Suspectless Searches

CHRISTOPHER SLOBOGIN[*]

Traditional searches of persons, houses, papers, or effects usually begin with an identified suspect or person of interest. But today police are increasingly using technology to engage in what might be called suspectless searches—searches that try to identify a perpetrator—using techniques like geofencing, TiVo droning, DNA matching, automated license plate readers, and facial recognition technology. The Fourth Amendment should govern use of such techniques. But application of its reasonableness requirement to suspectless searches should not always require a warrant or probable cause, given the minimal intrusion often associated with them. Instead, the focus in these types of cases should be how to circumscribe the scope of the search consistent with the Fourth Amendment's particularity mandate and ensure that normal Fourth Amendment constraints are followed when police act on the information they obtain from the suspectless search.

TABLE OF CONTENTS

I. INTRODUCTION 953
II. GEOFENCING 959
III. TIVO DRONING AND AIR 962
IV. DNA MATCHING 963
V. FACIAL RECOGNITION 968
VI. ALERTS 971
VII. CONCLUSION 974

I. INTRODUCTION

In November 2016, Nwabu Efobi, a taxi driver, was shot in front of the Universal Cab Company in Raleigh, North Carolina.[1] According to newspaper accounts, security video caught Efobi "in some kind of confrontation with the shooter before the unknown man opened fire."[2] The day before, cameras had

[*] Milton Underwood Professor of Law, Vanderbilt University. The author would like to thank participants at a Vanderbilt Law School workshop and Suzanna Sherry, Ingrid Wuerth, and Paul Edelman for their comments on this paper.

[1] Tyler Dukes, *To Find Suspects, Raleigh Police Quietly Turn to Google*, WRAL NEWS, https://www.wral.com/Raleigh-police-search-google-location-history/17377435/ [https://perma.cc/4B67-XU3H] (July 13, 2018).

[2] *Id.*

caught the unknown man "walking around the [same] building with what appeared to be a cell phone at his ear."[3]

Unfortunately, the camera image was too grainy to get a good fix on the man's face.[4] But police were able to resort to another type of investigative technique. On a satellite image of the area, they drew a "digital cordon" around the building and its environs.[5] They then convinced a judge to issue a warrant ordering Google to provide account identities for every cell phone that crossed the digital cordon during times related to the camera images and the shooting.[6] In October 2017, police arrested Tyron Cooper for Efobi's murder.[7] The inventory for the warrant proffered to Cooper's defense team indicated that electronic records within the cordon were in fact retrieved.[8]

The technique used in Efobi's case is sometimes called "geofencing," at other times a "reverse warrant," because it is used to locate a suspect rather than to investigate one who has already been identified.[9] Geofencing is quite common today in police departments around the country.[10] The city of Raleigh, where Efobi was killed, relied on it in at least four cases in 2017, involving two killings, an arson and a sexual assault (helping to solve two of the crimes, and coming up empty in the other two).[11] In 2018, Google reported it was receiving roughly nineteen geofencing requests a week,[12] in 2019 it reported an 800% increase in such requests,[13] and in 2020 it responded to 11,554 geofence demands, 3,000 more than in the previous year.[14]

Geofencing is just one of many types of modern "suspectless" police investigative techniques—techniques that use technology to identify the suspected perpetrator of a crime rather than find out more about an already identified suspect. A visual analogue to geofencing is "TiVo droning," which uses camera surveillance footage from drones or planes to reverse engineer the

[3] *Id.*

[4] Ed Crump, *Vigil a Call for Justice for Slain Raleigh Cabbie*, ABC 11 (Nov. 21, 2016), https://abc11.com/raleigh-shooting-police-hill-street-nwabu-cyril-efobi/1618668/ [https://perma.cc/7TXG-CT77].

[5] Dukes, *supra* note 1.

[6] *Id.*

[7] *Id.*

[8] Tyler Dukes & Lena Tillett, *In Quest to Solve Murders, Raleigh Community Targeted Twice by Google Warrants*, WRAL NEWS, https://www.wral.com/in-quest-to-solve-murders-raleigh-community-targeted-twice-by-google-warrants/18497624/ [https://perma.cc/R8J6-DR3H] (July 25, 2019).

[9] *Id.*

[10] *Id.*; *see also* Zack Whittaker, *Google Says Geofence Warrants Make Up One-Quarter of All US Demands*, TECHCRUNCH (Aug. 19, 2021), https://techcrunch.com/2021/08/19/google-geofence-warrants [https://perma.cc/4SUW-QDDY].

[11] *See* Dukes, *supra* note 1.

[12] *See* Whittaker, *supra* note 10.

[13] *Id.*

[14] *Id.*

routes of figures at a crime scene, in an effort to determine where they came from and who they are.[15] Less obviously, suspectless searches also are involved when police obtain DNA they believe to be the perpetrator's and then seek a match in public or private DNA databanks—here too police already have evidence about the crime and use it to help catch a criminal. Similarly, facial recognition technology ("FRT") can be used to identify a perpetrator by matching a surveillance photo from a crime scene to an image database.[16] Then there are a number of "alert systems" that help identify suspects. For example, software programs can sample social media sites for images of child pornography, which can then be linked to a particular IP address.[17] Automated License Plate Readers ("ALPRs"), if connected to "hotlists" of stolen vehicles, can signal to police when they come across a car on the list.[18]

All of these new police techniques are controversial, not only because they often are covert, but also because they are likely to cast a wide net.[19] To identify or find a suspect, law enforcement must often obtain data about a large number of innocent people: geofencing and TiVo droning will collect location information about anyone near the event, DNA analysis will discover all partial matches to the DNA submitted, facial recognition systems could scan thousands of faces, pornography software could access thousands of computer files, and ALPRs might capture the images of thousands of cars.[20] To use a phrase coined

[15] *See infra* text accompanying notes 63–66.

[16] U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-526, FACIAL RECOGNITION TECHNOLOGY: CURRENT AND PLANNED USES BY FEDERAL AGENCIES 3–4 (2021), https://www.gao.gov/assets/gao-21-526.pdf [https://perma.cc/TKP9-BBFG].

[17] Olivia Solon, *Inside the Surveillance Software Tracking Child Porn Offenders Across the Globe*, NBC NEWS (July 17, 2020), https://www.nbcnews.com/tech/internet/inside-surveillance-software-tracking-child-porn-offenders-across-globe-n1234019 [https://perma.cc/M6FA-WB3K].

[18] *Street-Level Surveillance: Automated License Plate Readers (ALPRs)*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/automated-license-plate-readers-alpr [https://perma.cc/XZ8L-55PP] (Aug. 28, 2017).

[19] *Id.*; Solon, *supra* note 17; Adam Schwartz, *Resisting the Menace of Face Recognition*, ELEC. FRONTIER FOUND. (Oct. 26, 2021), https://www.eff.org/deeplinks/2021/10/resisting-menace-face-recognition [https://perma.cc/LL6N-5KMY].

[20] *See* Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/6H94-ZGDP]; Lindsey Van Ness, *DNA Databases Are Boon to Police, but Menace to Privacy, Critics Say*, PEW CHARITABLE TRS. (Feb. 20, 2020), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/02/20/dna-databases-are-boon-to-police-but-menace-to-privacy-critics-say [https://perma.cc/A9TJ-UJ7F]; Labhesh Patel, *Balancing Privacy Concerns Around Facial Recognition*, FORBES (June 1, 2020), https://www.forbes.com/sites/jumio/2020/06/01/balancing-privacy-concerns-around-facial-recognition/?sh=4531822419a4 [https://perma.cc/6D29-8P9N]; Solon, *supra* note 17; *How ALPR Works*, NDIRS, https://www.ndi-rs.com/how-alpr-works/ [https://perma.cc/59Z3-NPVQ].

by Jane Bambauer,[21] the *hassle rates* of these techniques—the extent to which they ensnare innocent individuals who had nothing to do with the crime in question—can be quite high unless significant limitations are imposed on them. At the same time, the amount and type of information police obtain about any particular person through suspectless techniques—one's location at a particular point in time, the fact that one is related to a criminal, or the fact that one has engaged in crime or is driving a stolen vehicle—are often minimal.

