SURVEILLANCE AND POLICING TODAY: CAN PRIVACY AND THE FOURTH AMENDMENT SURVIVE NEW TECHNOLOGY, ARTIFICIAL INTELLIGENCE AND A CULTURE OF INTRUSION?

Jon L. Mills & Caroline S. Bradley-Kenney[*]

Abstract

We are on the verge of a surveillance state. New technologies enable intrusions unimagined two decades ago. Our current culture voluntarily provides intimate personal details that are available to the world and to law enforcement. Current interpretations of Fourth Amendment privacy protections are failing to protect individuals from this brave new world. This Article describes the current state of technology, culture, and deficiencies in the law. We propose a specific test that can provide a workable approach to current and emerging intrusions. That test expands upon existing theories, like the mosaic theory and a reformation of the third-party doctrine, but also relies on the basic Fourth Amendment tenets to protect against unreasonable searches and a potential dragnet state. This Article considers how the test can apply to six intrusive technologies currently in use.

* Jon L. Mills is a Professor of Law, Dean Emeritus, and Co-Director of the Center for Governmental Responsibility at the University of Florida Fredric G. Levin College of Law. Caroline S. Bradley-Kenney was a judicial law clerk for Judge Anthony N. Lawrence III at the Mississippi Court of Appeals. She currently works as a judicial law clerk for Justice David Ishee at the Mississippi Supreme Court. She received a J.D. from the University of Florida Fredric G. Levin College of Law. We would like to thank Kyler Gray for his excellent work researching and revising this Article.

INTRODUCTION

In the contemporary world, personal safety and security are a top priority. Post-9/11 American society traded privacy for security, but this trade-off carries significant risks as technology continues to evolve. Our culture routinely exposes personal information including locations, reading lists, and even what people had for lunch. However, there is a concern about whether the totality of the current technology and our current data driven way of life have incrementally allowed the creation of a surveillance society. The ability of police and security officials to ensure public safety is greatly enhanced by a culture of sharing personal information, the availability of legal, warrantless surveillance tools, and artificial intelligence (AI). But along with greater safety, this new reality and specific surveillance tools can intrude on our private lives. These tools include tower dumps, automatic license plate readers (ALPRs), social media searches, geofencing, closed-circuit television (CCTV) surveillance, and Stingrays.[1] All information law enforcement gathers using these tools can be aggregated and analyzed by AI that can then create an in-depth profile of an individual and identify suspects.[2]

New technologies changed the playing field for law enforcement and security officials. In earlier times, obtaining detailed information on potential suspects might take law enforcement weeks or months of investigating. Now, information is available almost instantly from modern technologies and the Internet. A combination of the culture of disclosure and intrusion, new technologies available for surveillance, and AI to put all that information together creates an environment that places personal privacy at great risk. The Authors believe that these circumstances, taken together, have formed an ecosystem that is

1. For more on tower dumps, *see* Emma Lux, *Privacy in the Dumps: Analyzing Cell Tower Dumps Under the Fourth Amendment*, 57 AM. CRIM. L. REV. 109 (2020). For more on ALPRs, *see Street-Level Surveillance: Automated License Plate Readers (ALPRS)*, ELEC. FRONTER FOUND. (Aug. 28, 2017) [hereinafter *Street-Level Surveillance*], https://www.eff.org/pages/automated-license-plate-readers-alpr [https://perma.cc/2P6L-V8YU]. For more on geofencing, *see* Sarah K. White, *What Is Geofencing? Putting Location to Work*, CIO (Nov. 1, 2017, 12:43 PM), https://www.cio.com/article/288810/geofencing-explained.html [https://perma.cc/56MV-Q8ST]. For more on CCTV surveillance, *see What Is CCTV and How Does It Work? Your Questions, Answered*, SECURE IT SEC. CORP. (Dec. 8, 2020) [hereinafter *What Is CCTV*], https://www.secureitsecurities.com/blog/what-is-cctv-and-how-does-it-work-your-questions-answered [https://perma.cc/4L9F-GW62]. For more on Stingrays, *see* Kim Zetter, *How Cops Can Secretly Track Your Phone*, INTERCEPT (July 31, 2020, 7:00 AM), https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/ [https://perma.cc/6WWH-WDEQ].

