https://ediscoverytoday.com/2022/12/02/google-geofence-data-identified-5723-devices-near-january-6th-us-capitol-attack-data-privacy-trends/ [https://perma.cc/ZL8N-YL4L]; Lynch, *supra* note 18.

168. Google's *Chatrie* Amicus Brief, *supra* note 160, at 7–8.

169. Austin, *supra* note 167.

170. Motion to Suppress, *Seymour*, *supra* note 23, at 4.

171. Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/T3S7-RLCU].

172. Google's *Chatrie* Amicus Brief, *supra* note 160, at 3.

173. United States v. Asghedom, 992 F. Supp. 2d 1167, 1169 (N.D. Ala. 2014), *aff'd*, 646 F. App'x 830 (11th Cir. 2016).

174. Yi-Jen (Ian) Ho, Sanjeev Dewan & Yi-Chun (Chad) Ho, *Distance and Local Competition in Mobile Geofencing*, 31 INFO. SYS. RSCH. 1421, 1421–22 (2020).

the crime.[175] A geofence warrant requests companies like Google to share their data on devices present within the geofenced zone around a crime at the time of its commission.[176] A powerful tool for when the fact that a crime was committed is known but the suspects are unknown, geofence warrants particularize "the physical area and the time range in which there is probable cause to believe that criminal activity occurred."[177]

Before the rise of geofence warrants, law enforcement officers sought cell site location information through two main strategies.[178] Subpoenas or warrants for historical cell site location information generally seek to track a suspect's movements through his phone's connection with cell towers.[179] A "tower dump" seeks all devices that connected to a cell tower within a window of time when a crime or crimes were perpetrated.[180] As further discussed in subpart I(B), the Supreme Court in *Carpenter v. United States*[181] ruled that police need a warrant based on probable cause to obtain seven days or more of a suspect's historical cell site location information because such prolonged tracking intrudes on reasonable expectations of privacy and is a Fourth Amendment-regulated search.[182] The *Carpenter* majority expressly declined to rule on whether the Fourth Amendment's warrant and probable cause protections apply at all to government requests to phone companies for cell site location information of less than seven days in length, or to tower dumps, which usually span only minutes or hours rather than days.[183] In the half-decade since *Carpenter*, the Supreme Court has not revisited the open questions. Meanwhile, police stratagems have far outpaced the glacial pace of appellate decisions, especially the certiorari-based review of the highest court.

The same year the Supreme Court issued *Carpenter*, in 2018, the FBI pursued its first geofence warrant to solve a series of robberies in Portland, Maine.[184] The geofence warrant asked Google to access its Sensorvault location database to determine if any phone was present near at least two of the nine robberies, using a thirty-minute window for each crime.[185] Google

175. United States v. Rhine, 652 F. Supp. 3d 38, 66–67 (D.D.C. 2023).

176. *In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 69 (D.D.C. 2021).

177. *Rhine*, 652 F. Supp. 3d at 66–67 (citing *In re Search of Info. Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d at 69).

178. *In re Search of Info. Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d at 68.

179. Carpenter v. United States, 138 S. Ct. 2206, 2211–12 (2018).

180. *Id.* at 2220.

181. 138 S. Ct. 2206 (2018).

182. *Id.* at 2217 n.3, 2220.

183. *Id.*

184. Elm, *supra* note 16, at 8.

185. *Id.*

refused to release the data.[186] Ultimately, FBI investigators identified suspects through other means instead, including highway toll pass records, DNA, and shoeprints.[187]

Other agencies sought geofence warrants from magistrate judges with more success to solve murders and sexual assaults, among other crimes.[188] The number of geofence warrants to Google rose by 1,500% between 2017 and 2018 and another 500% between 2018 to 2019.[189] In 2020, Google received more than 11,554 geofence warrants, and by 2021, geofence warrants constituted nearly a quarter of all warrants served on Google.[190]

Initially, investigators framed geofence warrants similarly to tower dump requests, simply asking for all Google users at a crime site within the relevant time frame.[191] Google argued that the geofence warrant requests were more intrusive than cell site location information or tower dumps because cell site location information requests are focused on a particular mobile device and tower dumps request the connection records for a particular tower within a set time interval.[192] In contrast, to respond to a geofence warrant request, Google must search the location histories of all users during the requested time frame to see if any were present in the area specified in the geofence warrant.[193]

Google developed a three-step protocol that included deidentification and narrowing of user information to respond to geofence warrants.[194] Google adopted a policy of objecting to any warrant that did not contain the deidentification and narrowing measures in its protocol, thereby leveraging litigation and delay costs to incentivize law enforcement compliance with the three-step process.[195] In the first step, Google strips account-identifying information from devices present at the time and place specified by the warrant.[196] In this "production version" of the data, Google gives law

186. Thomas Brewster, *To Catch a Robber, the FBI Attempted an Unprecedented Grab for Google Location Data*, FORBES (Aug. 15, 2018, 9:00 AM), https://www.forbes.com/sites/thomasbrewster/2018/08/15/to-catch-a-robber-the-fbi-attempted-an-unprecendeted-grab-for-google-location-data [https://perma.cc/F4XM-TFWJ].

187. *Id.*

188. Elm, *supra* note 16, at 8.

189. Google's *Chatrie* Amicus Brief, *supra* note 160, at 3.

190. *In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 68 n.3 (D.D.C. 2021).

191. Google Legal Investigations Lead Declaration, *supra* note 139, attach B. at 2; Google's *Chatrie* Amicus Brief, *supra* note 160, at 12.

192. Google's *Chatrie* Amicus Brief, *supra* note 160, at 14.

193. *Id.*; Google Legal Investigations Lead Declaration, *supra* note 139, attach B. at 2.

194. Google Legal Investigations Lead Declaration, *supra* note 139, attach. B at 2.

195. *Id.*

196. *Id.* attach. B at 2–3.

enforcement an assigned device number not associated with any account, "the latitude/longitude coordinates and timestamp of the stored LH [location history] information, the map's display radius, and the source of the stored LH information (that is, whether the location was generated via Wi-Fi, GPS, or a cell tower)."[197] The number of devices disclosed varies dramatically between cases, depending on the type of geographic area, time of day, number of perpetrators, and length of time requested.[198]

The protocol may be adapted to filter out suspect devices.[199] For example, in the investigation of the U.S. Capitol riots on January 6, 2021, in which objectors stormed the U.S. Capitol to disrupt certification of the Presidential election, Google produced three lists of deidentified devices at step one.[200] The geofence parameters specified for all three lists was "a target area slightly larger than but roughly tracing the contours of the Capitol building itself, excluding most of the plazas and lawns on both sides of the building and the abutting streets."[201] To winnow out rioters who converged in the afternoon between 2:00 and 6:30 PM from people who work at the Capitol, the government obtained at step one three deidentified lists: (1) a primary list of people present between 2:00 and 6:30 PM, the time of the riots; (2) a control list for the time range of 12:00 to 12:15 PM; and (3) another control list for 9:00 to 9:15 PM.[202] In addition there may be more than one production list if the company's database is updated with more data after an early initial inquiry: for example, the data "as it existed in the evening of January 6, 2021" contained 5,716 devices, but by the morning of January 7, 2021, the list numbered 5,721 devices.[203] The number of devices detected also may decrease if users later delete their location history data from the Google database: for example, seventy devices had deleted their data by January 13, 2021.[204]

In the second step, the government reviews the deidentified data and determines devices of potential interest.[205] To determine whether a device should be eliminated or retained from the suspect list, investigators can compel additional location coordinates to determine if the device was moving

197. *Id.* attach. B at 3.

198. *Id.*

199. United States v. Rhine, 652 F. Supp. 3d 38, 68–69 (D.D.C. 2023).

200. *Id.*

201. *Id.*

202. *Id.* at 68–69, 84; *see also id.* at 84 ("The absence of similar narrowing mechanisms was a significant factor motivating the rejection of the geofence warrants in *Chatrie*, *Pharma I*, *Pharma II*, and *Kansas*.").

203. *Id.* at 69.

204. *Id.* at 70.

205. Google Legal Investigations Lead Declaration, *supra* note 139, attach. B at 4.

in a manner consistent with perpetrating the crime or just passing through.[206] Finally, in the third step, if the warrant authorizes the production of account-identifying information, the government can compel Google to produce subscriber information for devices deemed relevant, such as the email addresses and name associated with the account.[207] The aim of the self-imposed discretionary protocol is to reduce disclosures regarding uninvolved parties and thereby reduce potential privacy harms to consumers.[208]

### *B. Evolving Technologies and Originalist Nostalgia*

Keyword and geofence warrants epitomize the kinds of modern-day technological strategies that fall into uncharted constitutional terrain, far outpacing the glacial churn of the Supreme Court's Fourth Amendment precedents.[209] A longstanding paradox of civil liberties and policing is that legislatures have left many vital questions for courts to tackle, in the form of interpreting the fifty-four words of the Fourth Amendment, which protects against unreasonable searches and seizures.[210] Legislatures are better suited for crafting laws addressing the complexities of technologies and balancing democratic views about the competing interests at stake.[211] Because the fierce politics of crime and safety impede legislative regulation on key matters, however, courts have reluctantly and awkwardly entered the gap in the form of interpreting the Fourth Amendment.[212] This subpart frames the challenges of applying Fourth Amendment doctrine to evolving technological strategies, epitomized by rulings on keyword and geofence warrants, and the resulting confusion and originalist nostalgia in the courts and pending litigation.

---

206. *Id.*

207. *Id.*

208. *Id.* attach. B at 2.

209. *See, e.g.*, United States v. Chatrie, 590 F. Supp. 3d 901, 926 (E.D. Va. 2022) (explaining that geofence warrants don't "fit neatly within the Supreme Court's existing . . . doctrine as it relates to technology," which "primarily deals with *deep*, but perhaps not *wide*, intrusions into privacy").

210. U.S. CONST. amend. IV; *see, e.g.*, BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 16 (2017) (discussing the democratic failure to enact laws and regulations giving guidance to police).

211. *Chatrie*, 590 F. Supp. 3d at 926–27; Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 806 (2004). *But see* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 773 (2005) ("In the context of crafting rules to regulate law enforcement and new technologies, I am not convinced that either the legislatures or the courts have strong advantages over the other.").

212. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 51 (2001) (Stevens, J., dissenting) ("It would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues rather than to shackle them with prematurely devised constitutional constraints.").

*1. Technological Gaps in Fourth Amendment Doctrine*.—As a threshold matter, the Fourth Amendment's protection against unreasonable searches and seizures and warrant requirements only apply to searches and seizures by government actors.[213] The amendment's protection requiring police to get a warrant based "upon probable cause . . . particularly describing the place to be searched, and the persons or things to be seized" only applies if the investigative tactic constitutes a search or seizure under the Fourth Amendment—and not just our ordinary lay conceptions.[214] Fourth Amendment searches are defined as either an incursion on a reasonable expectation of privacy or a trespass, which means physically occupying the suspect's property to gather information.[215] Because many technological tactics entail no need for a physical trespass on a suspect's device or other property, the main analytical question often is whether the police action constitutes an incursion on a reasonable expectation of privacy.[216]

Because of the Supreme Court's third-party exposure doctrine, there is no reasonable expectation of privacy under the Fourth Amendment and thus no search if the government gets information shared with a third party.[217] Therefore, the Fourth Amendment does not apply to police requests for data such as our call records from phone companies[218] or financial transaction history from banks.[219] Congress can frame legislative protections for financial or other data, but police do not need a warrant nor probable cause to obtain the information shared with these business third parties because the Fourth Amendment does not apply.[220] If the business does not voluntarily share the data, the government can compel the data in compliance with

213. City of Ontario v. Quon, 560 U.S. 746, 755–56 (2010) (quoting Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 613–14 (1989)).