This Article examines how the Fourth Amendment's guarantee of "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches" and its requirement that warrants be based on probable cause and "particularly describ[e] the place to be searched, and the persons or things to be seized" apply to suspectless investigative techniques.[22] In doing so, it defends two significant propositions.

The first is that technologically enhanced suspectless practices are searches under the Fourth Amendment. While none of these techniques physically invades the person, houses, papers, or effects of which the amendment speaks, recent Supreme Court decisions provide plausible grounds for concluding that all of them infringe "expectations of privacy society is prepared to recognize as reasonable," the Court's dominant definition of the word "search."[23] In *United States v. Jones*, which involved tracking Jones's car using signals from a GPS device affixed to his car,[24] five justices signaled that surveillance of public activities of the type contemplated by TiVo droning, FRT, and ALPRs can be a search, at least if prolonged.[25] And *Carpenter v. United States*, which required a warrant to obtain Carpenter's cell site location information ("CSLI") from his common carrier,[26] indicates that information held by third parties—like the location data collected by Google that is used in geofencing and the DNA profiles maintained by direct-to-consumer genetic databanks—is protected by the Fourth Amendment; *Carpenter* may be the beginning of the end for the "third-party doctrine" that, since the 1970s, has dictated that one cannot

[21] Jane Bambauer, *Hassle*, 113 MICH. L. REV. 461, 464 (2015) ("Hassle is the chance that the police will stop or search an innocent person against his will.").

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

[23] This language comes from Justice Harlan's concurring opinion in *Katz v. United States*, 389 U.S. 347, 361 (1967), but has since been adopted by the full Court. *See* United States v. Jones, 565 U.S. 400, 406 (2012).

[24] *Jones*, 565 U.S. at 402–03.

[25] In her concurring opinion in *Jones*, Justice Sotomayor stated "I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy'" and goes on to suggest the same conclusion with respect to "even short-term monitoring." *Id.* at 415 (Sotomayor, J., concurring) (quoting *id.* at 430 (Alito, J., concurring in judgment)). In dissent, Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, concluded that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* at 430 (Alito, J., concurring).

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

reasonably expect privacy in information surrendered to a third party.[27] Neither *Jones* nor *Carpenter* dealt directly with suspectless investigative techniques. But, as developed further below, their rationales can easily apply to those practices.

The second proposition advanced in this Article is that, to be "reasonable" under the Fourth Amendment, a suspectless search need not always be justified by a warrant based on probable cause. In previous writings culminating in a 2007 book entitled *Privacy at Risk*,[28] I not only argued for a broad definition of search but also for adoption of a "proportionality principle," which posits that the justification for a search or seizure should be roughly proportionate to its intrusiveness.[29] Under this principle, search of a house would require probable cause, but searches outside the home might not; long-term surveillance would require probable cause, but short-term surveillance would not. For better or worse, the Supreme Court appears to be moving toward this position in its more recent cases.[30] In *Jones*, four justices distinguished between "prolonged" and short-term GPS tracking in deciding whether the Fourth Amendment applied;[31] in her concurring opinion in *Jones*, a fifth justice, Justice Sotomayor, expressed particular concern about "aggregated" information.[32] In *Carpenter*, while requiring a warrant for accessing a week's worth of cell cite location data, the Court refused to address whether seeking only a few days of data should also trigger the warrant process.[33] *Riley v. California*, another Supreme Court case dealing with the Fourth Amendment and technology,[34] expresses a similar view. There, in the course of requiring a warrant to search a phone seized from an arrestee, the Supreme Court dismissed centuries-old precedent permitting

[27] *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) ("[An individual] takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

[28] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 30 (2007) [hereinafter SLOBOGIN, PRIVACY AT RISK]. I recently updated the arguments in *Privacy at Risk* in CHRISTOPHER SLOBOGIN, VIRTUAL SEARCHES: REGULATING THE COVERT WORLD OF TECHNOLOGICAL POLICING (2022).

[29] SLOBOGIN, PRIVACY AT RISK, *supra* note 28, at 28–30.

[30] *Jones*, 565 U.S. at 430–31 (Alito, J., concurring in judgment).

[31] *Id.* (citations omitted) ("[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

[32] *Id.* at 416 (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

[33] Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018).

[34] Riley v. California, 573 U.S. 373, 378 (2014).

warrantless, suspicionless searches of an arrestee's effects (such as a purse or wallet), asserting that comparing those actions to the search of a phone "is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[35] Admittedly, in all three cases, the choice was still between a warrant based on probable cause and no regulation at all, rather than between probable cause and some lesser degree of suspicion. But the intuition that the length of a technologically enhanced intrusion or the amount of information it obtains is relevant to Fourth Amendment analysis is imbedded in these opinions.

Building on these two propositions, this Article argues that the Fourth Amendment should govern suspectless searches but that the typical warrant-based authorization is not required to carry them out. The most important goal in these types of cases is to reduce hassle rates, which is most effectively realized by carefully circumscribing the scope of the search (consistent with the Fourth Amendment's particularity requirement) and by applying normal Fourth Amendment constraints on what police do with the information they obtain from the suspectless search. The Supreme Court case most relevant to this constitutional inquiry is *Illinois v. Lidster*, which involved a checkpoint set up one week after a hit-and-run incident, at the same hour of the day it occurred; the goal of the police was to identify eyewitnesses to, or the perpetrator of, the crime.[36] The Supreme Court held that the checkpoint did not violate the Fourth Amendment, despite the fact it resulted in the seizure (hassling) of a large number of individuals for whom the police had no individualized suspicion.[37] Instead, the Court said, courts should consider "the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty."[38] Because the checkpoint was aimed at finding a hit-and-run culprit, was constructed in a way that furthered the chances of finding that person while minimizing hassle rates, and involved a relatively minor seizure, the checkpoint was permissible.[39]

As this Article demonstrates, most suspectless searches initially involve minor interferences with privacy, and can potentially significantly advance the public interest, at least if limited to investigation of serious crimes. These general concepts are explored in each of the specific contexts mentioned above, beginning with geofencing.

[35] *Id.* at 385–86, 393.

[36] Illinois v. Lidster, 540 U.S. 419, 422 (2004).

[37] *Id.* at 427–28.

[38] *Id.* at 426–27 (citing Brown v. Texas, 443 U.S. 47, 51 (1979)).

[39] *Id.* at 427.