2. However, even with all these modern tools and information, sometimes the wrong person is identified. Consider the story of Zachary McCoy who became the prime suspect for a burglary based on his geolocation during a bike ride. His fate is discussed more fully below.

dangerously close to creating what the Supreme Court might term a "too permeating police surveillance" state.[3]

To note, this Article does not suggest that law enforcement can never use technology to investigate future and current crimes. Some investigations logically occur before a warrant is necessary. With proper warrants and safeguards, technologies can be used to fight crime without burying individual rights. This Article argues that such safeguards must be placed on law enforcement's use of intrusive new technologies to ensure that personal and private information is protected.

Technologies have consistently outrun constitutional protections. The law has simply not kept up with new means of intrusion and the consequences of the current culture of intrusion and disclosure.[4] For example, the Fourth Amendment is designed to protect each of us from unreasonable search and seizure,[5] but determining what constitutes a search grows more challenging as search tools grow more sophisticated. Whether by warrantless wiretapping or warrantless GPS tracking, it is fair to say warrantless information gathering went on for some time before the Supreme Court determined that a particular practice of "gathering" was required to obtain a warrant.[6] The Fourth Amendment is not a declaration of national policy; it is a protection of individual rights against the government.[7] Nevertheless, enforcement of Fourth Amendment rights in specific cases does build a national policy brick by brick. Sometimes, those individual decisions may lead to broader prohibitions or standards. However, this policy is a patchwork, leaving gaps where protections are still needed. Pointedly, at this stage, the Fourth

3. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)) (internal quotations omitted).

4. "The Digital Era is characterized by technology which increases the speed and breadth of knowledge turnover within the economy and society." Jill Shepherd, *What Is the Digital Era?*, *in* SOCIAL AND ECONOMIC TRANSFORMATION IN THE DIGITAL ERA 1 (Georgios Doukidis et al. eds., 2004).

5. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.").

6. *See Carpenter*, 138 S. Ct. at 2221 ("Having found that the acquisition of Carpenter's [cell-site location information] was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records."); *see also* United States v. Jones, 565 U.S. 400, 404 (2012) (holding that attaching a GPS tracking device to a vehicle and using the device to monitor the vehicle's movements constitutes a search within the meaning of the Fourth Amendment).

7. *See What Does the Fourth Amendment Mean?*, U.S. COURTS, https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0 [https://perma.cc/8DSP-RSWP] (last visited Feb. 15, 2023) ("On one side of the scale is the intrusion on an individual's Fourth Amendment rights. On the other side of the scale are legitimate government interests, such as public safety.").

Amendment protects information from being used against an individual at trial, but it does not protect that information from being collected.[8]

Law enforcement has always gathered and stored information, but today new technology provides unprecedented reams of data and analytical capacity. In the digital era, information is more readily available than ever, and law enforcement can use AI to aggregate and source all of it. AI can categorize and flag information that would have taken weeks to process manually, even when manual processing would have been altogether impractical.[9] AI utilizes "machine learning" to process and sort gathered information.[10] AI takes a large quantity of information and sorts it—looking for patterns, making predictions, and organizing the information it has sorted.[11] Accordingly, AI profiling is a powerful tool in criminal investigations. Law enforcement can use a person's AI-generated profile to obtain a probable cause search warrant, allowing them to use even more invasive surveillance.[12]

Law enforcement has access to various modes of legal warrantless surveillance tools that gather information that is then sorted through AI to identify suspects in criminal investigations.[13] Many uses of these technologies *could* be considered searches. This Article considers six technologies that have been used in warrantless surveillance: tower dumps, ALPRs, social media, geofencing, CCTV, and Stingrays. Of these six tools, the U.S. Supreme Court has not ruled that any of them require a search warrant, although some state legislatures and some state courts have started regulating their use.[14] Additionally, the Court has not ruled

---

8. *See* Elizabeth Goitein, *The Government Can't Seize Your Digital Data. Except by Buying It.*, WASH. POST (Apr. 26, 2021, 6:00 AM), https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/ [https://perma.cc/GGB2-9CHA] (explaining that voluntarily disclosed information can be collected and that the warrant requirement in *Carpenter* can be evaded by buying data through intermediaries).