214. U.S. CONST. amend. IV; *see* Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 120–22 (2002) (laying out two questionable moves made by the Supreme Court in framing third-party doctrine and thereby what constitutes a search for purposes of the Fourth Amendment).

215. *See* Florida v. Jardines, 569 U.S. 1, 11 (2013) ("The *Katz* reasonable-expectations test 'has been *added to*, not *substituted for*,' the traditional property-based understanding of the Fourth Amendment, and so is unnecessary to consider when the government gains evidence by physically intruding on constitutionally protected areas." (quoting United States v. Jones, 565 U.S. 400, 409 (2012))).

216. *See, e.g.*, Jonathan Turley, *Anonymity, Obscurity, and Technology: Reconsidering Privacy in the Age of Biometrics*, 100 B.U. L. REV. 2179, 2195 (2020) (discussing biometric technology as an example where "there is no need to trespass or attach devices to private property").

217. United States v. Miller, 425 U.S. 435, 443 (1976) (citing United States v. White, 401 U.S. 745, 751–52 (1971)).

218. Smith v. Maryland, 442 U.S. 735, 742 (1979).

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

220. *Id.*; *Smith*, 442 U.S. at 742; *see also, e.g.*, McDonough v. Widnall, 891 F. Supp. 1439, 1447 (D. Colo. 1995) (discussing how Congress passed the Right to Financial Privacy Act at 12 U.S.C. § 3401 *et seq.* in response to the privacy void created by *United States v. Miller*).

statutory regimes, such as the Electronic Communications Privacy Act, which requires a subpoena or court order depending on the type of information requested.[221] The information can be compelled on a standard lower than probable cause, based on mere relevance and materiality to an ongoing criminal investigation.[222]

The third-party exposure doctrine is heavily criticized because it often diverges from the average person's desires for privacy and does not reflect empirical reality.[223] The third-party exposure doctrine is particularly anachronistic to apply in an era where cell phones are virtually an organ or extended brain on our bodies, and we share vast volumes of data with companies like Google, YouTube, Microsoft, Verizon, and T-Mobile.[224] Are there any limits to the data held by private companies that the government can compel with a simple subpoena? The U.S. Supreme Court's main foray into cutting back the third-party exposure doctrine for the vast volumes of data that private companies hold came in *Carpenter v. United States*.[225] *Carpenter* addressed what the Fourth Amendment requires when the government seeks cell site location data from wireless telecommunications carriers.[226]

*Carpenter* involved a more traditional kind of investigation because the police had known suspects and phone numbers, implicated by their co-conspirator in a series of armed robberies.[227] Rather than obtaining a warrant based on probable cause, the police officers obtained a magistrate judge's order under 18 U.S.C. § 2703(d), which permits compelled disclosure of telecommunications records when there are reasonable grounds to believe that the records are relevant and material to an ongoing criminal investigation.[228] While a § 2703(d) order is issued by a magistrate judge, the low relevance and materiality standard is similar to that for a subpoena and short of probable cause.[229] The first § 2703(d) order sought cell-site records

221. Josh Goldfoot, *Compelling Online Providers to Produce Evidence Under ECPA*, U.S. ATT'YS' BULL., Nov. 2011, at 35, 35–37.

222. 18 U.S.C. § 2703(c)(2), (d).

223. *E.g.*, William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1872 (2016); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases*, 42 DUKE L.J. 727, 732, 740 (1993). *But see, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 n.5, 564 (2009) (collecting criticisms before defending the doctrine).

224. *Cf.* Riley v. California, 573 U.S. 373, 385 (2014) (noting that modern cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy").

225. 138 S. Ct. 2206 (2018).

226. *Id.* at 2211–12.

227. *Id.* at 2212.

228. *Id.*; 18 U.S.C. § 2703(d).

229. 18 U.S.C. § 2703(d).

spanning 152 days from MetroPCS.[230] The second § 2703(d) order sought records spanning seven days from Sprint.[231]

Under the customary third-party exposure doctrine, obtaining data shared with Sprint and MetroPCS would not be a Fourth Amendment search, so the warrant and probable cause requirements would not apply.[232] The Supreme Court revised the third-party exposure doctrine, however, for "the unique nature of cell phone location records," which when amassed over a prolonged period can give "an all-encompassing record of the holder's whereabouts."[233] Cell phones are special, the Supreme Court has repeatedly explained, because they are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[234] *Carpenter* ruled that the customary third-party exposure doctrine in precedents on bank or call records had to adapt to the "seismic shifts in digital technology" that makes tracking anyone—and even everyone—for prolonged periods feasible and far less costly than the gumshoe days of physical police tails.[235]

In a "narrow" and caveated holding that explicitly leaves important questions unanswered, the *Carpenter* majority held that investigators need to get a warrant based on probable cause to obtain location information spanning seven or more days.[236] The Supreme Court declined to explain whether obtaining business records of data for periods shorter than seven days is governed by the Fourth Amendment at all—or if the third-party exposure doctrine applies.[237] The *Carpenter* majority emphasized the decision was "narrow" and offered no view on real-time cell site location tracking nor on tower dumps, which reveal all devices that connected to a cell phone tower at a certain time.[238]

To show how fast technological strategies advance, even tower dumps, which the Supreme Court explicitly declined to address, are potentially passé with the surging popularity of geofence and keyword warrants. Keyword and geofence warrants fall in the murky morass of unanswered questions and conflicting signals in *Carpenter* that can be mined by litigants on both sides. On the one hand, *Carpenter* recognized the problematic and fictive nature of

230. *Carpenter*, 138 S. Ct. at 2212.

231. *Id.*

232. *See id.* at 2216 (acknowledging "the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of *Smith* and *Miller*").

233. *Id.* at 2217.

234. *Id.* at 2220 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

235. *Id.* at 2219.

236. *Id.* at 2217 n.3, 2220.

237. *Id.* at 2217 n.3.

238. *Id.* at 2220.

the third-party exposure doctrine in an age where we share vast volumes of data with businesses.[239] On the other hand, *Carpenter* left intact third-party exposure precedents holding that it is not a Fourth Amendment search for the government to obtain financial or phone records.[240] Moreover, *Carpenter* explicitly left largely intact longstanding practice, explaining: "The Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations. We hold only that a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party."[241]

Keyword and geofence warrants present new permutations of questions not presented with the historical cell site location data and § 2703(d) court orders based on mere relevance in *Carpenter*.[242] First, keyword and geofence warrants tend to be entryway strategies to crack cases where a crime has been committed but the perpetrator is unknown.[243] In contrast, with the cell site location data in *Carpenter*, as with tower dumps, investigators are seeking data on a known, discrete suspect.[244] Second and relatedly, because there is no discrete, named suspect, in order to find responsive data, companies responding to a geofence or keyword warrant must initially search through the data of all users who fit the requested time, place, and keyword parameters.[245] Third, unlike the failure to obtain a warrant based on probable cause in *Carpenter*, investigators do get a warrant based on probable cause, particularizing the data police seek with keyword and geofence warrants.[246] The legal complexity that is spurring litigation is whether the nature of the probable cause and particularity in keyword and geofence warrants satisfies the Fourth Amendment—and whether the Fourth Amendment even applies at all to the data requested from businesses.[247]

*2. The Perils of Originalist Nostalgia and General Warrants Analogies.*—Unlike typical warrants, which name a suspect and his items to be searched, a geofence or keyword warrant specifies a time frame and crime

239. *Id.* at 2217–19.

240. *Id.* at 2220.

241. *Id.* at 2222.

242. *See* United States v. Chatrie, 590 F. Supp. 3d 901, 926 (E.D. Va. 2022) ("As this Court sees it, analysis of geofences does not fit neatly within the Supreme Court's existing 'reasonable expectation of privacy' doctrine as it relates to technology.").

243. *See supra* sections I(A)(1)–(2).

244. *See Carpenter*, 138 S. Ct. at 2212 (seeking cell site location information for several accomplices identified by a man who confessed to a series of robberies).

245. *See supra* text accompanying notes 196–97.

246. *See, e.g.*, Oral Ruling, *Seymour*, *supra* note 4, at 25–26 (discussing probable cause and particularity of the keyword warrant).

247. *See infra* subpart II(A).

scene coordinates or keywords.[248] Suspects are not named because the point of keyword and geofence warrants is to identify the unknown suspect of a known crime using the parameters specified in the warrant.[249] The geofence and keyword warrants establish that there is probable cause of three varieties: (1) to believe there was a crime, (2) that the business has evidence that would identify the perpetrator of the crime, and (3) that the location and time parameters for geofence warrants or word search and timeframe parameters for keyword warrants will yield evidence of the crime.[250]

As litigation of geofence warrants increases, the lack of a named suspect has roused repeated arguments likening geofence warrants to the hated 1700s-era general warrants that occasioned the framing of the Fourth Amendment.[251] The main litigated keyword warrant case also raised a constitutional challenge relying on an analogy to general warrants.[252] Almost all of the emerging scholarship on geofence warrants and the comment on keyword warrants also make the general warrants claim.[253]

While alluringly wrapped in the Romantic Luddism of contemporary originalism, the attempt to analogize keyword and geofence warrants to general warrants from the founding era is inapposite and anachronistic. Beyond the obvious lack of an analogy from a time before electric power to digital data amassed from cell phones and apps by Big Tech companies, general warrants required neither probable cause nor magistrate judge review.[254] In contrast, geofence and keyword warrants are based on three types of probable cause and magistrate judge review.[255] Moreover, as further discussed below, the argument, wrapped in seeming originalist robes, also fails on the originalist interpretation of the Fourth Amendment advanced by

248. *See supra* sections I(A)(1)–(2).

249. *See supra* sections I(A)(1)–(2).

250. *See* Oral Ruling, *Seymour*, *supra* note 4, at 25–26 (noting (1) that the culprits of known arson-murders (2) likely searched for the victims' address and (3) that the keyword warrant parameters were tailored such that the returns would likely help identify the culprit); *In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 77–79 (D.D.C. 2021) (noting (1) that the culprits of a known crime (2) were likely communicating location data to Google via their phones and (3) that the geofence warrant parameters were tailored such that the returns would likely help identify the culprit).

251. *E.g.*, Brief of Amicus Curiae Electronic Frontier Foundation in Support of Gavin Seymour's Petition for Review at 3, People v. Seymour, 536 P.3d 1260 (Colo. 2023) (No. 2023SA12).

252. Motion to Suppress, *Seymour*, *supra* note 23, at 1–3, 11, 17.

253. Amster & Diehl, *supra* note 43, at 434; Edano, *supra* note 41, at 989–91, 995; *Geofence Warrants and the Fourth Amendment*, *supra* note 43, at 2511; De La Torre, *supra* note 43, at 339; Owsley, *supra* note 43, at 863.

254. *See, e.g.*, Wilkes v. Wood (1763) 98 Eng. Rep. 489, 490 (explaining that general warrants were a license to enter homes "upon any frivolous or no pretence at all").

255. *See supra* text accompanying note 250.

at least two of the major originalists on the contemporary Supreme Court: Justices Clarence Thomas and Neil Gorsuch.[256]

Originalism is a method of constitutional exegesis that seeks the answer to contemporary controversies based on the original meaning of constitutional text framed by the Founders.[257] The rise of originalism is relatively new in the long arc of constitutional interpretation, becoming influential as part of the backlash against the expansion of civil rights and liberties by the Warren Court and under the influence of Justices Antonin Scalia, William Rehnquist, Clarence Thomas, and now Neil Gorsuch and sometimes Samuel Alito.[258] The emphasis on history by originalists has longer roots in constitutional interpretation and is ascendant with originalism's rise.[259]

Originalist readings of the Fourth Amendment often hearken back to the "founding generation's" concern with "the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[260] Used in England through the 1700s, general warrants were a license to search wherever they wanted—and potentially target political dissidents—without even reasonable suspicion much less probable cause.[261] In the American colonies, a species of general warrants called writs of assistance similarly permitted "all and singular justices, sheriffs, constables, and all other officers and subjects" to enter any colonial home to search for goods smuggled past the Crown's customs taxes.[262] Opposition to the general warrants roused riots in the colonies and were included in the Petition to King

256. *See infra* text accompanying notes 285–93.