II. GEOFENCING

Google has been hit by so many geofencing requests of the type used in the Efobi case that it has developed a procedure that it insists law enforcement use, consisting of three stages, all requiring a "warrant."[40] The first step—the initial data dump—must be authorized by a court order that defines the geographic area and time window for the location data.[41] So, for instance, the warrant application might ask for data about any user within 200 yards of the crime scene during a thirty minute period both before and after the crime. The second step—called selective expansion—allows law enforcement to ask for more location data information about the phones identified in the initial dump that are of special interest; for instance, it might ask that, for phones that stayed near the crime scene during the relevant time period, Google provide location data outside the original geographic zone and/or beyond the original time window to see where those phones came from and where they went.[42] The final stage is the unmasking—the disclosure of the account owner's identity—which could include the owner of every phone within the original warrant but presumably would be narrowed down considerably if the warrant is to issue.[43]

Some courts have readily issued the geofence order that starts this process.[44] Others have been more reluctant to do so, especially if the scope of the initial data dump is significant.[45] For instance, in one case, law enforcement requested a warrant for location data within a 7.7-acre area that included residences, seven businesses, and healthcare providers.[46] The judge refused to issue the warrant, stating that the "vast majority of cellular telephones likely to be identified in this geofence will have nothing whatsoever to do with the offenses under investigation."[47] The same judge also rejected a second request for a warrant for a smaller area and time frame, as well as a third request that kept those variables

[40] Declaration of Sarah Rodriguez at ¶ 5, United States v. Chatrie, No. 3:19-cr-00130 (E.D. Va. Mar. 3, 2022), ECF 96-2; *see supra* notes 1–3 and accompanying texts.

[41] John C. Ellis, Jr., *Google Data and Geofence Warrant Process*, NAT'L LITIG. SUPPORT BLOG (June 6, 2022), https://nlsblog.org/2022/06/06/google-data-and-geofence-warrant-process-2/ [https://perma.cc/NJ9Q-F8QD]; Haley Amster & Brett Diehl, Note, *Against Geofences*, 74 STAN. L. REV. 385, 399–403 (2022).

[42] Ellis, *supra* note 41; Amster & Diehl, *supra* note 41, at 404–05.

[43] Ellis, *supra* note 41; Amster & Diehl, *supra* note 41, at 405–06.

[44] Commonwealth v. Perry, No. 1984CR00396, 2021 WL 2019293, at *1 (Mass. Super. Ct. Apr. 21, 2021), *aff'd in part, rev'd in part* 184 N.E.3d 745, 771 (Mass. 2022); Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345, 349 (N.D. Ill. 2020).

[45] United States v. Chatrie, No. 3:19-cr-130, 2022 U.S. Dist. LEXIS 38227, at *12–13 (E.D. Va. Mar. 3, 2022).

[46] *In re* Search of Info. Stored at Premises Controlled by Google, No. 20 M 297, 2020 U.S. Dist. LEXIS 165185, at *8 (N.D. Ill. July 8, 2020).

[47] *Id.* at *13 (emphasis omitted).

constant but did not ask for the unmasking step (but also reserved the right to achieve the same goal through a subpoena).[48]

Note first that all these cases assume that geofencing is a search. After *Carpenter*, that conclusion seems solid, since geofencing involves accessing CSLI from a third party, just as in that case.[49] However, unlike in *Carpenter*, which involved investigation of an identified suspect, geofencing is suspectless.[50] Requiring a traditional warrant based on probable cause to believe a named individual has engaged in wrongdoing, as the Supreme Court did on *Carpenter*'s facts,[51] would make geofencing virtually impossible. While the police might be able to demonstrate probable cause to believe one of the phones in the geofence zone belonged to the perpetrator, they cannot particularly describe which person or persons are suspects, probably even at the second or third stages, much less the first. Consistent with that view, one magistrate concluded that execution of a geofence warrant was an unconstitutional general search unless everyone within the designated area was reasonably believed to be involved in the crime, in effect precluding such warrants.[52]

Proportionality analysis, in contrast, would allow geofencing, with certain limitations. It would not (and could not) require a warrant, given the Fourth Amendment's traditional probable cause requirement. Instead, it would require a court order based on a finding by the judge that the police have made a good faith effort to minimize the area and time zones consistent with the known facts about the crime. Although this showing would be analogous to the mandate found in the amendment that warrants must "particularly describ[e]" the place or person to be searched and the items seized,[53] neither probable cause nor reasonable suspicion with respect to any given individual or phone would be required, for two reasons. First, the location data are anonymous; police will not know whose location they are learning (and if they tried to de-anonymize the data by, say, going to a databroker, they *would* need individualized suspicion).[54]

[48] *Id.* at *2.

[49] JENNIFER LYNCH, MODERN-DAY GENERAL WARRANTS AND THE CHALLENGE OF PROTECTING THIRD-PARTY PRIVACY RIGHTS IN MASS, SUSPICIONLESS SEARCHES OF CONSUMER DATABASES 3–4 (Hoover Inst. Working Paper on Nat'l Sec. Tech. & L., Aegis Paper Ser. No. 2104 2021) https://www.hoover.org/sites/default/files/research/docs/lynch_webreadypdf.pdf [https://perma.cc/SDU3-7XAU].

[50] *Id.*

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

[52] *In re* Search of Info. Stored at Premises Controlled by Google, No. 20 M 297, 2020 U.S. Dist. LEXIS 165185, at *18–20 (N.D. Ill. July 8, 2020).

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

[54] *See* Charlie Warzel & Stuart A. Thompson, Opinion, *They Stormed the Capitol. Their Apps Tracked Them*, N.Y. TIMES (Feb. 5, 2021), https://www.nytimes.com/2021/02/05/opinion/capitol-attack-cellphone-data.html [https://perma.cc/EL8A-SL6C] (describing how Times reporters were "able to connect dozens of devices to their owners, tying anonymous locations back to names, home addresses, social networks and phone numbers of people in attendance"); Gennie Gebhart & Bennett Cyphers, *Data Brokers Are the Problem*, ELEC.

Second, and most importantly, the only information learned about any particular individual after the initial data dump is where he or she was during a short period of time, just as occurred with the checkpoint in *Lidster*.[55]

Thus, consistent with *Lidster*, a legislature might permit the first stage of geofencing if police can articulate to a judge why the requested area and time coordinates are likely to provide relevant information about the perpetrators of or eyewitnesses to a serious crime, and the judge then ensures that a geofence of smaller scope would be insufficient. If the police want to expand the geofence for particular phones, as contemplated in the second stage of Google's procedure,[56] they would need to provide additional justification for doing so. But again, given the limited information sought, probable cause would not be required. Nor would it be required at the unmasking stage, unless, perhaps, police had acquired multiple days of location data about the individuals they seek to unmask, thus triggering *Carpenter*'s ruling that access to significant amounts of CSLI must be authorized by a warrant.[57]

Note that the hassle rate for this type of procedure is minimal. It is true that a given geofence might, at the initial data dump stage, allow police access to the location information on hundreds or even thousands of people.[58] But none of these people—presumably whittled down to only a few individuals by the unmasking stage—will be *physically* hassled or even identified until after that stage. And what the police do after unmasking would be governed by traditional rules. Any subsequent arrest or custodial interrogation would, of course, require probable cause.[59] If instead the police merely want to question some or all of those who have been unmasked, they would be engaging in encounters no different than those the police have routinely conducted in traditional investigations, when they go from door to door in the area around a crime scene asking residents if they heard or saw anything.

The case of Jorge Molina, often cited as an example of how geofencing can go awry,[60] needs to be viewed with these considerations in mind. Based on a geofence investigation, police accosted Molina, stating that they knew "one hundred percent, without a doubt" that he had committed a murder.[61] Instead of checking out the possibility Molina had logged into an account on the phone of

FRONTIER FOUND. (July 23, 2021), https://www.eff.org/deeplinks/2021/07/data-brokers-are-problem [https://perma.cc/QB5M-BDRY] (describing how data brokers link sensitive data to real people).

[55] Gebhart & Cyphers, *supra* note 54.

[56] Ellis, *supra* note 41.