9. Steven Feldstein, *The Global Expansion of AI Surveillance*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Sept. 17, 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 [https://perma.cc/MW2B-CXND].

10. Ed Burns et al., *What Is Artificial Intelligence (AI)?*, TECHTARGET, https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence [https://perma.cc/AB4F-TLL2] (last visited Mar. 5, 2023).

11. Steven Bellovin et al., *When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 NYU J.L. & LIBERTY 555, 589 (2014).

12. *See* T.J. Benedict, Note, *The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest*, 79 WASH. & LEE L. REV. 849, 852 (2022) ("Courts provide little to no supervision over [facial recognition technology] in policing, especially when police use [facial recognition technology] to establish probable cause.").

13. KELSEY Y. SANTAMARIA, CONG. RSCH. SERV., R46541, FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT: SELECT CONSTITUTIONAL CONSIDERATIONS 1 (2020).

14. *See* E. Barlow Keener, *Facial Recognition: A New Trend in State Regulation*, WOMBLE BOND DICKINSON (Apr. 29, 2022), https://www.womblebonddickinson.com/us/insights/alerts/

on whether using AI data-sorting to identify a suspect constitutes a search. Arguably, AI's analysis of the information gathered by law enforcement is not a search but rather an evaluation of data. However, as this Article will discuss, there are troubling indications that available technology could facilitate the creation of a surveillance society. Consequently, it is essential to scrutinize warrantless gathering of information and to evaluate at what point the use of these tools should require a warrant.

To better understand the potential for intrusive surveillance, one should understand the various roles and duties that law enforcement and security officials play. As citizens, we want a law enforcement system that prevents crime, and when crime occurs, we want that system to identify the criminals for prosecution. To that end, law enforcement relies on various forms of technology to gather and process information efficiently. One form of criminal investigation is law enforcement gathering information on its own and storing it in various databases.[15] The gathered information can then be input into an analytical system that uses AI to sort the information and identify potential suspects.[16]

The information that law enforcement provides to the system can come in the form of fingerprints, photographs, DNA, and criminal records—all information that is usually already part of law enforcement's records. However, data can also be easily obtained by law enforcement through technologies like CCTV and ALPR cameras, which capture individuals' daily movements.[17] Some information is also readily available to law enforcement through the third-party doctrine.[18] Information from cell service providers and websites can be obtained through requests to the third-party vendors.[19] Regardless of the mode of information-gathering, law enforcement is not required to obtain a probable cause search warrant before obtaining these types of valuable, and often personal, information.[20]

---

facial-recognition-new-trend-state-regulation [https://perma.cc/BPG6-2L92] ("Several states and municipalities are seeking to protect persons from abuse of biometrics by private companies and by law enforcement.").

15. For example, CODIS is a database that local, state, and federal agencies can use to access DNA records. *Frequently Asked Questions on CODIS and NDIS*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet [https://perma.cc/LM3E-DLDY] (last visited Mar. 8, 2023).

16. *See* Benedict, *supra* note 12, at 854 ("For example, law enforcement agencies use [facial recognition technology] to try to match an image of a suspect against databases of driver's license photos or mugshots.").

17. *What Is CCTV*, *supra* note 1; *Street-Level Surveillance*, *supra* note 1.

18. H. Brian Holland, *A Third-Party Doctrine for Digital Metadata*, 41 CARDOZO L. REV. 1549, 1550 (2020).

19. *Id.* at 1596–97.

20. *Id.* at 1573.

If a threat occurs, law enforcement can input the vast collection of information it has gathered through various modes of surveillance technology into a system using AI.[21] After quickly sorting through the information, the system will identify a potential suspect or suspects. Once a target is identified, information-gathering strategies change; with probable cause, warrants can be issued for specific in-depth searches[22] because data has produced a probable suspect. A second scenario occurs when general data about the specific crime area may be useful. Instead of going to the scene and questioning witnesses, law enforcement can rely on technologies like CCTV, geofencing, tower dumps, ALPRs, and Stingrays to gather all information about a given location on a specific date. That information can be input into AI to quickly identify all potential suspects. Finally, if a specific person is a suspect, substantial data can be gathered about him or her without a search warrant,[23] using all of the technologies discussed in this Article.