257. Antonin Scalia, *Originalism: The Lesser Evil*, 57 U. CIN. L. REV. 849, 852 (1989); Donohue, *supra* note 44, at 1182–83.

258. Donohue, *supra* note 44, at 1182–84.

259. Sklansky, *supra* note 44, at 1762–64.

260. Carpenter v. United States, 138 S. Ct. 2206, 2251 (2018) (Alito, J., dissenting) (quoting Riley v. California 573 U.S. 373, 403 (2014)); *see also* Virginia v. Moore, 553 U.S. 164, 168–69 (2008) ("The immediate object of the Fourth Amendment was to prohibit the general warrants and writs of assistance that English judges had employed against the colonists."); Ferguson, *supra* note 43, at 4, 6–14 (drawing an anti-"rummaging" principle from the founding generation's distaste for general warrants).

261. Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 YALE J.L. & TECH. 120, 123 (2007); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1334 (2012); Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 296–97 (1993); Levy, *supra* note 43, at 82.

262. James Otis, Against Writs of Assistance, Oral Argument Before the Massachusetts Superior Court (Feb. 24, 1761), https://www.sas.upenn.edu/~cavitch/pdf-library/Otis_Against%20Writs.pdf [https://perma.cc/FB6D-CCJA].

George III listing the colonists' grievances.[263] The founding-era colonists objected to the King: "The officers of the customs are impowered [sic] to break open and enter houses, without the authority of any civil magistrate founded on legal information."[264]

A landmark 1763 case against general warrants that influenced the founders who framed the Fourth Amendment was *Wilkes v. Wood*.[265] *Wilkes* involved the execution of a general warrant against Parliament member John Wilkes, a vociferous critic of King George III.[266] Wilkes filed a trespass suit against Robert Wood, who joined the King's messengers and a constable in searching Wilkes's home.[267] Counsel for Wilkes argued that the civil liberties of all Englishmen were at stake because at issue was whether homes could be "entered, upon any frivolous or no pretence at all, by a Secretary of State."[268] In a celebrated decision, the jury in the case found the search pursuant to the general warrant illegal and issued a thousand-pound damages verdict for Wilkes.[269]

The originalist's celebrity, Justice Scalia, wrote in 1993 that the Fourth Amendment's purpose is "to preserve that degree of respect for the privacy of persons and the inviolability of their property that existed when the provision was adopted."[270] Justice Scalia first framed the view that the Fourth Amendment's aim is to freeze the original status quo in a concurrence that begins with the originalist's creed: "I take it to be a fundamental principle of constitutional adjudication that the terms in the Constitution must be given the meaning ascribed to them at the time of their ratification."[271] In the Supreme Court's Fourth Amendment decisions wrestling with technological evolution decades later, Justice Scalia's declaration became a majority refrain.[272] Writing for the majority in *Kyllo v. United States*,[273] Justice Scalia invalidated the warrantless use of a thermal imager to detect suspicious heat emanating from a home, explaining: "This assures preservation of that degree

263. Petition to King George III, The First Continental Congress 3 (Oct. 20, 1774), https://www.masshist.org/database/viewer.php?item_id=663&mode=large&img_step=3#page3 [https://perma.cc/S7MQ-VDC3].

264. *Id.* at 3.

265. Wilkes v. Wood (1763) 98 Eng. Rep. 489; *see also, e.g.*, Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 772 (1994) (explaining that the Fourth Amendment "was undeniably designed to embody" the lessons of *Wilkes*).

266. *Wilkes*, 98 Eng. Rep. at 490, 493.

267. *Id.* at 489.

268. *Id.* at 490.

269. *Id.* at 499.

270. Minnesota v. Dickerson, 508 U.S. 366, 380 (1993) (Scalia, J., concurring).

271. *Id.* at 379.

272. *E.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001).

273. 533 U.S. 27 (2001).

of privacy against government that existed when the Fourth Amendment was adopted."[274] In *United States v. Jones*,[275] Justice Scalia, again writing for the majority, repeated the refrain with only slight variation in invalidating the use of a GPS tracking device affixed to a vehicle the suspect drove as a warrantless trespass on property.[276] Chief Justice Roberts took up Justice Scalia's refrain in his decision for the majority in *Carpenter v. United States* on cell site location information, writing: "[T]his Court has sought to 'assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[277]

The originalists on the Supreme Court write that contemporary controversies over what the Fourth Amendment requires should be answered by asking "whether a particular governmental action . . . was regarded as an unlawful search or seizure under the common law when the Amendment was framed."[278] Yet the reality is that there are no true analogues for our lives today, which could not even be envisioned in the science fiction of the eighteenth century. Leading scholars such as Christopher Slobogin have argued that originalism is a problematic interpretative methodology, especially in the criminal procedure context, in which there are no good historical analogues or accounts of analogues for contemporary controversies.[279] Of course, ludicrousness has not kept Justice Scalia from sometimes trying to imagine an originalist analogue—such as likening a GPS tracking device to a constable hiding in a wagon to track a suspect's movements.[280] An unusual coalition of Justices Alito, Ginsburg, Breyer and Kagan joined in noting the ridiculousness of Justice's Scalia's analogy, wryly noting, "this would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience."[281]

Preserving the same degree of privacy as the 1700s is also a Romantic fantasy in the digital age where Big Tech companies track our movements and online behaviors to target advertising and leverage the intimate thoughts

274. *Id.* at 29, 34.

275. 565 U.S. 400 (2012).

276. *Id.* at 404–06.

277. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (second alteration in original).

278. Wyoming v. Houghton, 526 U.S. 295, 299 (1999); *see also, e.g.*, Sklansky, *supra* note 44, at 1743–44 (noting the oddity of the approach and arguing that "[n]either the text nor the background of the Fourth Amendment suggests it aims merely to codify eighteenth-century rules of search and seizure").

279. Christopher Slobogin, *An Original Take on Originalism*, 125 HARV. L. REV. F. 14, 19 (2011).

280. *Jones*, 565 U.S. at 406 n.3.

281. *Id.* at 420 n.3 (Alito, J., concurring).

and prurient curiosities we type into search boxes.[282] A Bill of Rights that regulates only government actors misses much of the privacy impact of business big data and of our consumer choices and private actions, such as making security cameras so ubiquitous that the video can track a murderer from fleeing the scene of the crime to returning home.[283] Yet the nostalgic Luddism of Justice Scalia's declaration resonates even with readers without originalist sympathies.[284] We give our privacy away every day for far less weighty reasons than solving murders or bombings, yet we are wistful for the kind of privacy the Framers enjoyed.

The originalist-tinged effort to analogize keyword and geofence warrants to general warrants, besides being inapposite, also fails under the views of the two prime originalists on the current Supreme Court: Justices Thomas and Gorsuch.[285] With personnel changes and new alignments, Justice Thomas's vote has become increasingly decisive in cases, leading some to proclaim the contemporary Supreme Court effectively the "Thomas Court."[286] As the longest-serving member of the high court, Justice Thomas's influence and originalism pervades the judiciary beyond the Supreme Court, with the most former clerks appointed to the federal judiciary under the administration of former President Donald Trump.[287]

Justice Thomas's originalism, once viewed as anachronistic, is now rising[288]—and Justice Thomas rejects the claim that there is a protectible interest in our digital data held by businesses. In his *Carpenter* dissent, Justice Thomas delved extensively into founding history and Framers' intent and argued that the concern about general warrants was about rummaging in

282. *See, e.g.*, Nir Kshetri, *Big Data's Impact on Privacy, Security and Consumer Welfare*, 38 TELECOMM. POL'Y 1134, 1137 (2014) (discussing company use of consumer data to predict addictions, predilections, and other private intimate details).

283. *See supra* text accompanying notes 110–11; *see also* Farhang Heydari, *The Private Role in Public Safety*, 90 GEO. WASH. L. REV. 696, 750 (2022) (offering a parity lens for the private–public divide).

284. *See supra* text accompanying notes 85–97.

285. *See infra* text accompanying notes 289–91.

286. *See, e.g.*, Jill Abramson, *This Justice Is Taking Over the Supreme Court, and He Won't Be Alone*, N.Y. TIMES (Oct. 15, 2021), https://www.nytimes.com/2021/10/15/opinion/clarence-thomas-supreme-court.html [https://perma.cc/8FRR-PSP6] (positing that we may be "entering the era of the Thomas court"); James Romoser, *John Roberts Is the Chief. But It's Clarence Thomas's Court*, SCOTUSBLOG (Oct. 2, 2022, 7:00 PM), https://www.scotusblog.com/2022/10/john-roberts-is-the-chief-but-its-clarence-thomass-court/ [https://perma.cc/CPV7-8ARZ] (noting that Justice Thomas often "gets the last word").

287. Romoser, *supra* note 286; Orlando Mayorquin, *Who Is Clarence Thomas? What to Know About the Supreme Court's Longest Serving Justice*, USA TODAY (June 23, 2022, 12:13 PM), https://www.usatoday.com/story/news/politics/2022/04/03/supreme-court-justice-clarence-thomas-facts/7005948001/ [https://perma.cc/R96Q-BA2W].

288. Romoser, *supra* note 286.

a person's physical property—not someone's expectation of privacy.[289] From his originalist perspective, business records that collect data are not a suspect's papers within the original meaning of the Fourth Amendment and might not even be cognizable property.[290] The other major originalist on the Court, Justice Gorsuch, largely agreed and would return to an exclusively property-based approach.[291]

The *Carpenter* dissents of Justices Thomas and Gorsuch further underscore the mistake in the repeated attempts to argue that keyword and geofence warrants are general warrants abhorred by the Founders. If the Framers' understandings are the touchstone, then the proponent of this position must contend with Justice Thomas's apparent view that the Fourth Amendment does not apply at all to digital data because data is not "persons, houses, papers, and effects" as understood by the Framers.[292] It is logically impossible for the Framers to have contemplated digital data within the original meaning of those terms because nothing like the digital data troves of behemoth corporations like Google existed in the 1700s. Originalism may seem beguiling in its Romantic Luddism, particularly in Justice Scalia's version of preserving the degree of privacy that existed at the founding.[293] But originalism and the strains of Romantic Luddism sown in Fourth Amendment doctrine are not equipped to answer the complex questions presented by evolving technologies. A more nuanced approach is needed, informed by history where instructive but also filling the large gaps in contemporary constitutional procedure when it comes to evolving technologies and competing values.[294]

## II. Collateral Impact, Overbreadth, and Technological Exceptionalism

What is more terrifying: a SWAT team breaking down your door and armed officers detaining you while officers search your home because of something your housemate allegedly did[295] or Google disclosing to the government that your electronic device was one of nineteen in the vicinity of a bank and church at 4:52 PM, around the time a bank was robbed?[296]

289. Carpenter v. United States, 138 S. Ct. 2206, 2238–42 (2018) (Thomas, J., dissenting).

290. *Id.* at 2235, 2241–43, 2241 n.8.

291. *Id.* at 2267–68 (Gorsuch, J., dissenting).

292. *See supra* text accompanying notes 289–91.

293. *See supra* text accompanying notes 270–77.

294. *See infra* Part III.

295. *See* Muehler v. Mena, 544 U.S. 93, 95–96, 98 (2005) (upholding detention in cuffs by SWAT team during warrant execution of a person not suspected of the crime, a gang-related drive-by shooting, specified in the warrant).

296. *See* United States v. Chatrie, 590 F. Supp. 3d 901, 905, 926–27 (E.D. Va. 2022) (discussing geofence warrant radius and overbreadth concerns).