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

[58] *See* Ellis, *supra* note 41.

[59] Gerstein v. Pugh, 420 U.S. 103, 111 (1975) ("The standard for arrest is probable cause.").

[60] *See* Sidney Fussell, *Creepy 'Geofence' Finds Anyone Who Went Near a Crime Scene*, WIRED (Sept. 4, 2020), https://www.wired.com/story/creepy-geofence-finds-anyone-near-crime-scene/ [https://perma.cc/BHM5-L48C].

[61] *Id.*

his mother's boyfriend (who was later found to have committed the murder), the police immediately arrested Molina and put him in jail, where he spent six days before he was freed.[62] The police conduct in Molina's case had little to do with geofencing, and much to do with police willingness to act precipitously, without a full pre-arrest investigation.

III. TIVO DRONING AND AIR

Even less problematic under proportionality analysis is a visual version of geofencing operated by a company called Persistent Surveillance Systems. In a Baltimore program dubbed Aerial Investigation Research ("AIR"), the company used cameras on high-flying planes and drones to monitor the city during the daytime.[63] If a crime was caught on camera or otherwise came to the attention of the police, the aerial recordings could be used to trace the people and cars near the crime scene at the time it occurred, both forward and backward in time, to help identify who they were.[64] Because any individuals picked up on the cameras appeared merely as blurry dots, facial features were not observable.[65] The only information revealed about them was their location for a short period of time.[66] Consistent with *Lidster*'s admonition that the "gravity" of the state's interest be factored into the analysis,[67] legislative rules could, and Baltimore did, limit the types of crimes AIR was used to investigate.[68] Presumably, if people were identified by connecting them to certain locations, subsequent interviews, interrogations, stops and arrests would be governed by traditional Fourth and Fifth Amendment law.

Perhaps because of concerns about disparate racial impact, but also because of straightforward cost-benefit calculations, Baltimore discontinued its AIR program in 2021.[69] That response is, of course, the government's prerogative.

[62] *Id.*; Valentino-DeVries, *supra* note 20.

[63] *See* ANDREW R. MORRAL ET AL., RAND, EVALUATING BALTIMORE'S AERIAL INVESTIGATION RESEARCH PILOT PROGRAM: INTERIM REPORT, at ix (2021); *see also* Matthew Feeney, *Baltimore Air Surveillance Should Cause Concerns*, HILL (Aug. 25, 2016), https://thehill.com/blogs/pundits-blog/civil-rights/293329-baltimore-police-drones-should-cause-concerns [https://perma.cc/5TRX-8GNP].

[64] *See* Feeney, *supra* note 63.

[65] Craig Timberg, *New Surveillance Technology Can Track Everyone in an Area for Several Hours at a Time*, WASH. POST (Feb. 5, 2014), https://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html [https://perma.cc/NMG2-SAKM] (describing persons viewed through the technology as "indistinguishable from any other person").

[66] *See id.*

[67] Illinois v. Lidster, 540 U.S. 419, 427 (2004).

[68] MORRAL ET AL., *supra* note 63, at ix.

[69] Nathan Sheard, *Officials in Baltimore and St. Louis Put the Brakes on Persistent Surveillance Systems Spy Planes*, ELEC. FRONTIER FOUND. (Mar. 2, 2021), https://www.eff.org/fr/

But in *Leaders of a Beautiful Struggle v. City of Baltimore*, the Fourth Circuit took it upon itself to hold that, had the department not ended AIR, it would have found the program unconstitutional under the Fourth Amendment.[70] Relying on *Carpenter*, the fifteen member court held, 8–7, that the aerial surveillance that took place under AIR was a search.[71] It then went on to hold that this surveillance required a warrant, which of course is impossible to obtain until a specific crime has occurred, thus preventing the pre-crime and citywide recordings on which AIR depended.[72]

The court appeared to be particularly concerned about the fact that the program retained recordings of the movements of everyone caught on camera for forty-five days.[73] But those recordings were not accessed unless violent crime—a serious problem in Baltimore at the time—was caught on camera.[74] Further, as the district court had pointed in refusing to grant a preliminary injunction against the program, AIR images show only "a series of anonymous dots traversing a map of Baltimore."[75] In rebuking the lower court for relying on this fact, the Fourth Circuit correctly observed that the habitual behavior of those "dots" (such as starting and ending the day at home), "analyzed with other available information, will often be enough for law enforcement to deduce the people behind the pixels."[76] But if these deductions are made in the tiered manner described above in connection with geofencing investigations, with court orders required during a two- or three-stage whittling process, then *Lidster* and proportionality analysis would permit it.

IV. DNA MATCHING

Law enforcement's attempts to match crime-scene DNA with a profile in a DNA database are common today.[77] All fifty states and the federal government allow collection of DNA from convicted individuals and at least thirty-one states and the federal government allow collection of DNA from arrested

deeplinks/2021/03/officials-baltimore-and-st-louis-put-brakes-persistent-surveillance-systems-spy [https://perma.cc/GVX3-4HA5].

[70] Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 346 (4th Cir. 2021) (en banc).

[71] *Id.*

[72] *Id.* at 346–48.

[73] *Id.* at 344–45.

[74] *Id.* at 334; MORRAL ET AL., *supra* note 63, at 1–4 (describing Baltimore's violent crime problem and the role AIR could play in reducing its effects on Baltimore).

[75] *Leaders of a Beautiful Struggle*, 2 F.4th at 342.

[76] *Id.* at 343.

[77] Karen Norrgard, *Forensics, DNA Fingerprinting, and CODIS*, NATURE EDUC. (2008), https://www.nature.com/scitable/topicpage/forensics-dna-fingerprinting-and-codis-736/ [https://perma.cc/XJD2-XAGF].

individuals.[78] DNA profiles are also maintained both by publicly accessible databases, such as GEDmatch, and by private direct-to-consumer databases, like Ancestry.com, 23andMe, FamilyTreeDNA and My Heritage, that cater to people hoping to find relatives, learn about their ancestry, or discover health problems.[79] In querying these various databases, police hope for a direct match, but increasingly are also looking for partial "familial matches," which can often identify people to whom the perpetrator is related and allow police to construct a family tree that they hope includes the perpetrator.[80] The power of "familial searching" was illustrated by a 2019 study, which calculated that the three million-profile databank maintained by GEDmatch could, by itself, "be used to identify well over half of the people in the United States [with] European ancestry, either directly or through a relative who had contributed genetic information to the database"; the authors went on to predict that this figure would grow to over 99% as the database grew.[81]

In the most famous recent case involving DNA, police used the familial matching process to identify and arrest Joseph DeAngelo, the so-called "Golden State Killer" ("GSK") responsible for dozens of sadistic rape-murders.[82] After decades of dead ends, an officer (posing as a donor), got FamilyTree DNA to produce a profile of the DNA in the semen from one of the case's rape kits, and then sought matches from both FamilyTreeDNA's two million person database and GEDmatch's even larger database.[83] Unfortunately, the only match was to distant cousins, which meant there were too many individuals in the suspect pool to provide police with useful leads.[84] But then a civilian genealogy expert working with police, using the My Heritage database, identified some second cousins of the GSK who appreciably narrowed the pool, especially after females and others who could not or were unlikely to have committed the crime were excluded.[85] Police visited one of the second cousins and asked for her DNA,

[78] *DNA Sample Collection from Arrestees*, NAT'L INST. JUST. (Dec. 6, 2012), https://nij.ojp.gov/topics/articles/dna-sample-collection-arrestees [https://perma.cc/Z2U3-PZRS].