Regardless of the scenario, if an incident occurs, law enforcement will seek information. The question is whether it is reasonable to obtain that information using the six technology tools that this Article will discuss. The tools are just examples of the multiple technologies that law enforcement uses, but these six provide excellent insight. It is likely that the initial gathering of information using these tools is so broad that there are not Fourth Amendment protections. However, once the use of those tools gets more specific—when a particular individual's information becomes the target—the Fourth Amendment is implicated.

Technology-facilitated investigations may become so comprehensive that they provoke policy questions about whether we are building a surveillance society. Allowing law enforcement to acquire and keep a database that contains individual citizens' information, obtained through sophisticated and opaque technologies, searchable on demand and without restrictions, may indeed give rise to a "too permeating police

21. *See Does the Fourth Amendment Block Cops from Using Artificial Intelligence?*, CRIME REP. (Nov. 6, 2018), https://thecrimereport.org/2018/11/06/does-the-fourth-amendment-block-cops-from-using-artificial-intelligence/ [https://perma.cc/B558-GGFG] ("The police today enjoy a surfeit of data that can be collected, stored, mined, and sifted through easily and cheaply: license plate data, social media posts, social networks, and soon our own faces.").

22. *See* Michael J. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 886–87 (2016) (noting that probable cause, rather than reasonable suspicion, is required for more intrusive searches).

23. *See* Bryan McMahon, *How the Police Use AI to Track and Identify You*, GRADIENT (Oct. 3, 2020), https://thegradient.pub/how-the-police-use-ai-to-track-and-identify-you/ [https://perma.cc/YWG2-G7JK] ("Technology and lax data and privacy laws have enabled the rise of dragnet surveillance systems that regularly search and seize critical data and devices from Americans without a warrant.").

surveillance" state.[24] Therefore the situation is two-fold: the law must protect individuals from intrusions by law enforcement, and our policies should ensure that investigations do not create a permeating surveillance state.

In this Article, we apply the traditional test of reasonable expectation of privacy from *Katz v. United States* to the various surveillance techniques and technologies that law enforcement can access in this digital world. Any location-related information derived from tower dumps, ALPRs, social media, geofencing, CCTV, and Stingrays may be judged based on the duration and detail of the information obtained. In other words, this Article critiques how much of a person's life is tracked by these technologies to reveal personal information that law enforcement would otherwise not be able to ascertain. The aggregate of the information is intrusive. There is a difference between a snapshot and a movie. The movie tells an entire story and presents a mosaic. The aggregation of mundane information can create an intimate profile. Intrusion can also occur based on acquisition of intimate information not acquired over a long period of time. One snapshot can be intrusive. If law enforcement obtains information about a person's health or financial data through cell phone data obtained from a tower dump, that information is not location data, but it is personal data.[25]

The first test we apply throughout this Article is the traditional two-part test from *Katz*.[26] Justice Harlan articulated the *Katz* test in his concurrence: to determine whether law enforcement's actions are a search, a court must look at (1) whether an individual has an actual, subjective expectation of privacy and (2) whether that expectation is one society is prepared to recognize as reasonable.[27] Determining an individual's subjective expectation of privacy means considering things like phone settings, social media privacy settings, and the policy implications of preventing a permeating police state.[28] The objective

---

24. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)) (internal quotations omitted).