Both scenarios entail what this Article terms collateral impact to signify the effect of an investigative tactic on persons who are not the target of the investigation.[297] Collateral impact can result in collateral harm, such as the terror of armed law enforcement cuffing you and asking you about your immigration status during the execution of a warrant wholly unrelated to you or your immigration status.[298] The collateral impact may also result in low to de minimis collateral harm, such as if yours is one of the nineteen deidentified devices in the initial anonymized list ruled out by law enforcement, who ultimately only sought identifying information for three suspect devices.[299] Even if your device is among the three where law enforcement received identifying information for your account, the collateral impact on persons uninvolved in the crime is still less than the SWAT team breaking down your door and holding you against your will.[300]

Under the U.S. Supreme Court's controlling precedent, the Fourth Amendment permits the detention of any person with the misfortune of being present during the execution of a warrant.[301] Yet lower courts are split over whether the collateral impact of geofence and keyword warrants on persons not involved in the crime means the strategies violate the Fourth Amendment.[302] This Part explains the conflict in the courts over overbreadth in digital data searches and how the technological exceptionalism in concern

297. In the public health context, collateral impact refers to the impact on groups that are not the direct target of an intervention or vector. *See, e.g.*, Prasad Nagakumar, Ceri-Louise Chadwick, Andrew Bush & Atul Gupta, *Collateral Impact of COVID-19: Why Should Children Continue to Suffer?*, 180 EUR. J. PEDIATRICS 1975, 1976 (2021) (discussing the collateral impact on children of COVID-19); Chiara Anchangwa, Huikyung Park, Sukhyun Ryu & Moo-Sik Lee, *Collateral Impact of Public Health and Social Measures on Respiratory Virus Activity During the COVID-19 Pandemic 2020–2021*, VIRUSES, May 17, 2022, at 1, 2 (investigating collateral impact of COVID-19 control measures on other viruses).

298. *Mena*, 544 U.S. at 95–96.

299. *Chatrie*, 590 F. Supp. 3d at 920–21.

300. Of course, if you are mistakenly arrested based on faulty electronic data, then the collateral harm is much greater—and you may even have a lawsuit. *See, e.g.*, Meg O'Connor, *Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder*, PHX. NEW TIMES (Jan. 16, 2020, 9:11 AM), https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374 [https://perma.cc/VPX3-98R2] (reporting on $1.5 million lawsuit for wrongful arrest based on erroneous Google data putting a man's phone at a shooting scene).

301. *Mena*, 544 U.S. at 98; Michigan v. Summers, 452 U.S. 692, 705 (1981).

302. *Compare, e.g.*, *Chatrie*, 590 F. Supp. 3d at 927, 929–30, 933 (holding a geofence warrant invalid because it did not have particularized probable cause as to each of the nineteen deidentified accounts netted), *with In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 84 (D.D.C. 2021) ("[G]iven the often inherently intrusive task that is evidence gathering, even when performed lawfully by the police—it is neither novel nor surprising that reasonable searches intrude on the privacy interests of individuals who are not the target of criminal investigation.").

over collateral impact reflects overarching disparities in empathy surfeits and deficits in constitutional criminal procedure.[303]

The harms of brute physical tactics like SWAT team deployment are disproportionately borne by BIPOC communities.[304] In contrast, digital data is held by people across all income brackets and demographics—especially wealthier people, because of the continuing digital divide in access to electronic resources.[305] This Part argues that the law regarding the collateral impact of the flexible, low probable cause standard should be equal between strategies likely to harm people with the least power and resources, such as detained persons, and technological strategies more likely to rouse the concern of people with power. This equal treatment of collateral impact allows for convergence of the interests of the powerful and the powerless.[306] The interest convergence theory of eminent theorist Derrick Bell illuminates that converging the interests of the powerful and powerless can ultimately advance civil rights and liberties.[307]

### *A. Judicial Splits over Collateral Impact, Overbreadth in Digital Searches*

A major split in the emerging jurisprudence on digital searches for unknown perpetrators is whether the impact on the data of uninvolved persons violates the Fourth Amendment's probable cause and particularity requirements.[308] In *Carpenter v. United States*, the Supreme Court left

303. *See infra* subparts II(A)–(B).

304. Jonathan Mummolo, *Militarization Fails to Enhance Police Safety or Reduce Crime but May Harm Police Reputation*, 115 PROC. NAT'L ACAD. SCIS. 9181, 9181, 9183, 9185–86 (2018) (finding that "militarized police units are more often deployed in communities with high concentrations of African Americans, a relationship that holds at multiple levels of geography and even after controlling for social indicators including crime rates").

305. *See, e.g.*, Emily A. Vogels, *Digital Divide Persists Even as Americans with Lower Incomes Make Gains in Tech Adoption*, PEW RSCH. CTR. (June 22, 2021), https://www.pewresearch.org/fact-tank/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption/ [https://perma.cc/245Y-UU8W] (noting that smartphone ownership and access to the Internet decreases with low income).

306. *See infra* subpart II(B).

307. *See* Derrick A. Bell, Jr., Brown v. Board of Education *and the Interest-Convergence Dilemma*, 93 HARV. L. REV. 518, 524–25 (1980) (explicating the interest convergence theory in the context of how progress was achieved on school desegregation).

308. *Compare, e.g.*, United States v. Chatrie, 590 F. Supp. 3d 901, 927 (E.D. Va. 2022) (finding violation by geofence warrant), *In re* Search of Info. Stored at Premises Controlled by Google, LLC, 542 F. Supp. 3d 1153, 1158–59 (D. Kan. 2021) (same), *and In re* Search of Info. Stored at Premises Controlled by Google, No. 20 M 297, 2020 WL 5491763, at *6–7 (N.D. Ill. July 8, 2020) (same), *with In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 84, 90–91 (D.D.C. 2021) (no violation by geofence warrant), United States v. Rhine, 652 F. Supp. 3d 38, 81 (D.D.C. 2023) (same), Oral Ruling, *Seymour*, *supra* note 4, at 25–27 (no violation by keyword warrant), *and In re* Search Warrant Application for Geofence Location Data Stored at Google, 497 F. Supp. 3d 345, 353, 364 (N.D. Ill. 2020) (no violation by geofence warrant).

undecided whether the Fourth Amendment even applies when the government obtains digital data from businesses spanning less than seven days or whether the traditional third-party exposure doctrine means there is no reasonable expectation of privacy in the data.[309] Lower courts considering keyword and geofence warrants tend to assume or hold that directing Big Tech companies to search their databases is a Fourth Amendment-regulated search.[310] The question is whether the keyword or geofence warrants satisfy the Fourth Amendment's probable cause and particularity requirements.[311]

A major repeated challenge to geofence and keyword warrants is overbreadth.[312] The argument contests two types of alleged overbreadth (1) requiring companies to search the data of all users in an alleged "fishing expedition," and (2) disclosing deidentified data of multiple users to winnow the data down to potential suspects.[313] The courts to consider the issue conflict sharply over whether individualized probable cause is required for the user of each device whose data is released pursuant to the geofence or keyword warrant.[314]

Most of the publicly available litigation action thus far concerns geofence warrants.[315] Even this pool of decisions is limited because magistrate judges can grant or deny warrant applications without any oral or written statement of reasons.[316] Thus, the pool of data of decisions reporting the details of geofence or keyword warrants is far more limited than the more

309. *See supra* section I(B)(1); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018) (expressly declining to reach the question).

310. *See, e.g.*, Oral Ruling, *Seymour*, *supra* note 4, at 22 ("I'm not prepared to say that simply by availing oneself of the internet, that the users surrender all expectation of privacy with respect to that use.").

311. *E.g.*, *Chatrie*, 590 F. Supp. 3d at 927 (invalidating a geofence warrant for lack of probable cause and particularity); *In re* Search of Info. Stored at Premises Controlled by Google, LLC, 542 F. Supp. 3d at 1158–59 (refusing to grant a geofence warrant request for lack of probable cause and particularity); Oral Ruling, *Seymour*, *supra* note 4, at 26–27 (upholding a keyword warrant based on probable cause and sufficient particularity).

312. *See, e.g.*, Motion to Suppress, *Seymour*, *supra* note 23, at 19–20 (arguing overbreadth in keyword warrant litigation).

313. *E.g.*, *Rhine*, 652 F. Supp. 3d at 82 (overbreadth argument based on the search of all users' data); *Chatrie*, 590 F. Supp. 3d at 927 (overbreadth argument based on the disclosure of nineteen deidentified accounts).

314. *Compare, e.g.*, *Chatrie*, 590 F. Supp. 3d at 927 (holding that a geofence warrant is unconstitutional because it lacks individualized probable cause for every Google user whose data is returned), *with In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 84 (D.D.C. 2021) (recognizing that warrants often have collateral impact on uninvolved parties who are not targets of the investigation and that probable cause need not be shown for each person impacted).

315. *See supra* note 308.

316. *See, e.g.*, *Chatrie*, 590 F. Supp. 3d at 917–18 (noting that the magistrate judge "simply 'read [the Warrant] and signed it'" and that the detective had similarly obtained three other geofence warrants (alteration in original)).

than 11,000 geofence warrant applications and unknown number of keyword warrant applications submitted each year.[317]

The jurisprudence on keyword warrants is even sparser: the main public decision on a motion to suppress a keyword warrant thus far is an oral ruling by a Colorado district judge affirming the grant of the keyword warrant.[318] Reviewing the oral ruling in the Diol family murder investigation, the Colorado Supreme Court concluded that the keyword warrant sufficiently "particularized the place to be searched and the things to be seized" and that even assuming the warrant lacked individualized probable cause—an issue the court did not decide—the police relied in good faith on the keyword warrant.[319] The geofence jurisprudence is instructive for both keyword and geofence warrants, however, because the arguments over probable cause, particularity, and overbreadth in the collateral impact on uninvolved persons are similar.[320]

A contrasting pair of recent geofence cases illustrate the stark conflict in the judicial analyses of overbreadth claims and the sufficiency of probable cause and particularity.[321] *United States v. Rhine*[322] involved a geofence warrant to identify insurrectionists who stormed the U.S. Capitol between 2:00 and 6:30 PM on January 6, 2021 in an effort to circumvent certification of the Presidential election results.[323] Because the U.S. Capitol building was closed for the Electoral College proceeding that day, every entry into the Capitol by an unauthorized member of the public was a crime.[324]

In *Rhine*, federal investigators sought a geofence warrant that disclosed deidentified device data for more than 5,700 users, and identifiable account information for 1,498 devices present on the U.S. Capitol grounds at the time of the January 6 insurrection.[325] To winnow down the list of anonymized devices, investigators at step one obtained three lists: a primary list of devices at the U.S. Capitol on January 6 between 2:00 and 6:30 PM, when the

317. GOOGLE, SUPPLEMENTAL INFORMATION ON GEOFENCE WARRANTS IN THE UNITED STATES (2020), https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf [https://perma.cc/3B42-CUJE] (noting more than 11,000 geofence warrant applications).

318. Oral Ruling, *Seymour*, *supra* note 4, at 26–27.

319. People v. Seymour, 536 P.3d 1260, 1268 (Colo. 2023).

320. *See, e.g.*, Motion to Suppress, *Seymour*, *supra* note 23, at 19–20 (arguing that keyword warrant was overbroad, not sufficiently particularized and lacked individualized probable cause for each of Google's billions of users).

321. *Compare Chatrie*, 590 F. Supp. 3d 901, 927 (E.D. Va. 2022) (invalidating a geofence warrant), *with* United States v. Rhine, 652 F. Supp. 3d 38, 89–90 (D.D.C. 2023) (upholding a geofence warrant).

322. 652 F. Supp. 3d 38 (D.D.C. 2023).

323. *Rhine*, 652 F. Supp. 3d at 46, 66.

324. *Id.* at 85; 18 U.S.C. § 1752(a)(1).