[79] *See* Van Ness, *supra* note 20.

[80] For a description of the process, see generally Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 293–94, 297–300 (2010).

[81] James W. Hazel & Christopher Slobogin, *"A World of Difference"? Law Enforcement, Genetic Data, and the Fourth Amendment*, 70 DUKE L.J. 705, 727 (2021); Yaniv Erlich, Tal Shor, Itsik Pe'er & Shai Carmi, *Identity Inference of Genomic Data Using Long-Range Familial Searches*, 362 SCI. 690, 690 (2018) ("[A] genetic database needs to cover only 2% of the target population to provide a third-cousin match to nearly any person.").

[82] Paige St. John, *The Untold Story of How the Golden State Killer Was Found: A Covert Operation and Private DNA*, L.A. TIMES (Dec. 8, 2020), https://www.latimes.com/california/story/2020-12-08/man-in-the-window [https://perma.cc/7B9N-VSZU].

[83] *Id.*

[84] *Id.*

[85] *See id.*

thinking that her brother might be the killer.[86] While that testing cleared the brother, it indicated that the GSK was related to women in another family tree that police were building using Ancestry.com's database, which narrowed the pool to six male suspects.[87] Only one of those six had the blue eyes that fit the genealogist's profile: DeAngelo, a white police officer.[88] Police then surreptitiously collected DeAngelo's DNA, first from the door handle of his car, and later from a discarded tissue.[89]

The fact that the DNA profiles used in the GSK case came from databases containing the profiles of people who submitted their DNA for purposes other than fighting crime bothered many people.[90] As even a relative of one of DeAngelo's victims stated, "Any time you are using a DNA service, it should be between you and the service."[91] The human "leads" in cases like the GSK case are subjected to heightened scrutiny despite being completely innocent of crime and perhaps even ignorant of the existence of their criminal relatives.[92] Because of backlash against police use of its database to solve another case, GEDmatch now allows its users to opt out of allowing law enforcement to use their profiles (and a high percentage have done so),[93] while companies like Ancestry.com tout their resistance to law enforcement requests.[94] Meanwhile, FamilyTreeDNA has gone the opposite direction, promoting the fact that police may use its services for crime scene matching.[95]

[86] *Id.*

[87] *Id.*

[88] Heather Murphy, *She Helped Crack the Golden State Killer Case. Here's What She's Going to Do Next*, N.Y. TIMES (Aug. 29, 2018), https://www.nytimes.com/2018/08/29/science/barbara-rae-venter-gsk.html [https://perma.cc/9VK2-3APB].

[89] Kathleen Ronayne, *Records: DNA from Tissue Led to Golden State Killer Arrest*, ASSOCIATED PRESS (June 1, 2018), https://apnews.com/article/north-america-us-news-ap-top-news-joseph-deangelo-arrests-16441bb64e374a56b3ba444f39a48461 [https://perma.cc/4AH3-GADF].

[90] St. John, *supra* note 82.

[91] *Id.*

[92] *See* SARA DEBUS-SHERRILL & MICHAEL B. FIELD, ICF, UNDERSTANDING FAMILIAL DNA SEARCHING: POLICIES, PROCEDURES, AND POTENTIAL IMPACT 5 (2017), https://www.ncjrs.gov/pdffiles1/nij/grants/251043.pdf [https://perma.cc/6T95-BU2A].

[93] Jon Schuppe, *Police Were Cracking Cold Cases with a DNA Website. Then the Fine Print Changed.*, NBC NEWS, https://www.nbcnews.com/news/us-news/police-were-cracking-cold-cases-dna-website-then-fine-print-n1070901 [https://perma.cc/64MM-LYM5] (Oct. 25, 2019).

[94] Peter Aldhous, *A Court Tried to Force Ancestry.com to Open Up Its DNA Database to Police. The Company Said No.*, BUZZFEED NEWS (Feb. 3, 2020), https://www.buzzfeednews.com/article/peteraldhous/ancestry-dna-database-search-warrant [https://perma.cc/RQ7W-FRNC] ("Ancestry and its main competitor, 23andMe . . . have publicly vowed to defend their customers' genetic privacy, and say they will fight efforts to open up their databases to searches by police.").

[95] *You Can Help*, FAMILYTREEDNA, https://www.familytreedna.com/join [https://perma.cc/4X5S-6DQL]; *Ed Smart, Father of Elizabeth Smart Teams Up with FamilyTreeDNA*, PR NEWSWIRE (Mar. 26, 2019), https://prn.to/2Z5QgcZ [https://perma.cc/2QNG-7P5U].

Some states ban certain familial matching practices, while other states and the federal government place restrictions on them.[96] However, under current Fourth Amendment doctrine, familial matching is likely to be immune to challenge.[97] Even if the Supreme Court decided to expand *Carpenter*'s rejection of the third-party doctrine to information other than CSLI, DNA matching can be distinguished fairly easily. The *Carpenter* majority opinion focused on two reasons for its decision requiring a warrant for CSLI: "[T]he exhaustive chronicle of location information casually collected by wireless carriers today," and the fact that CSLI "is not truly 'shared' as one normally understands the term [because] cell phones and the services they provide are . . . indispensable to participation in modern society."[98] As is true of geofencing and AIR, the personal information discovered through familial matching is minimal—a list of potential relatives.[99] And, at least when the database accessed is maintained by a private company like GEDmatch or Ancestry.com, it is also willingly shared (with the company), much more intentionally than one shares one's digitized location information with phone companies. Only if the DNA is compelled from the person, as occurs when people are arrested or convicted, does the second rationale have any purchase, and in that setting the Court has held, over a Fourth Amendment challenge, that the state's interest in identifying arrestees and solving crimes justifies obtaining the genomic information.[100]

Application of the proportionality principle would arrive at the same result but using different reasoning. The Court's second rationale in *Carpenter*—having to do with the extent to which information has been "shared" with a third party[101]—would not be relevant to Fourth Amendment analysis, unless the sharing amounts to exposure of the information to the public at large. As Justice Gorsuch recognized in his dissent in *Carpenter*, in reasoning that is consistent with other Court opinions,[102] when people bail their property to a third person they do so with the expectation the property will be maintained in accordance with the bailor's preferences.[103] The focus should be on privacy expectations, not on whether information in possession of a third party was surrendered voluntarily or instead obtained through coercion or trickery.

The first rationale, in contrast, is pertinent, because it goes to the type and amount of information that is accessible to the police, and thus its privacy valence. In *Carpenter*, Justice Gorsuch asked "can [the government] secure your DNA from 23andMe without a warrant or probable cause?" and went on to state

[96] *See* DEBUS-SHERRILL & FIELD, *supra* note 92, at 10.

[97] Murphy, *supra* note 80, at 330–40.

[98] Carpenter v. United States, 138 S. Ct. 2206, 2219–20 (2018).

[99] *See* DEBUS-SHERRILL & FIELD, *supra* note 92, at 2.

[100] Maryland v. King, 569 U.S. 435, 441–42, 449, 464–65 (2013).

[101] *Carpenter*, 138 S. Ct. at 2220.

[102] *See* Rawlings v. Kentucky, 448 U.S. 98, 105 (1980) (indicating that a valid bailment would support a "reasonable inference" of "normal precautions" to "maintain . . . privacy").