25. Overlying these concerns is the third-party doctrine, how it is applied, and the need for it to be reworked.

26. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

27. *Id.*

28. *Reasonable Expectation of Privacy*, LAW SHELF EDUC. MEDIA, https://lawshelf.com/shortvideoscontentview/reasonable-expectation-of-privacy [https://perma.cc/G7A2-UFWQ] (last visited Mar. 3, 2023). Social media in particular presents unique questions regarding users' expectations of privacy. United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012). In the context of Facebook, the court in *Meregildo* explained:

> Facebook users may decide to keep their profiles completely private, share them only with "friends" or more expansively with "friends of friends," or disseminate

prong of this test concerns society's expectations, the third-party doctrine, and the public nature of some information.[29] Applying this test to modern technology and police surveillance tools is no easy task. To apply this test, we must look at the totality of the circumstances and the intimate nature of the information being obtained. It is likely that the general gathering of anonymized information is not a search, but when that general search turns specific and certain individuals become targets of legal warrantless surveillance, a search occurs.[30]

The second test we will apply is the mosaic theory, which will help us prove the subjective and objective prongs of *Katz*. The mosaic theory requires government action to be considered as a whole.[31] Specifically, instead of "asking if a particular act is a search, the mosaic theory asks whether a series of acts that [may not be] searches in isolation amount to a search when considered as a group."[32] The Massachusetts Supreme Judicial Court recently articulated how it applies the mosaic theory: to determine if government action constitutes a search that requires a warrant under the mosaic theory, the court must determine "whether the surveillance was so targeted and extensive that the data it generated, in the aggregate, exposed otherwise unknowable details of a person's

---

> them to the public at large. Whether the Fourth Amendment precludes the Government from viewing a Facebook user's profile absent a showing of probable cause depends, *inter alia*, on the user's privacy settings.
>
> When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment. However, postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected.

Id. (emphasis in original). Thus, the social media privacy settings that an individual selects can be an indicator of the individual's subjective expectation of privacy. *Id.*

29. Caitlin Campbell, *Mixed Signals: An Analysis of the Third-Party Doctrine as Applied to Warrantless Collection of Historical Cell Site Location Information*, ARK. J. SOC. CHANGE & PUB. SERV. (Apr. 4, 2018), https://ualr.edu/socialchange/2018/04/04/mixed-signals-analysis-third-party-doctrine-applied-warrantless-collection-historical-cell-site-location-information/ [https://perma.cc/53M7-52K6].

30. To note, the new technology doctrine from *Kyllo v. United States* should not be applicable to the digital era and law enforcement's use of surveillance technologies. That doctrine stands for the premise that law enforcement's warrantless use of technology that is not in "general public use" in order to search a home is unlawful. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001). However, applying this doctrine would mean that law enforcement could still use highly invasive technologies if they just wait a few months or years. This suggests that *Kyllo* may no longer be good law and is becoming obsolete in its applicability.

31. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2010).

32. Commonwealth v. Perry, 184 N.E.3d 745, 757 (Mass. 2022) (quoting Kerr, *supra* note 31, at 320) (internal quotations omitted).

life."[33] Further, the Massachusetts court explained that there are three concerns to consider when making this determination.[34] First, there is the concern of how much of an individual's public movement is revealed by the surveillance.[35] The second concern is what kind of information is obtained through the search, and the third concern is whether law enforcement could have achieved the same kind of surveillance and gathering using "traditional law enforcement techniques."[36] The mosaic theory guides our approach to each of the law enforcement technologies discussed below.

The challenge begins when attempting to prove the subjective prong of *Katz*. Under the subjective prong, it must be shown that an individual has an actual, subjective expectation of privacy.[37] Individuals do not voluntarily disclose information revealed by blanket surveillance such as health issues, relationships, and political preferences. For the objective prong, the issue is whether society views an intrusion as a violation of a reasonable expectation of privacy.[38] As the *Perry* court suggests, an intrusion becomes unreasonable when the surveillance reveals "otherwise unknowable details of a person's life."[39] That level of constitutionally unconstrained data gathering and searching may signal a permeating surveillance state. Therefore, the mosaic theory of the Fourth Amendment should be considered as a limitation on data gathering from tower dumps, ALPR imaging, social media, geofencing, CCTV footage, Stingrays, or the aggregation of information through AI. With these tests in mind, this Article moves to the first mode of surveillance technology: tower dumps.

I. TOWER DUMPS

Any time a cell phone is turned on, it connects to a cell tower every seven seconds,[40] and each connection to a cell tower registers the cell phone user's location.[41] Tower dumps allow law enforcement to gather data about the identity, activity, and location of any cell phone that

33. *Id.* (quoting Commonwealth v. Mora, 150 N.E.3d 297, 310 (Mass. 2020)) (internal quotations omitted).