325. *Rhine*, 652 F. Supp. 3d at 69–70.

insurrectionists were present, and two "control" anonymized lists of devices present between 12:00 and 12:15 PM and 9:00 and 9:15 PM when employees but not insurrectionists were present.[326] The control lists excised the authorized personnel from the suspects.[327]

U.S. District Judge Contreras for the District of Columbia upheld the grant of the geofence warrant in the U.S. Capitol insurrection investigation despite the thousands of devices implicated by the disclosures.[328] He reasoned that "January 6 was a unique event in a geographically unusual place such that the scope of probable cause was uncommonly large."[329] The number of rioters who violated 18 U.S.C. § 1752(a)(1) and other laws was "extremely large" with over "500 guilty verdicts or pleas and hundreds more pending charges for January 6 defendants."[330] There was ample probable cause to believe the suspects carried smartphones inside the Capitol building, the court ruled, based on the abundance of surveillance and news footage and photos and videos taken by the insurrectionists.[331] The *Rhine* court reasoned that using control lists of persons at the Capitol in the morning and evening to winnow down the primary list of persons present the afternoon of the insurrection was a reasonable strategy to sort out uninvolved bystanders in the geofence area.[332]

Via geofence warrant, the January 6 insurrection investigators also obtained account information for thirty-seven devices located within an error radius that could have fallen outside the U.S. Capitol—but deleted location data suggested potential concealment and guilty knowledge.[333] The *Rhine* court upheld the inclusion of the account information for the thirty-seven deleted devices, noting that "the area around the Capitol is unusual for its lack of nearby commercial businesses or residences."[334] Extensive road closures around the U.S. Capitol also reduced the likelihood of sweeping up unrelated devices.[335] At both the step one and step three disclosures, there remained the significant likelihood of collateral impact on uninvolved

326. *Id.* at 68–69.
327. *Id.* at 69.
328. *Id.* at 69, 81.
329. *Id.* at 85.
330. *Id.*
331. *Id.*
332. *Id.* at 85–86.
333. *Id.* at 70.
334. *Id.* at 86–87.
335. *Id.* at 87.

persons whose devices happened to be in the geofence radius.[336] This did not render the geofence warrant defective, Judge Contreras ruled.[337]

While *Rhine* did not delve deeply into collateral impact, another geofence warrant decision by a colleague on the U.S. District Court for the District of Columbia, Magistrate Judge Harvey, offered an illuminating analysis.[338] Because the decision dealt with a geofence warrant filed under seal to avoid jeopardizing a pending investigation, the details of the crime and the number of devices impacted were not revealed.[339] The geofenced area covered part of a center in an industrial area and its parking lot—a triangular area of "up to 875 square meters."[340] Addressing overbreadth concerns over the impact of the geofence warrant on uninvolved persons, Magistrate Judge Harvey reasoned that "given the often inherently intrusive task that is evidence gathering, even when performed lawfully by the police—it is neither novel nor surprising that reasonable searches intrude on the privacy interests of individuals who are not the target of criminal investigation."[341] He observed that "for nearly every suspect's text or email account lawfully seized, or house searched, there are frequently other 'innocent' and 'uninvolved' persons whose privacy is compromised."[342]

In a conflicting legal reading, U.S. District Judge Lauck of the Eastern District of Virginia invalidated a geofence warrant that implicated far fewer devices than in *Rhine*.[343] *United States v. Chatrie*[344] involved a bank robbery investigation in which the suspect threatened a teller at gunpoint telling the teller in a handwritten note, "I got your family as hostage . . . [and if] you or your coworker alert the cops . . . [I] am going to start hurting everyone in sight."[345] Witnesses reported seeing the perpetrator "come from the southwestern corner of the Journey Christian Church."[346] Surveillance cameras revealed that the suspect held a cell phone against the side of his face when entering the bank.[347]

---

336. *See id.* (acknowledging the remaining risk of false positives).

337. *Id.*

338. *In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 84 (D.D.C. 2021).

339. *Id.* at 67 n.1, 68.

340. *Id.* at 72.

341. *Id.* at 84.

342. *Id.*

343. United States v. Chatrie, 590 F. Supp. 3d 901, 927 (E.D. Va. 2022); *see supra* text accompanying note 325.

344. 590 F. Supp. 3d. 901 (E.D. Va. 2022).

345. *Id.* at 905–06.

346. *Id.* at 917.

347. *Id.*

Investigating the robbery, Detective Hylton obtained a geofence warrant approved by a magistrate judge.[348] The geofence covered a 150-meter radius encompassing the bank and church and sought information regarding devices present from 4:20 to 5:20 PM at the time and date of the offense.[349] At step one, Google returned a deidentified list of nineteen devices present within the geofenced time and place of the robbery.[350] At step two, Detective Hylton initially requested a larger two-hour window of enlarged movement information for all nineteen anonymized users, but when Google resisted and asked him to narrow the request, he limited his request to nine users.[351] Ultimately, at step three, Detective Hylton narrowed the list of anonymized devices based on movements and sought account identifiers for three users, leading him to the defendant Chatrie.[352]

Considering a motion to suppress the evidence, Judge Lauck expressed concern that "individuals other than criminal defendants caught within expansive geofences may have no functional way to assert their own privacy rights."[353] While noting the lack of clear precedent or guidance, the *Chatrie* court concluded that the geofence warrant violated the Fourth Amendment because the government's probable cause was not particularized to each of the persons whose device data was revealed.[354] Quoting a Supreme Court decision on the individualized probable cause required to search or arrest a *person*, the *Chatrie* court argued that individualized probable cause specific to each person must exist to search Google's *location data*.[355]

An error that arises in litigation of digital searches, illustrated by the *Chatrie* decision, is to conflate searches through data amassed in a vault with the search or arrest of a person.[356] Before a person can be physically searched or arrested, there must be individualized probable cause regarding that person.[357] A search of data amassed in a corporate vault for information responsive to a warrant is plainly a different act than physically arresting or searching your body. Rather, the step one identification of devices pursuant

348. *Id.* at 918.

349. *Id.* at 918–19.

350. *Id.* at 920.

351. *Id.* at 919, 921.

352. *Id.* at 921, 924.

353. *Id.* at 926.

354. *Id.* at 927, 936.

355. *Id.* at 929 (quoting Maryland v. Pringle, 540 U.S. 366, 371 (2003)).

356. *See, e.g.*, *id.* ("[W]arrants must establish probable cause that is 'particularized with respect to the person to be searched or seized.' This [geofence] warrant did no such thing." (citation omitted) (quoting *Pringle*, 540 U.S. at 371)).

357. Ybarra v. Illinois, 444 U.S. 85, 91 (1979) ("Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person.").

to a geofence or keyword warrant is akin to looking through files in a cabinet to retrieve the information particularized in a warrant based on probable cause.[358] Searches of filing cabinets or home offices entail sorting through innocuous documents that may belong to persons other than the target of the investigation and are routinely permitted.[359]

Fundamentally, the *Chatrie* court was concerned by potential overbreadth, especially because the location data of some of the users had a confidence interval that extended outside the geofence area.[360] The court expressed concerns about false positives for individuals driving outside the geofence area but falling within a confidence interval inside the geofence.[361] While declining to opine on whether a geofence warrant could ever satisfy the Fourth Amendment, the *Chatrie* court's reading of the Fourth Amendment's probable cause and particularity requirements seems to imply that the warrant must be drawn so tightly that "only the perpetrator's privacy interests are implicated."[362] A California trial judge was so persuaded by *Chatrie* that the judge invalidated a geofence warrant granted by a magistrate judge and suppressed the results even though only nine deidentified devices were produced by Google at step one and the identifiers for only one account—the defendant's—were produced at step three.[363]

It is tempting to try to systematize the varying geofence decisions and draw some unifying principle. A potential pragmatic unifying factor could be that the narrower the geographical scope and timeframe and the fewer devices impacted, the more likely that the warrant will be upheld. Such a pragmatic standard would cohere with Fourth Amendment reasonableness or cost-benefit balancing to minimize the collateral impact on privacy interests and maximize investigative utility. The disarray in the conflicting decisions do not appear to neatly follow such a unifying factor, however.[364]

Rather, there is a fundamental legal disagreement exemplified by the difference in the decision in *Chatrie* compared to decisions by judges of the

358. *See* United States v. Rhine, 652 F. Supp. 3d 38, 82 (D.D.C. 2023) ("Under Defendant's theory, no doubt many search warrants and most third-party subpoenas for protected records would be unconstitutionally overbroad because they necessarily would require the third party to search some group of records larger than those specifically requested, whether they reside in a file cabinet or on a server.").

359. *In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 84 (D.D.C. 2021) (quoting Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976)).

360. *Chatrie*, 590 F. Supp. 3d at 930.

361. *Id.*

362. *Id.* at 932 (quoting *In re* Search Warrant Application for Geofence Location Data Stored at Google, 497 F. Supp. 3d 345, 361–62 (N.D. Ill. 2020)).

363. Order Granting Motion to Quash Geofence Search Warrant at 20, 43, 49, People v. Dawes, No. 19002022 (Cal. Super. Ct. Sept. 30, 2022) (on file with author).

364. *See supra* text accompanying notes 336–43, 353–55.

U.S. District Court for the District of Columbia.[365] *Chatrie* reflects the assumption that probable cause must be particularized for every person who is impacted by the warrant.[366] In contrast, the decisions in *Rhine* and *In re Search of Information Stored at Premises Controlled by Google LLC*[367] recognize that collateral impact on persons who are not the target of an investigation is rife throughout constitutional criminal procedure and does not amount to a Fourth Amendment violation.[368]

### *B. Interest Convergence, Collateral Harms, and Technological Exceptionalism*

Demanding individualized probable cause for every user whose data is incidentally impacted by a geofence or keyword warrant would be major technological exceptionalism compared to current doctrine on warrant execution. The U.S. Supreme Court has repeatedly underscored that the probable cause standard governing Fourth Amendment searches and seizures is a flexible common-sense standard "well short of absolute certainty."[369] As a result, the Supreme Court held, innocent people might be inconvenienced, humiliated, or terrified in the execution of warrants, even absent a Fourth Amendment violation.[370] Because the probable cause standard deals in fluid probabilities, the Fourth Amendment even contemplates that valid warrants may result in searches of the innocent, according to the Supreme Court.[371]

The impact of the search through the data vault on all the consumers whose information is amassed is a form of collateral impact, akin to the impact on people present on the premises during the execution of an arrest or search warrant for another person.[372] Fourth Amendment doctrine permits collateral impact on persons not involved with the crime during the execution of a search or arrest warrant.[373] When executing a search warrant based on

365. *See supra* text accompanying notes 336–43, 353–55.

366. *Chatrie*, 590 F. Supp. 3d at 929 (quoting Maryland v. Pringle, 540 U.S. 366, 371 (2003)).

367. *In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62 (D.D.C. 2021).

368. *Id.* at 84.

369. Los Angeles County v. Rettele, 550 U.S. 609, 615 (2007); Illinois v. Gates, 462 U.S. 213, 231 (1983).

370. *Rettele*, 550 U.S. at 615–16.

371. *Id.* at 615.

372. *See supra* text accompanying notes 297–300.