[103] *Carpenter*, 138 S. Ct. at 2268–69 (Gorsuch, J., dissenting).

that, while the answer would apparently be yes under the Court's cases prior to *Carpenter*,[104] application of the third-party doctrine to the DNA setting "is not only wrong, but horribly wrong."[105] Survey research that I carried out with James Hazel confirmed that view, at least as far as "society" is concerned.[106] We found that, on average, our sample of over 1,500 participants perceived unrestricted law enforcement access to public databases like GEDmatch and direct-to-consumer companies like Ancestry.com to be at least as intrusive as accessing the content of emails or texts and almost as intrusive as a search of one's bedroom.[107]

So, accessing DNA for matching purposes should be considered a search. But Justice Gorsuch's further assertion that a warrant should be required does not follow, at least if he had in mind a traditional warrant. First, of course, as with geofencing and TiVo droning,[108] a traditional warrant could not be obtained for the typical DNA familial matching process, since at the time the match is sought no suspect has been identified.[109] More importantly, from a proportionality perspective, a demonstration of probable cause to believe a match will be discovered should not be necessary. If a court authorizes the match query and no match is discovered, no privacy invasion of any kind has occurred; the hassle rate is zero. If instead, a direct or partial match occurs, personal data—specifically, identification of people related to a criminal suspect—will be revealed but, assuming standard limitations on the matching process, no other information (about, for instance, health predispositions[110]) will be disclosed.

Accordingly, Hazel and I proposed that when police want DNA profile data to determine whether a match or partial match exists, they should follow a reverse warrant process similar to the geofence process described above.[111] First, police would have to demonstrate probable cause to believe that the DNA sample they plan to submit for the matching procedure in fact comes from the perpetrator.[112] Second, they would have to demonstrate some reason to believe that the databases to which they plan to submit the sample will produce at least a partial match.[113]

[104] *Id.* at 2262.

[105] *Id.*

[106] *See* Hazel & Slobogin, *supra* note 81, at 745 tbl.1.

[107] *Id.*

[108] *See supra* notes 53–57, 76 and accompanying text.

[109] *See* Hazel & Slobogin, *supra* note 81, at 759–60.

[110] *Cf.* Maryland v. King, 569 U.S. 435, 464 (2013) (emphasizing that the DNA collected from arrestees in the program in question was analyzed "for the sole purpose of generating a unique identifying number against which future samples may be matched").

[111] Hazel & Slobogin, *supra* note 81, at 759–60.

[112] *Id.* at 759.

[113] *Id.*

Furthermore, as with geofencing, subsequent police actions should be governed by the Fourth Amendment. As occurred in the GSK case,[114] relatives might be asked for a DNA sample, but only a warrant based on probable cause could compel such a sample. Whether police can obtain a DNA sample from a suspect through covert means—as they did with DeAngelo[115]—is a slippery Fourth Amendment issue that will not be addressed here, although most courts have answered in the affirmative.[116]

V. FACIAL RECOGNITION

Probably the most controversial new police technology is facial recognition. Much in the news has been a company called Clearview, which claims to have scraped billions of images from public records on the web and social media and used them to train an algorithm that is able to identify those faces, with close to 100% accuracy, when later captured on CCTV, cellphones, and police body cameras.[117] According to BuzzFeed News, the company "hawked free trials of its technology to seemingly anyone with an email address associated with the government or a law enforcement agency and told them to 'run wild,'" and hundreds of agencies have taken it up on the offer, at least on a trial basis.[118]

Clearview's claim that its algorithm is accurate is highly suspect, especially with respect to identifying people of color, since its training sample contains fewer of them.[119] Civil rights groups are also concerned that Clearview's "face-prints" will be abused by police—for instance, to track down immigrants, identify protesters, and harass minority groups—and by private citizens—for

[114] *See* St. John, *supra* note 82.

[115] *See id.*

[116] Elizabeth E. Joh, *DNA Theft: Recognizing the Crime of Nonconsensual Genetic Collection and Testing*, 91 B.U. L. REV. 665, 699 & n.197 (2011).

[117] Ryan Mac, Caroline Haskins, Brianna Sacks & Logan McDonald, *Clearview AI Offered Thousands of Cops Free Trials*, BUZZFEED NEWS, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition [https://perma.cc/S6KZ-B43S] (Apr. 9, 2021). *See generally* Russell Weaver, *The Constitutional Implications of Drones, Facial Recognition Technology and CCTV*, 6 PUB. GOVERNANCE, ADMIN. & FINS. L. REV. 53 (2021).

[118] Mac, Haskins, Sacks & McDonald, *supra* note 117.

[119] *See* Tom Simonite, *Photo Algorithms ID White Men Fine—Black Women, Not So Much*, WIRED (Feb. 6, 2018), https://www.wired.com/story/photo-algorithms-id-white-men-fineblack-women-not-so-much/ [https://perma.cc/BXD5-AYU5] (reporting studies from MIT and Georgetown); *see also* Henry Kenyon, *ACLU Rips Clearview AI Claims of Facial Recognition Accuracy*, CQ ROLL CALL, Feb. 12, 2020, 2020 CQDPRPT 0115.

example, to find domestic abuse victims.[120] More generally, advocates are concerned that Clearview's services will "end privacy as we know it."[121]

Assume, as eventually is likely to be the case, that facial recognition technology ("FRT") evolves to the point that accuracy claims like Clearview's can withstand scrutiny. Under the Supreme Court's jurisprudence, a facial image on a public website or sent out over unrestricted social media would be "knowingly exposed" to the public, so scraping it would not violate the Fourth Amendment.[122] In any event, governments already possess, in their divisions of motor vehicles and other agencies, a vast treasure trove of images.[123] The FBI is spending more than a billion dollars expanding its Next Generation Identification system to include not only fingerprints and photos, but "iris scans . . . palm prints, gait and voice recordings, scars, tattoos, and DNA" legitimately obtained through other means.[124]

The Fourth Amendment question is not whether these images may be collected, but when government may use them to seek matches. For reasons I discussed at length in *Privacy at Risk*, a person should be able to expect privacy in public, based on what I called a right to anonymity,[125] or as others have put it, a right to obscurity.[126] An amalgam of freedoms—freedom of association, freedom to travel and freedom to define oneself—could be said to bolster such

[120] *Court Cases: ACLU v. Clearview AI*, ACLU, https://www.aclu.org/cases/aclu-v-clearview-ai [https://perma.cc/K9YN-T4SA] (May 11, 2022).

[121] Vera Eidelman, *Clearview's Dangerous Misreading of the First Amendment Could Spell the End of Privacy Laws*, ACLU (Jan. 7, 2021), https://www.aclu.org/news/privacy-technology/clearviews-dangerous-misreading-of-the-first-amendment-could-spell-the-end-of-privacy-laws [https://perma.cc/2X3Y-95L4]. As a result, the ACLU filed a suit claiming that Clearview was violating Illinois's Biometric Information Privacy Act, 740 Ill. Comp. St. 14/1 (2008), which resulted in a consent decree barring Clearview from providing its faceprint database to private entities and individuals (but not to law enforcement agencies) and allowing Illinois citizens to block their facial data from Clearview's database. *See* Consent Order of Permanent and Time-Limited Injunctions Against Defendant Clearview AI, Inc. at 2–4, Am. Civ. Liberties Union v. Clearview AI, Inc., No. 2020 CH 04353 (Ill. Cir. Ct. May 11, 2022).

[122] *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

[123] *See* Christopher De Lillo, Note, *Open Face: Striking the Balance Between Privacy and Security with the FBI's Next Generation Identification System*, 41 J. LEGIS. 264, 276 (2014–2015).