34. *Id.* at 758.

35. *Id.*

36. *Id.*

37. *Id.* at 756; Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

38. Commonwealth v. Perry, 184 N.E.3d 745, 756 (Mass. 2022); *Katz*, 389 U.S. at 361.

39. *Perry*, 184 N.E.3d at 757.

40. *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. on Priv., Tech. & L. of the S. Comm. on the Judiciary*, 112th Cong. 228 (2011) (statement of the Am. Civ. Liberties Union), https://www.judiciary.senate.gov/imo/media/doc/CHRG-112shrg86775.pdf [https://perma.cc/BL85-R4NR].

41. *Id.*

connects to a specific cell tower during a one or two hour time frame.[42] To access this information, law enforcement must request records of every cell phone that connected to a cell tower in a certain area.[43] Law enforcement must make these requests to "cellular telephone providers" who have "detailed historical records" of their cell phone users.[44] Law enforcement's use of tower dumps as a legal warrantless surveillance tool poses a significant threat to an individual's reasonable expectation of privacy.

The danger of tower dumps was made clear during the summer of 2020 when thousands of Americans participated in the Black Lives Matter Protests.[45] Many protesters brought their cell phones with them, but most did not realize the risk that came with bringing their phones.[46] Throughout the summer, privacy experts warned protesters that law enforcement agencies had surveillance tools capable of tracking cell phones.[47]

Law enforcement's use of tower dumps is analogous to law enforcement's use of cell site location information (CSLI). In *Carpenter v. United States*, the Supreme Court ruled that the collection of an individual's CSLI was an unconstitutional warrantless search.[48] In *Carpenter*, law enforcement gathered CSLI information on a single person for 127 days.[49] The *Carpenter* Court ultimately held that the warrantless gathering of seven days of CSLI on a specific person was

---

42. John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (Aug. 11, 2015, 11:51 AM), https://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/ [https://perma.cc/HW8Y-ALSC].

43. Wendy J. Wagner, *Tower Dump Production Orders: Restricting Police Access to Cellular Records in R v. Rogers Communications*, GOWLING WLG (Jan. 18, 2016), https://gowlingwlg.com/en/insights-resources/articles/2016/tower-dump-production-orders-restricting-police-a/ [https://perma.cc/SFD8-WDFJ].

44. Hon. Brian L. Owsley, *The Fourth Amendment's Implication of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CON. L. 1, 5 (2013).

45. *See* Keeanga-Yamahtta Taylor, *Did Last Summer's Black Lives Matter Protests Change Anything?*, NEW YORKER (Aug. 6, 2021), https://www.newyorker.com/news/our-columnists/did-last-summers-protests-change-anything [https://perma.cc/8QNL-ATRT] ("On June 1st last year, a week after George Floyd was murdered, more than three hundred fires blazed across Philadelphia . . . . By that Saturday, June 6th, tens of thousands of people clogged the streets of downtown, demanding justice, proclaiming that Black Lives Matter.").

46. Thomas Germain, *How to Protect Phone Privacy and Security During a Protest*, CONSUMER REPS. (June 3, 2020), https://www.consumerreports.org/privacy/protect-phone-privacy-security-during-a-protest-a5990476708/ [https://perma.cc/YCV2-WTHP].

47. *Id.* This phenomenon is not unique to the Black Lives Matter Protests, but these protests are a manifestation of this risk. "Protests in the United States and elsewhere have been monitored in the past, and information gathered through digital surveillance has been introduced in situations where protesters have been prosecuted." *Id.* (internal quotations omitted).

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

49. *Id.* at 2212, 2217.

unconstitutional,[50] but the Court did not answer whether a shorter amount of time would be violative of someone's reasonable expectation of privacy.[51] Tower dumps involve the gathering of CSLI over a short amount of time and gathering data about hundreds of individuals in a specific area rather than one individual.[52] The question is whether there is a material difference between tower dumps and targeted CSLI collection as in *Carpenter*.