373. *See Rettele*, 550 U.S. at 615 ("Valid warrants will issue to search the innocent, and people like Rettele and Sadler unfortunately bear the cost."); Muehler v. Mena, 544 U.S. 93, 98 (2005) (justifying the automatic power to detain those present during the execution of a search warrant as appropriate "because the character of the additional intrusion is slight and because the justifications for detention are substantial"); Michigan v. Summers, 452 U.S. 692, 701–03, 705 (1981) (justifying the same rule along similar lines).

probable cause to believe contraband is present in a home, the police can detain all persons present, even those for whom police lack probable cause of any involvement in the offense under investigation.[374] The automatic power to detain persons present on the premises without individualized probable cause can wreak collateral harms far worse than the collateral impact of an anonymized Sensorvault search yielding deidentified device information.[375]

For Iris Mena, the collateral harm of a search warrant execution was terrifying: multiple armed SWAT team members burst into her bedroom at around 7:00 AM.[376] The warrant was based on probable cause to believe that Raymond Romero, who rented a room in the home, was involved in a drive-by shooting.[377] Although Mena was a "5-foot-2-inch young lady [who] posed no threat to the officers at the scene," officers held her in handcuffs in the garage for two to three hours.[378] Immigration agents accompanied the SWAT team, questioned Mena about her immigration status, and asked to see her papers.[379] Mena sued, arguing that both the search warrant and its execution were overly broad, harming residents in the home for whom police had no probable cause of any crime.[380] The Supreme Court ruled that the police had the categorical power to detain Mena and that handcuffing her for two to three hours was reasonable.[381]

The bland acceptance of collateral harm in the physical execution of warrants has severe distributional consequences for people with the fewest resources and least voice. Mena's case starkly encapsulates the issue. Mena suffered the harms of the search warrant execution because she lived with her family in what factfinders described as a "poor house" that was home to multiple unrelated people.[382] The lived experience of collateral harms is even broader and more severe under cases holding that police may enter a shared home if they have an arrest warrant based on probable cause to arrest anyone in the home.[383] Immigration authorities have entered shared homes based on probable cause for one resident and swept up families and groups for

374. *Summers*, 452 U.S. at 705.

375. *See Mena*, 544 U.S. at 96, 98, 100 (holding that *Summers* justified the two- to three-hour-long detention of an innocent woman who was handcuffed at gunpoint by SWAT members).

376. *Id.* at 96–97.

377. *Id.* at 106 (Stevens, J., concurring).

378. *Id.* at 105.

379. *Id.* at 96 (majority opinion).

380. *Id.* at 96–97.

381. *Id.* at 100.

382. *Id.* at 106 (Stevens, J., concurring).

383. *E.g.*, United States v. Litteral, 910 F.2d 547, 553 (9th Cir. 1990); Perez v. Simmons, 884 F.2d 1136, 1140 (9th Cir. 1988); United States v. Robertson, 833 F.2d 777, 780 (9th Cir. 1987).

immigration-related offenses and deportation.[384] The impact is particularly severe on young people, people with fewer resources, and BIPOC persons because of the higher prevalence of living in shared homes among these demographic groups, according to census data.[385]

Constitutional criminal procedure doctrine suffers from an empathy deficit when it comes to searches that impact people whose lived experience is very different from that of most judges.[386] As Judge Kozinski put it, "[t]he everyday problems of people who live in poverty are not close to our hearts and minds because that's not how we and our friends live."[387] People with the power to make and interpret law are less likely to be forced by economic circumstances to rent a room in the house to someone afoul of the law, like Iris Mena and her family were forced to do.[388] Compared with Mena and families split in immigration home sweeps, people with status, power, and resources are far less likely to suffer the collateral impact resulting from arrest and search warrants.

Conversely, access to electronic devices, apps, and digital amenities increases with income.[389] Digital privacy is increasingly becoming a luxury good sought by persons with resources.[390] Technological exceptionalism in refusing to tolerate the collateral impact of digital searches on uninvolved persons is tempting because digital warrants are more likely to have collateral impact on people with resources than physical warrant executions. This inequality in empathy should not be ratified by law.

Critical race theory has illuminated how advances in civil rights and liberties arise where the interests of the powerful are tied to the interests of

384. Caitlin Dickerson, Nick Corasaniti & Edgar Sandoval, *ICE Launches Raids Targeting Migrant Families*, N.Y. TIMES (July 14, 2019), https://www.nytimes.com/2019/07/14/us/ice-immigration-raids.html [https://perma.cc/DGS8-TRM6]; Nick Miroff, *ICE Raids Targeting Migrant Families Slated to Start Sunday in Major U.S. Cities*, WASH. POST (June 21, 2019, 1:50 PM), https://www.washingtonpost.com/immigration/ice-raids-targeting-migrant-families-slated-to-start-sunday-in-major-us-cities/2019/06/21/f2936318-942e-11e9-b570-6416efdc0803_story.html [https://perma.cc/X3MT-UXTU].

385. Harlan Thomas Mechling, Comment, *Third Party Consent and Container Searches in the Home*, 92 WASH. L. REV. 1029, 1042–44 (2017).

386. Mary D. Fan, *Justice Visualized: Courts and the Body Camera Revolution*, 50 U.C. DAVIS L. REV. 897, 940 (2017).

387. United States v. Pineda-Moreno, 617 F.3d 1120, 1123 (9th Cir. 2010) (Kozinski, C.J., dissenting from the denial of rehearing en banc).

388. Muehler v. Mena, 544 U.S. 93, 106 (2005) (Stevens, J., concurring).

389. *See* Vogels, *supra* note 305 (discussing wealth, poverty, and differences in access to technology).

390. Amanda Hess, *How Privacy Became a Commodity for the Rich and Powerful*, N.Y. TIMES MAG. (May 9, 2017), https://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html [https://perma.cc/FYG7-QR6Y].

people with fewer resources.[391] More widely distributing the costs of a tactic or doctrinal position is also more likely to activate political process or judicial checks when the costs are too high because people with the resources to attain change are impacted.[392]

Technological exceptionalism in tolerance for collateral harms enables the persistence of empathy deficits and differences in protections for tactics most likely to impact people with the least power.[393] Fourth Amendment tolerance for collateral harms in search warrants should be equal as between digital searches and physical searches so that there is not a hierarchy of tolerance of harm for searches most likely to impact the people with the least power. Symmetrically linked fate regarding collateral impact on uninvolved persons means that if the costs are intolerable in the digital search context, they should be intolerable and revised in the physical search warrant execution context most likely to impact people with the least power to seek change. Fourth Amendment doctrine currently contemplates and even facilitates collateral impact on the interests of persons for whom there is no probable cause to search or seize.[394] Unless and until protections are extended in the context of strategies most likely to impact persons without power and resources, the doctrine on collateral impact should equally apply in the context of digital as well as physical search warrant execution.

## III. Digital Probable Cause and the Future of Criminal Procedure

The lack of a named suspect is a major point of conflict and confusion in litigation over new digital search strategies such as keyword and geofence

391. *See, e.g.*, DERRICK BELL, FACES AT THE BOTTOM OF THE WELL: THE PERMANENCE OF RACISM 7 (1992) ("Black people . . . [are] disadvantaged unless whites perceive that nondiscriminatory treatment for us will be a benefit for them."); Bell, *supra* note 307, at 524–25 (discussing the benefits of *Brown v. Board of Education* on enabling industrialization in the South); Richard Delgado, *Explaining the Rise and Fall of African American Fortunes—Interest Convergence and Civil Rights Gains*, 37 HARV. C.R.-C.L. L. REV. 369, 373 (2002) (demonstrating that a motivating factor in the success of *Brown v. Board of Education* was the effect on foreign relations); Cynthia Lee, *Cultural Convergence: Interest Convergence Theory Meets the Cultural Defense*, 49 ARIZ. L. REV. 911, 925–27 (2007) (discussing the foreign policy motivation of a civil rights victory in *Hernandez*).

392. *See* Bernard E. Harcourt & Tracey L. Meares, *Randomization and the Fourth Amendment*, 78 U. CHI. L. REV. 809, 859 (2011) ("[T]he more likely it is that the typical person who encounters the police in a checkpoint reflects the median voter in a given community, the more likely it is that police will be attentive to the demands of that voter when shaping and developing policy.").

393. *Cf.* William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2167 (2002) ("The more people who see a police raid and feel its effects, the more people who are in a position to complain if police tactics are needlessly harsh . . . .").

394. *In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 84 (D.D.C. 2021); *In re* Search Warrant Application for Geofence Location Data Stored at Google, 497 F. Supp. 3d 345, 361 (N.D. Ill. 2020).

warrants.[395] While the use of digital searches to crack cases with unknown perpetrators is relatively new, an analogy can be drawn to the decades-old practice of "John Doe" warrants for perpetrators whose identity is unknown but can be particularized by other means.[396] Simply referring to the unknown perpetrator as John Doe without particularizing other parameters in the John Doe warrant is insufficient under the Fourth Amendment.[397] The John Doe warrant must either "truly name" the person or "describe him sufficiently to identify him."[398] The probable cause and particularity requirements can be satisfied by drawing on other parameters when the target's identity is unknown, such as a work position at a certain place of employment or a location combined with a suspect or vehicle description.[399] For example, the Third Circuit held that a John Doe search warrant was sufficiently particularized to authorize a search of the suspect's person with the following description: "John Doe, a white male with black wavy hair and stocky build observed using the telephone in Apartment 4–C, 1806 Patricia Lane, East McKeesport, Pennsylvania."[400]

Advances in science and technology are providing new parameters to satisfy the Fourth Amendment's requirements of probable cause and particularity for warrants investigating unknown perpetrators. This Part draws lessons from DNA-based John Doe warrants for keyword and geofence warrants.[401] Framing the concepts of digital probable cause and particularity, this Part argues that technological advances can open new bases for probable cause and particularity.[402]

---

395. *See infra* sections I(A)(1)–(2).

396. *See, e.g.*, Heller v. New York, 413 U.S. 483, 485 (1973) (noting issuance of John Doe warrants "for the arrest of the theater manager, the projectionist, and the ticket taker" involved in broadcasting allegedly obscene material); United States v. Barber, 303 F. App'x 652, 653 (10th Cir. 2008) (noting the use of a John Doe warrant to search a house used for illegal drug sales where the identity of the person residing and dealing drugs there was unknown).

397. West v. Cabell, 153 U.S. 78, 86 (1894); United States v. Doe, 703 F.2d 745, 747 (3d Cir. 1983).

398. *Cabell*, 153 U.S. at 85.

399. *E.g.*, *Heller*, 413 U.S. at 485 (discussing a John Doe warrant naming the theater manager, projectionist, and ticket taker at a venue that allegedly showed an obscene film); United States v. Ferrone, 438 F.2d 381, 389 (3d Cir. 1971) (holding that the Fourth Amendment's particularity requirement was satisfied by a physical description of the suspect combined with the suspect's location); Fomby v. State, 170 S.E.2d 585, 586–87 (Ga. Ct. App. 1969) (upholding a John Doe warrant specifying the physical description and location of the suspect as "John Doe @ Blue . . . in the vicinity of Magnolia and Sunset, vehicle being either a green pickup truck or a blue and white Ford").

400. *Ferrone*, 438 F.2d at 389.

401. *See, e.g.*, Frank B. Ulmer, *Using DNA Profiles to Obtain "John Doe" Arrest Warrants and Indictments*, 58 WASH. & LEE L. REV. 1585, 1593–606 (2001) (discussing DNA profiling technology and its use in identifying suspects in warrants and in courts).

402. *See infra* subparts III(A)–(B).

"Digital probable cause" is probable cause that arises from data parameters sufficiently specified to give rise to a fair probability that evidence of a crime is contained within the data boundaries, as defined. These data boundaries could be geolocation coordinates, if sufficiently drawn, or keyword search parameters, if sufficiently narrowed to searches only a suspect is likely to use, such as an arson target's home address. This Article theorizes the concept of digital probable cause and particularity as a foundation for two important goals for the future of constitutional criminal procedure. A robust understanding of what constitutes digital probable cause can address conflicts and confusion in the courts—and safeguard against abuses, such as roving through business data vaults hunting for protestors or abortion seekers.[403]

### *A. Identifying Unknown Suspects: From DNA to Digital Trails*

Attorney and sexual assault survivor P.Y. woke to find a man sprawled across her, pinning her down.[404] The assailant fled after the sexual assault but police obtained his DNA profile from a piece of the skin that P.Y. bit off the assailant.[405] The case went cold, unsolved, and the statute of limitations of eight years for a sexual assault was running.[406] In the sixth year, as time was running out, the police sought an arrest warrant for the unknown perpetrator, identifying him by his DNA profile and gender.[407]

The challenge of how to protect the rights of survivors of crimes with unknown perpetrators is longstanding. Since the 1960s, the rate of unsolved homicides has increased, now hovering near 40%.[408] The rate of unsolved sexual assaults is even more dismal, nearing 70% by 2017.[409] Put another way, only 32% of sexual assault investigations are successfully cleared.[410] Statutes of limitations imposing time limits within which sexual assault and other felonies must be filed vary between states, generally ranging from three to thirty years.[411] Since the 1990s, sexual assault prosecutors have used John

403. *See infra* subpart III(B).