[124] Weaver, *supra* note 117, at 57; Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 431 (2014); *see Next Generation Identification (NGI)*, FED. BUREAU OF INVESTIGATION, https://le.fbi.gov/science-and-lab-resources/biometrics-and-fingerprints/biometrics/next-generation-identification-ngi [https://perma.cc/B64Z-FXAP]; De Lillo, *supra* note 123, at 269, 275–76.

[125] SLOBOGIN, PRIVACY AT RISK, *supra* note 28, at 90–91.

[126] *See generally* Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1355–69 (2015).

a right,[127] but the Fourth Amendment's prohibition on unjustifiably intrusive government actions, filtered through proportionality analysis, provides the most solid protection of this interest in public anonymity. In the absence of justification, FRT, which relies on capturing and matching one's image with images already collected,[128] should not be permitted.

However, proportionality analysis also suggests that, *with* justification, FRT should not be barred as an investigative tool. If police obtain a facial image from the scene of the crime, they should be able to seek a match if—analogous to the procedure outlined in connection with DNA matching—they can demonstrate that the image is likely that of the perpetrator or a key eyewitness and that there is a nontrivial chance a match will be found. At the same time, as suggested in connection with previous examples, legislation might limit use of FRT to investigations of serious crimes, with the aim of preventing harassment of people of color, protesters, or people who look "dirty."

Further, as with the previous examples of suspectless searches, a match should never automatically permit a stop or arrest. For instance, the New York Police Department's FRT policy states that, if a potential match is produced using FRT, an investigator is to make a visual comparison and perform a "detailed background check to confirm the reliability" of the match; further, the match is to be considered "an investigative lead only."[129] As the Supreme Court stated in *Illinois v. Gates,*[130] "[o]ur decisions applying the totality-of-the-circumstances analysis [in determining whether probable cause exists] have consistently recognized the value of corroboration of details of an informant's tip by independent police work."[131] The same should be true in this setting. In the absence of exigency, this independent corroboration should be seconded by a judge. It is too easy for officers in the field to confirm that an FRT match is in fact a match when no one is looking over their shoulder.

With these types of limitations, a ban on FRT may be an overreaction. Any technology can be misused. FRT that can accurately identify faces could be a very useful law enforcement technique. It reportedly has helped police track down suspects in hundreds of serious criminal cases.[132] FRT was also used to

[127] SLOBOGIN, PRIVACY AT RISK, *supra* note 28, at 98–104 (making these arguments, although also admitting that the Court's ungenerous interpretation of those rights make them tenuous).

[128] *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 16, at 3–4.

[129] N.Y.C. POLICE DEP'T, PATROL GUIDE PROCEDURE NO: 212-129, FACIAL RECOGNITION TECHNOLOGY (2020).

[130] Illinois v. Gates, 462 U.S. 213 (1983).

[131] *Id.* at 238–41.

[132] Ryan Saavedra, *'Groundbreaking' Clearview AI Technology Used to Take Down Alleged Child Sex Predators*, DAILY WIRE (Jan. 21, 2020), https://www.dailywire.com/ news/groundbreaking-clearview-ai-technology-used-to-take-down-alleged-child-sex-predators [https://perma.cc/AA24-MJYD].

identify people involved in the January 6, 2021 storming of the Capitol and those who committed crimes during the post-George Floyd protests.[133]

VI. ALERTS

FRT could aid law enforcement in still another way. Police could use a CCTV system equipped with FRT to scan faces on the streets for possible matches with known at-large criminals, in effect, generating self-executing "electronic wanted posters."[134] Automated License Plate Readers can carry out a similar function with respect to cars; in fact, most police ALPRs are tied into nationally generated "hot lists" of stolen cars and cars used to commit crime.[135] The reach of such alert systems could be vastly expanded by patching in private cameras, operated by both businesses and by homeowners, either through Cloud-based camera systems, such as Amazon's Ring, or independently of any such system.[136] There are many other types of alert systems using technology. For instance, every computer file has a unique identifier called a "hash value," essentially a computer fingerprint.[137] Analogous to its fingerprint database, the FBI maintains a database with the hash value of computer files containing child pornography.[138] Software has been developed that sifts through digital files looking for those associated with these values and then alerts when one is found.[139]

A common problem with all alert systems is the potential unreliability of the predicate for the alert. The federally maintained "terrorist" and "No Fly" watch lists are infamous for including numerous innocent people (including, at one point, Senator Edward Kennedy and Assistant Attorney General James Robinson).[140] Unless the government has demonstrated the requisite cause to believe that the basis for an alert (the face, car or hash value) justifies whatever post-alert action is to be taken (arrest, interrogation, exclusion from travel), alert

[133] U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-518, FACIAL RECOGNITION TECHNOLOGY: FEDERAL LAW ENFORCEMENT AGENCIES SHOULD ASSESS PRIVACY AND OTHER RISKS 18–20 (2021), https://www.gao.gov/assets/gao-21-518.pdf [https://perma.cc/32Z6-4DMR].

[134] *See* Andrew Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1116–26 (2021) (describing this and other uses of FRT).

[135] *Street-Level Surveillance: Automated License Plate Readers (ALPRs)*, *supra* note 18.

[136] *See* Christopher Frascella, Note, *Amazon Ring Master of the Surveillance Circus*, 73 FED. COMM. L.J. 393, 395 (2021).

[137] Ric Simmons, *Ending the Zero-Sum Game: How to Increase the Productivity of the Fourth Amendment*, 36 HARV. J.L. & PUB. POL'Y 549, 583 (2013).

[138] *Id.*

[139] *See* Marcia Hofmann, *Arguing for Suppression of 'Hash' Evidence*, 33 CHAMPION 20, 20 (2009); United States v. Reddick, 900 F.3d 636, 639–40 (5th Cir. 2018).

[140] *See Unlikely Suspects*, ACLU (Dec. 28, 2009), https://www.aclu.org/other/unlikely-suspects [https://perma.cc/ZM7T-4A4T] (discussing the many U.S. and foreign leaders who have been ensnared in the bureaucracy of government watch lists).

systems should be considered unconstitutional from the get-go. The following discussion assumes that this hurdle, which is not trivial, has been overcome.

On that assumption, one could try to justify all of these alert systems under the Supreme Court's decision in *United States v. Place*, involving a drug-sniffing dog.[141] In dictum, since converted into a holding, *Place* concluded that the Fourth Amendment does not apply to techniques that—like drug-sniffing dogs—discover only evidence of crime,[142] a phenomenon that some have dubbed a "binary search."[143] Arguably all of the alert-based searches described here are binary because, at least in theory, they are triggered only by information that is highly probative of crime—a wanted suspect, an automobile that is the fruit or instrumentality of crime, or pornographic material.[144] At the same time, these techniques, like dogs, vary significantly in the extent to which they *actually* alert only to criminal events or evidence.[145] While hash value software ("HVS") almost always correctly identifies pornographic images, most researchers have concluded that FRT has some way to go to approach that level of accuracy,[146] and ALPRs may be appreciably worse (even a study conducted by police produced an error rate of over 35%).[147]

Yet allegations of potential error did not seem to faze the Supreme Court when analogous arguments were made against a search based on an alert by a drug-sniffing dog.[148] Because canines can alert to trace amounts of drugs, the handler's unconscious suggestions, and even the smell of other dogs, their alerts can often be erroneous.[149] Thus, dog alerts are not always responding solely to contraband; in this sense, they are not really "binary." Yet in *Florida v. Harris*,[150] the Court, per Justice Kagan, held that "[t]he question—similar to

[141] United States v. Place, 462 U.S. 696, 698–700 (1983).

[142] *Id.* at 707 ("A 'canine sniff' by a well-trained narcotics detection dog . . . discloses only the presence or absence of narcotics, a contraband item. . . . Therefore, . . . exposure of respondent's luggage, which was located in a public place, to a trained canine—did not constitute a 'search' within the meaning of the Fourth Amendment."); *see also* Illinois v. Caballes, 543 U.S. 405, 409 (2005) ("[T]he use of a well-trained narcotics-detection dog—one that 'does not expose noncontraband items that otherwise would remain hidden from public view'—during a lawful traffic stop, generally does not implicate legitimate privacy interests." (citing United States v. Place, 462 U.S. 696, 707 (1983))).

[143] Lawrence Rosenthal, *Binary Searches and the Central Meaning of the Fourth Amendment*, 22 WM. & MARY BILL RTS. J. 881, 882 (2014).

[144] *See id.* at 882–83.

[145] *See id.* at 921–22.

[146] *See supra* notes 119 and accompanying text.

[147] Jason Potts, *Research in Brief: Assessing the Effectiveness of Automated License Plate Readers*, POLICE CHIEF, Mar. 2018, at 14, 14–15.

[148] Florida v. Harris, 568 U.S. 237, 246–48 (2013).

[149] *See, e.g.*, Robert C. Bird, *An Examination of the Training and Reliability of the Narcotics Detection Dog*, 85 KY. L.J. 405, 430–31 (1997) (discussing the false positives generated by drug sniffing dogs).

[150] Florida v. Harris, 568 U.S. 237 (2013).

every inquiry into probable cause—is whether all the facts surrounding a dog's alert, viewed through the lens of common sense, would make a reasonably prudent person think that a search would reveal contraband or evidence of a crime."[151] Strongly hinting that a dog that has successfully completed training can be used to detect drug odors,[152] *Harris* concluded that the state does not need to prove that its binary search technique is perfect.[153]

In a proportionality regime, that conclusion is correct, but with an important empirical caveat. The majority in *Harris* can be faulted for ignoring the fact that dogs that do very well during training can often do much worse in the field. Depending on how closely training samples reflect base rate drug possession on the streets, even "certified" dogs might have an inadequate real-world accuracy rate. Say, for instance, dog testers parade in front of a dog a group of people, 50% of whom have drugs on their person, and the dog accurately alerts 50% of the time, a figure that many agree can be a quantified stand-in for probable cause.[154] While, on its face, the dog's alerts may appear to satisfy *Harris*, in fact the dog is doing no better than chance. Even if the dog is correct 90% of the time, the accuracy rate generated during testing could well be an overestimate of what will happen in the field since, unlike the group in the test sample, most people do not carry drugs.[155] However, if dogs are instead tested under conditions that replicate the real world (e.g., only one test person in fifty has drugs on them), the success rate of a particular dog during certification is likely to carry over into the field. Dogs tested under realistic conditions that have accuracy rates over 50% should be seen as meeting *Harris*'s test, even though they do not produce truly "binary" results.

If this analysis of *Harris* applies, all three types of suspectless searches at issue here are probably permissible under proportionality analysis. Take first FRT and ALPR. Both FRT and ALPR have accuracy rates well above 50% under real-world conditions.[156] More importantly, the hassle rates associated with them are probably very low compared, for instance, to the use of drug-

[151] *Id.* at 248.

[152] *Id.* at 246–47.

[153] Christopher Slobogin & Sarah Brayne, *Surveillance Technologies and Constitutional Law*, 6 ANN. REV. CRIMINOLOGY (forthcoming 2023) (manuscript at 12) (on file with the *Ohio State Law Journal*); *Harris*, 568 U.S. at 240.

[154] *See* Ronald J. Bacigal, *Making the Right Gamble: The Odds on Probable Cause*, 74 MISS. L.J. 279, 338–39 (2004) (suggesting a range for probable cause of 40%–49% but cautioning against too much precision); Daniel A. Crane, *Rethinking Merger Efficiencies*, 110 MICH. L. REV. 347, 356 (2011) (noting that commentators estimate probable cause to be "in the 40–45 percent range").

[155] If testing is carried out appropriately, arguments that reasonable suspicion should be required before a dog can be used (based on Bayesian analysis) are inapposite. *See* Richard E. Myers II, *Detector Dogs and Probable Cause*, 14 GEO. MASON L. REV. 1, 12–18 (2006).

[156] Susan McCoy, Comment, *O'Big Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology*, 20 J. MARSHALL J. COMPUTER & INFO. L. 471, 478–79 (2002); Potts, *supra* note 147, at 14.

sniffing dogs in airports (something courts have upheld[157]). Even a dog that alerts falsely only one out of twenty times could subject a large number of innocent people to searches of their luggage and clothing, given the crowds in the typical airport. In contrast, because they are triggered by unique identifiers (a particular face, a particular license plate number) rather than an odor that is not person-specific, FRT and ALPR systems are likely to alert much less often than dogs, and thus, ineluctably, will have fewer erroneous alerts.

At the same time, even one false arrest based on an FRT or ALPR alert is significant hassle for the person involved. Given that fact, even if FRT identifies a person as a wanted felon and we assume FRT is highly accurate, police should never automatically arrest; rather, as they would if an informant named someone as a perpetrator, they should first seek corroboration and, in the absence of exigency, obtain a warrant. Again, the NYPD FRT policy noted above makes sense: before acting on an FRT match, investigators must make a visual comparison and perform a detailed background check to confirm the reliability of the match, and until then may consider the match "an investigative lead only";[158] I would add that any physical confrontation based on an FRT match ought to be authorized by a court. Similarly, if an ALPR alerts to a car, police should double-check the license number before engaging with the driver.

The HVS technique is much closer to the airport dog scenario; it scans hundreds or perhaps thousands of files.[159] Thus, even a very accurate HVS system could produce, over the breadth of cases, a large number of false positives and a high hassle rate. Once again, however, much depends on what law enforcement does after an HVS alert. Attempts at corroboration should be made prior to arrest or a search of the relevant computer (presumably based on a warrant). Moreover, only the identified file should be searched, not the entire computer, unless the initial search produces probable cause to do so. Under these circumstances, the HVS alert should be permissible as well.

VII. CONCLUSION

When police have information about a crime that gives them a profile of the suspect or, better yet, an image of the suspect, today's technology gives them numerous ways to use searches as a means of identifying or capturing that person, including geofencing, genomic sleuthing, facial recognition algorithms, and various types of alert systems. Most of these technologies involve querying databases about, or conducting visual surveillance of, large numbers of people. However, they usually do not require revelation of a significant amount of personal information about any identifiable individual. Often the information

[157] *See* United States v. Sundby, 186 F.3d 873, 876 (8th Cir. 1999) (citing cases).

[158] N.Y.C. POLICE DEP'T, *supra* note 129, at 1–2.

[159] Denae Kassotis, Note, *The Fourth Amendment and Technological Exceptionalism After* Carpenter: *A Case Study on Hash-Value Matching*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1243, 1249 (2019).

police already have gives them good cause for carrying out these minimally intrusive searches.

Nonetheless, to ensure against arbitrary use of technology and unnecessary intrusions on innocent people, courts should impose in general terms, and legislatures should implement in more detail, mechanisms for limiting both virtual hassle rates (the proportion of people whose personal information is accessed) and physical hassle rates (the proportion of people who are interviewed, stopped, interrogated, or arrested as a result of the suspectless search). Most importantly, suspectless searches should be closely tied to the event in question and be limited to investigation of serious crimes. If those steps are taken, and the technology is effective at what it purports to do, suspectless searches may end up being the most useful, least intrusive type of data-driven search.