404. State v. Burdick, 395 S.W.3d 120, 122 (Tenn. 2012).

405. *Id.* at 123.

406. *Id.* at 122–23, 123 n.3.

407. *Id.* at 123 & n.3.

408. Avdija et al., *supra* note 90, at 102.

409. Jim Mustian & Michael R. Sisak, *Despite #MeToo, 'Clearance Rate' for Rape Cases at the Lowest Point Since 1960s*, USA TODAY (Dec. 27, 2018, 12:41 PM), https://www.usatoday.com/story/news/nation/2018/12/27/rape-cases-clearance-rate-hits-low-despite-metoo/2421259002/ [https://perma.cc/8C5P-RF62].

410. *Id.*

411. AJ Vicens & Jordan Michael Smith, *Map: How Long Does Your State Give Rape Survivors to Pursue Justice?*, MOTHER JONES (Nov. 24, 2014), https://www.motherjones.com/politics/2014/11/rape-statutes-of-limitation-maps-table/ [https://perma.cc/MX22-Q9KP].

Doe DNA arrest warrants and indictments to address statute of limitations problems with cold cases.[412]

A John Doe DNA warrant uses the perpetrator's DNA profile, rather than his name, to particularize his identity.[413] While the DNA blueprints between humans are more than 99% identical, the pattern of short stretches of repeating DNA sequences, called short tandem repeats (STRs), are nearly unique for every individual.[414] If several unlinked loci of DNA sequences are used to create a DNA profile of a suspect, the random match probability (RMP), meaning the probability that a person at random has the same DNA profile as the sample, is vanishingly low.[415] Between 1998 and 2016, DNA profiles in the FBI's Combined DNA Index System (CODIS), were based on thirteen loci.[416] For the typical 13-loci profile in CODIS, the random match probability is near zero—though not quite zero.[417] In 2017, the CODIS DNA profile expanded to using twenty loci to further reduce the possibility of false positives, even for familial search techniques that try to identify close relatives.[418]

Also known as DNA warrants, John Doe warrants rely on DNA to particularly identify an unknown perpetrator by describing the thirteen or twenty loci that make up the suspect's profile.[419] To sufficiently particularize the suspect, DNA warrants may not merely reference generic labels for loci common to all humans or no loci at all.[420] Moreover, there must be probable cause that the DNA sample in the profile is from the suspect, not just a low

412. Cassidy Kesler Pinegar, *DNA Evidence in Sexual Assault Cases*, CRIM. JUST., Fall 2019, at 37, 38; Julian E. Barnes, *East Side Rapist, Known Solely by DNA, Is Indicted*, N.Y. TIMES (Mar. 18, 2000), https://www.nytimes.com/2000/03/16/nyregion/east-side-rapist-known-solely-by-dna-is-indicted.html [https://perma.cc/RRK4-TWGX].

413. Commonwealth v. Parker, No. 2975 EDA 2012, 2014 WL 10752171, at *2 n.3 (Pa. Super. Ct. Dec. 23, 2014).

414. Nicole Wyner, Mark Barash & Dennis McNevin, *Forensic Autosomal Short Tandem Repeats and Their Potential Association with Phenotype*, FRONTIERS GENETICS, Aug. 6, 2020, at 1, 1; Rana Saad, *Discovery, Development, and Current Applications of DNA Identity Testing*, 18 BAYLOR U. MED. CTR. PROC. 130, 130–32 (2005).

415. Yun S. Song, Anand Patil, Erin E. Murphy & Montgomery Slatkin, *Average Probability that a "Cold Hit" in a DNA Database Search Results in an Erroneous Attribution*, 54 J. FORENSIC SCIS. 22, 23 (2009).

416. Douglas R. Hares, Letter to the Editor, *Selection and Implementation of Expanded CODIS Core Loci in the United States*, 17 FORENSIC SCI. INT'L 33, 33–34 (2015).

417. Song et al., *supra* note

418. Alyssa Lyn Fortier, Jaehee Kim & Noah A. Rosenberg, *Human-Genetic Ancestry Inference and False Positives in Forensic Familial Searching*, 10 G3 2893, 2901 (2020).

419. People v. Robinson, 224 P.3d 55, 60 (Cal. 2010).

420. State v. Belt, 179 P.3d 443, 449–50 (Kan. 2008).

quality sample that may contain a mixture of DNA from multiple possible contributors, none of whom might even be the suspect.[421]

The decades-long practice of using John Doe DNA warrants or DNA-based indictments has survived numerous constitutional challenges in the courts.[422] As the Supreme Judicial Court of Massachusetts explained, DNA is essentially eponymous.[423] Some courts even suggest that a DNA profile is more precise than a name because it is more likely for names to be identical between random people in a population than a DNA profile based on thirteen or twenty loci.[424]

In addition to shedding DNA, perpetrators can shed identity-revealing digital data at crime scenes.[425] The digital data can be essentially eponymous as well, if linked to device IP addresses and user account information.[426] Just as the circumstances in which a DNA sample is obtained can give rise to probable cause to believe the DNA belongs to a perpetrator, so can the circumstances in which digital data is shed give rise to probable cause that the data belongs to the perpetrator. For example, a tissue sample bitten off an assailant gives rise to probable cause that the DNA profile obtained belongs to the assailant.[427] Semen left on an assault victim's body also gives rise to probable cause to believe the DNA profile belongs to the perpetrator.[428]

The DNA arrest warrant analogy is informative, but not an exact correlate for digital data searches pursuant to keyword or geofence warrants because of a fundamental difference between arrest and search warrants. In an arrest warrant, the person to be seized is the suspect, who must be individually particularized.[429] Therefore a John Doe warrant must either correctly and "truly name" the person to be physically searched or seized or "describe him sufficiently to identify him."[430] Where a John Doe warrant uses DNA to identify the unknown person to be seized, there must be a reasonable

421. *See, e.g.*, State v. Police, 273 A.3d 211, 228, 231 (Conn. 2022) (invalidating a DNA warrant as insufficiently particularized because the DNA sample might have come from multiple people).

422. *E.g.*, State v. Younge, 321 P.3d 1127, 1131–33 (Utah 2013) (DNA-based indictment); State v. Burdick, 395 S.W.3d 120, 128 (Tenn. 2012) (DNA warrant); Commonwealth v. Dixon, 938 N.E.2d 878, 884–85 (Mass. 2010) (DNA-based indictment); *Belt*, 179 P.3d at 450 (DNA warrant); State v. Neese, 366 P.3d 561, 564 (Ariz. Ct. App. 2016) (DNA-based indictment).

423. *Dixon*, 938 N.E.2d at 884.

424. State v. Dabney, 663 N.W.2d 366, 372 (Wis. Ct. App. 2003).

425. *See supra* sections I(A)(1)–(2).

426. *See supra* sections I(A)(1)–(2).

427. *See Burdick*, 395 S.W.3d at 123, 128 (upholding a DNA warrant based on skin tissue bitten off of the perpetrator as sufficiently particularized).

428. People v. Robinson, 224 P.3d 55, 61 (Cal. 2010).

429. Ybarra v. Illinois, 444 U.S. 85, 91 (1979).

430. West v. Cabell, 153 U.S. 78, 85 (1894).

certainty that the DNA belongs to that individual and not a mixture of potentially uninvolved persons.[431] In contrast, the thing to be searched in a keyword or geofence warrant is digital data that reveals the identity of the perpetrator.[432]

Search warrants require probable cause that "'the evidence sought will aid in a particular apprehension or conviction' for a particular offense."[433] For search warrants, "all that is required for probable cause" is "a fair probability" that evidence of the crime will be uncovered in the search.[434] There must be both probable cause that a crime has been committed and probable cause that evidence will be found in the place to be searched.[435] Unlike arrest warrants, search warrants need not particularize a specific individual. Rather, search warrants must particularize the types of evidence of a crime that investigators have probable cause to believe is on the premises.[436]

In the context of new digital search strategies such as keyword and geofence warrants, there must be both probable cause that a crime was committed and probable cause that the data search parameters will yield evidence of that crime.[437] The data search parameters mean the records to be searched, such as Google's Sensorvault, and the boundaries of that search, such as the keyword terms or geocoordinates.[438] Because the greatest utility of digital search strategies such as keyword and geofence warrants is to crack

431. *See* State v. Police, 273 A.3d 211, 228, 231 (Conn. 2022) (invalidating a DNA warrant as insufficiently particularized because the DNA sample might have come from multiple people).

432. *See supra* sections I(A)(1)–(2).

433. Dalia v. United States, 441 U.S. 238, 255 (1979) (quoting Warden v. Hayden, 387 U.S. 294, 307 (1967)).

434. Florida v. Harris, 568 U.S. 237, 246 n.2 (2013).

435. *See* Zurcher v. Stanford Daily, 436 U.S. 547, 554 (1978) ("[W]arrants may be issued to search *any* property . . . at which there is probable cause to believe that fruits, instrumentalities, or evidence of a crime will be found.").

436. *See id.* at 555 ("Search warrants are not directed at persons; they authorize the search of 'place[s]' and the seizure of 'things,' and as a constitutional matter they need not even name the person from whom the things will be seized." (citing United States v. Kahn, 415 U.S. 143, 155 n.15 (1974))); *see also* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized.").

437. *See, e.g.*, *In re* Search Warrant Application for Geofence Location Data Stored at Google, 497 F. Supp. 3d 345, 353–56 (N.D. Ill. 2020) (evaluating probable cause to believe arsons were committed and probable cause to believe that evidence of those arsons will be within the parameters of the geofence); *In re* Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 750–53 (N.D. Ill. 2020) (analyzing the failure to establish probable cause in a geofence warrant with coordinates that included residential units, a busy thoroughfare, a parking lot, and businesses); *In re* Search of Info. Stored at Premises Controlled by Google LLC, 579 F. Supp. 3d 62, 77–79 (D.D.C. 2021) (discussing probable cause to believe that a crime of a redacted nature was committed and that the evidence will be found within parameters of geofence).

438. *See supra* sections I(A)(1)–(2).

cases involving unknown perpetrators, the evidence of the crime usually sought in digital search warrants is the perpetrator's identity.[439]

Digital probable cause arises from the likelihood that the perpetrators of a known unsolved crime are identifiable from the digital data sought, as defined by the search parameters. Whether there is the sort of fair probability required for digital probable cause depends on the circumstances of the crime, such as whether it was committed in a time and place with few people other than the perpetrator, and the nature of the data search parameters, such as whether the keyword search terms are likely to be used only by the perpetrator of a crime in planning and executing it. The greater the number of potential devices and users likely to be captured in the data search parameters, the less likely there is digital probable cause because gathering a large haystack of user data does not give a fair probability of finding the needle in that haystack.

### *B. Protesters, Abortion Seekers, and Beyond: Preventing Dragnet Searches*

Some advocates contend that keyword or geofence warrants should be wholly forbidden as a Fourth Amendment matter, arguing that the tactics could be used to target people for political speech or to hunt abortion seekers.[440] Advocacy organizations warn of keyword searches used to "identify and track those searching for abortion-inducing drugs like mifepristone, misoprostol, and other abortifacients, as well as those providing medical care."[441] Concerns about abuse of Sensorvault data to go on roving searches surveilling intimate health decisions led Google to promise to delete location history showing visits to "medical facilities like counseling centers, domestic violence shelters, abortion clinics, fertility centers, addiction treatment facilities, weight loss clinics, cosmetic surgery clinics, and others."[442] Google executive Jen Fitzpatrick announced the

439. *See supra* sections I(A)(1)–(2).

440. Albert Fox Cahn & Julian Melendi, *The New Way Police Could Use Your Google Searches Against You*, SLATE (Aug. 1, 2022, 2:18 PM), https://slate.com/technology/2022/08/keyword-search-warrants-colorado-roe.html [https://perma.cc/366X-XKZM]; Jennifer Lynch & Andrew Crocker, *Update: Colorado Supreme Court Grants Review in First U.S. Case Challenging Dragnet Keyword Warrant*, ELEC. FRONTIER FOUND. (Jan. 18, 2023), https://www.eff.org/deeplinks/2022/06/eff-file-amicus-brief-first-us-case-challenging-dragnet-keyword-warrant [https://perma.cc/2GZQ-ZBGM].

441. Cahn & Melendi, *supra* note 440.

442. Jen Fitzpatrick, *Protecting People's Privacy on Health Topics*, KEYWORD, GOOGLE (May 12, 2023), https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/ [https://perma.cc/A3JM-2DB2].

policy shortly after a draft of the decision in *Dobbs v. Jackson Women's Health Organization*[443] overturning *Roe v. Wade*[444] leaked.[445]

In New York, legislators introduced a bill banning keyword and geofence warrants and providing for exclusion of any evidence obtained by such searches as well as punitive damages.[446] While the bill was introduced in 2021, before the leak about the demise of *Roe v. Wade*, co-sponsors trying to gain support for the bill post-*Dobbs* raise the specter of abuse of keyword warrants to search for people who search for abortion drugs.[447]

Democratic debate spurred by elected legislators over how police may use technology and amassed data is refreshing and important for the future of criminal procedure. From a democratic policing framework, it is important for voters and elected representatives to take responsibility for the kind of policing and balance between competing values desired.[448] Moreover, action by state legislatures has the federalism advantage of recognizing that "We the People" are actually many peoples with diverse local tastes about the right balance between police power to investigate crimes and privacy.

As a matter of Fourth Amendment interpretation, however, imagining a possible worst-case abuse of an investigative strategy is usually not a basis for a constitutional straitjacket prohibiting the practice altogether.[449] The sad reality is that all investigative powers can be abused in the wrong hands of a brutal or tyrannical regime. The fundamental question is how to interpret and adapt constitutional protections in light of evolving technologies and digital search strategies to protect against the slide into the worst-case scenario. Three guiding principles for what constitutes digital probable cause can help sort out constitutionally infirm practices from strategies to solve crimes involving unknown perpetrators that do not run afoul of the Fourth Amendment.

A first protective principle of digital probable cause is that there must be probable cause to believe that a grave, known crime has been committed, such as the arson-murders of the Diol family or the series of pipe bombings

443. 142 S. Ct. 2228 (2022).

444. 410 U.S. 113 (1973), *overruled by* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022).

445. *See* Press Release, Supreme Court of the United States, Statement of the Court Concerning the Leak Investigation (Jan. 19, 2023), https://www.supremecourt.gov/publicinfo/press/Dobbs_Public_Report_January_19_2023.pdf [https://perma.cc/M4ZD-UFEJ] (giving a timeline of the *Dobbs* leak).

446. Assemb. B. A00084, 2021 Assemb., Reg. Sess. (N.Y. 2021), https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A00084&term=2021&Text=Y [https://perma.cc/WRR8-U3WR].

447. Cahn & Melendi, *supra* note 440.

448. BARRY FRIEDMAN, *supra* note 210, at 27.

449. *See, e.g.*, Atwater v. City of Lago Vista, 532 U.S. 318, 346–47 (2001) (recognizing abuse of power by police officer on the facts of the case but explaining that constitutional rules must bind across all cases).

and killings where keyword and geofence warrants have been deployed.[450] The requirement of a discrete, known crime prevents roving searches through data to target persons and persecute them for searching how to exercise what was once a constitutional right, but which has now been criminalized in some jurisdictions.[451] If there is not a known, discrete, and unsolved crime, then there is no probable cause to go roving through Google's Sensorvault or other data repositories in search of crimes and perpetrators.

Considering the gravity of the crime is a more controversial principle because the Supreme Court has in several cases avoided having rules based on whether a crime is considered major or minor.[452] Yet as the Supreme Court has increasingly turned to reasonableness balancing in interpreting the Fourth Amendment's requirements, the Court has crafted more permissive rules for grave crimes, particularly where a search is minimally intrusive.[453] The prime example is *Illinois v. Lidster*,[454] in which the Supreme Court upheld brief, suspicion-less stops of motorists to solve a grave crime: the hit-and-run of a bicyclist.[455] What constitutes a grave crime? The *Lidster* Court explained that "a crime that had resulted in a human death" is grave.[456]

A second protective principle is that the digital data search parameters must be sufficiently tightly drawn to yield a fair probability that the perpetrator of a discrete, known crime will be identified. The broader the keywords or the more people swept up in a geofence, the less the probability that any perpetrator will be identifiable in the mass. The probability of identifying the perpetrator is heightened for crimes committed in times and places where few persons, other than the perpetrator, would be, or for keywords that people other than perpetrator would be unlikely to search. The touchstone is not merely the number of users who might be revealed because some crimes, such as the January 6 insurrection, entail hundreds of perpetrators or may involve multiple co-conspirators at the scene.[457]

---

450. *See supra* text accompanying notes 23–37, 130–37.

451. *See* Elizabeth Nash & Isabel Guarnieri, *13 States Have Abortion Trigger Bans—Here's What Happens When Roe Is Overturned*, GUTTMACHER INST. (June 6, 2022), https://www.guttmacher.org/article/2022/06/13-states-have-abortion-trigger-bans-heres-what-happens-when-roe-overturned [https://perma.cc/87PB-Y2K3] (listing states that criminalize abortion).

452. *See, e.g.*, Mincey v. Arizona, 437 U.S. 385, 395 (1978) (rejecting a murder scene exception to the Fourth Amendment's warrant requirement); *Atwater*, 532 U.S. at 346, 353–54 (rejecting a limitation on warrantless arrests for minor offenses).

453. *E.g.*, Illinois v. Lidster, 540 U.S. 419, 427 (2004) (upholding brief information-seeking stops to investigate a serious crime, a hit-and-run homicide).

454. 540 U.S. 419 (2004).

455. *Id.* at 427.

456. *Id.*

457. *See supra* text accompanying notes 323–37.

The third protective principle is that digital searches may not sweep so broadly as to burden other constitutional rights, such as the First Amendment rights of free speech and association.[458] This principle cuts to the core of a concern that geofence and keyword warrants may impact political protesters, such as persons present at Black Lives Matter protests.[459] For example, police investigating the burning of the Seattle Police Officers Guild building sought a geofence warrant with coordinates bounding a whole city block in downtown Seattle.[460] The area included not only the Police Guild building but also other structures,[461] along with hundreds of protesters who may not have been involved in the arson. While Fourth Amendment doctrine currently tolerates collateral impact in the execution of search warrants, as discussed in Part II, the collateral impact cannot be in contravention of other constitutional rights. Whether there is digital probable cause for a search tactic such as a keyword or geofence warrant must be construed to avoid conflict with other constitutional rights, including First Amendment freedoms.[462]

## Conclusion

The massive vault of data that companies have about our search histories, movements, and behaviors is giving rise to new police investigative strategies.[463] The rise of new digital search strategies exemplified by keyword and geofence warrants is both tempting and terrifying in its power, and it is spurring litigation with important implications for the future of constitutional criminal procedure. This Article advances beyond the Romantic Luddism of originalist-tinged attempts to liken these new digital search strategies to 1700s-era general warrants, an inapposite analogy from a time before electric power, much less electronic data.[464] The digital age is transforming how and why crimes are perpetrated and people are targeted. Our conceptions of what constitutes probable cause and particularity under the Fourth Amendment must evolve too.

---

458. U.S. CONST. amend. I.

459. Corin Faife, *FBI Used Geofence Warrant in Seattle After BLM Protest Attack, New Documents Show*, VERGE (Feb. 5, 2022, 8:00 AM), https://www.theverge.com/2022/2/5/22918487/fbi-geofence-seattle-blm-protest-police-guild-attack [https://perma.cc/D2W5-8BFF].

460. Application for a Search Warrant at 10–11, 15–16, *In re* Search of Info. Stored by Google, No. 20-MJ-643 (W.D. Wash. 2020) (on file with author).

461. *Id.* at 16.

462. *Cf.* Fox v. Washington, 236 U.S. 273, 277 (1915) ("So far as statutes fairly may be construed in such a way as to avoid doubtful constitutional questions they should be so construed; and it is to be presumed that state laws will be construed in that way by the state courts.") (citation omitted).

463. *See supra* text accompanying notes 23–37, 130–37; *see also supra* sections I(A)(1)–(2).

464. *See supra* subpart I(B).

This Article offers a theoretical and conceptual framework to analyze the constitutionality of keyword and geofence search warrants where probable cause arises from digital data parameters and the data of uninvolved persons may be impacted.[465] The Article frames the concepts of collateral impact and collateral harm to analyze Fourth Amendment claims that the execution of warrants will impact or even injure innocent third parties.[466] The doctrine on physical warrant execution tolerates and even facilitates collateral harms that are most likely to be experienced by people with the least power and fewest resources.[467] Arguments that the Fourth Amendment is violated if the data of uninvolved third parties are impacted essentially seek technological exceptionalism from the usual Fourth Amendment tolerance of collateral impact under the probable cause standard.[468] While technological exceptionalism is alluring—especially because people with power and resources have greater access to technology and thus more empathy for technology-related concerns—the temptation to ratify divergences in empathy must be resisted.[469] Interest convergence theory teaches that civil rights for all, including the least powerful, ultimately advance when the interests of the powerful converge with those of the powerless—so linking the outcomes plants the seeds to force potential change.[470]

Elucidating the principles of digital probable cause, this Article addresses major points of conflict and confusion in the courts over digital search strategies deploying warrants for unknown perpetrators.[471] This Article also addresses the conflation in some courts between probable cause to arrest or search a person, which must be particularized to that specific person, and probable cause to search for evidence, which is based on a fair probability that evidence will be found.[472] Drawing on decades of practice involving John Doe warrants, the Article shows how warrants can be valid even if a perpetrator is unknown but her identity is particularized by other parameters.[473] The rise of DNA-profile-based arrest warrants used to toll the statute of limitations in sexual assault cases illustrates how the advances of science and technology can offer new parameters for probable cause and particularity in search warrants.[474]

---

465. *See supra* Parts II–III.

466. *See supra* Part II.

467. *See supra* subpart II(B).

468. *See supra* subpart II(B).

469. *See supra* subpart II(B).

470. *See supra* subpart II(B).

471. *See supra* Part III.

472. *See supra* text at notes 356–362, 429–436.

473. *See supra* Part III.

474. *See supra* subpart III(B).

Advances in technology also enable the use of digital data parameters to meet the probable cause and particularity requirements for warrants. This Article frames the concept of digital probable cause, which arises if a warrant specifies data-based parameters that give rise to a fair probability that evidence of a crime is contained within the data sought.[475] The parameters could be geolocation coordinates for geofence warrants or keyword search parameters, if sufficiently focused on terms only a suspect would likely use. Where the data-based parameters are too broad and net too many uninvolved people, then digital probable cause that the warrant will find the perpetrator in the haystack of data is lacking. The Article also elucidates three principles to safeguard against the abuse of keyword and geofence warrants, such as hunting for abortion seekers or chilling the rights of protesters to exercise First Amendment freedoms.[476]

475. *See supra* Part III.

476. *See supra* subpart III(B).