The tower dump is not targeted at an individual and covers a shorter period.[53] No warrant is required before law enforcement requests the information.[54] Because a warrant is not required, a law enforcement agency might seek to use a tower dump to investigate an incident in a particular area by identifying multiple individuals in the area. Part of the justification for allowing warrantless collection via tower dumps is the third-party doctrine, which is becoming a highly criticized area of law.[55] A tower dump is obtained through the third-party cell tower provider.[56]

Both the subjective and objective prongs of *Katz* are implicated in law enforcement's use of tower dumps. The process of using tower dumps to obtain vast amounts of information on hundreds of cell phones at a given location and during a certain period of time must be broken down to best understand the intrusive nature of this mode of surveillance. First, the whole of an individual's public movement at certain locations can be revealed by tower dumps.[57] With a tower dump, law enforcement

50. *See id*. at 2217 n.3 ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

51. *See* Emma Lux, *Privacy in the Dumps: Analyzing Cell Tower Dumps Under the Fourth Amendment*, 57 AM. CRIM. L. REV. 109, 113 (2020) ("[*Carpenter*] explicitly left open the question of whether governmental acquisition of historical CSLI for shorter periods of time, like tower dump CSLI, also triggers Fourth Amendment protections.").

52. *See* Mason Kortz & Christopher Bavitz, *Cell Tower Dumps*, BOSTON BAR ASS'N (Mar. 18, 2019), https://bostonbar.org/journal/cell-tower-dumps/ [https://perma.cc/VYZ7-8E43] ("A tower dump, by its nature, involves access to more users' data than historical CSLI does . . . . That said, a typical tower dump is confined in the sense that it covers both a small area and a relatively short time period—often a few hours or even a few minutes.").

53. *Id.*

54. *See id.* (explaining that a majority of courts have held that a warrant is not required to obtain a cell tower dump).

55. The third-party doctrine stands for the principle that whatever an individual discloses to a third party can be accessed by law enforcement without a warrant. RICHARD M. THOMPSON II, CONG. RSCH. SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 1 (2014).

56. Katie Haas, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions*, AM. CIV. LIBERTIES UNION (Mar. 27, 2014), https://www.aclu.org/blog/national-security/privacy-and-surveillance/cell-tower-dumps-another-surveillance-technique [https://perma.cc/ANJ6-MLGB].

57. *See id.* ("This is a cell tower dump: the practice of demanding an enormous amount of cell phone location information—anywhere from hundreds to hundreds of thousands of data points—in an effort to identify just a few suspects."); *see also* Kelly, *supra* note 42 (explaining

accesses the identity, activity, and location of cell phones that connected to a specific tower at a specific date.[58] In fact, a "tower dump . . . provides officers with CSLI from every device that connected to a particular cell site within a specified period; allowing law enforcement to infer that the owners of those devices most likely were present in that site's coverage area during that time."[59]

Additionally, law enforcement can potentially access very specific, identifying information about an individual. Individuals take their cell phones everywhere, so depending on which cell towers law enforcement is requesting information from, they could obtain deeply personal and private information about a user. People bring cell phones into public places, like grocery stores and schools, but also into private places like doctors' offices, their homes, and churches, to name a few. With tower dumps, intimate details of a cell phone user's life could be in law enforcement's hands in a matter of minutes.

Finally, this level of surveillance is not something law enforcement could achieve with traditional law enforcement techniques. Prior to tower dumps, law enforcement officers would have to identify suspects by questioning witnesses at the scene of a crime. Law enforcement did not have the ability to "secretly monitor and catalogue every movement of an individual."[60] By using tower dumps, law enforcement is able to quickly gather identifying information on thousands of people in a short amount of time. This identifying information provides information on a cell phone user's life, "revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[61]

The Court has yet to determine whether tower dumps are unconstitutional. However, in other contexts such as GPS monitoring, the wide-scale blanket collection of information over a period of time is considered intrusive.[62] If law enforcement is to collect that vast amount of location information over a specific period of time on cell phones, they should be able to state a reason. Indeed, there may be reasons such as a

---

that tower dumps give police officers the location of any phone that connects to a targeted cell phone tower).

58. Kelly, *supra* note 42.

59. Commonwealth v. Perry, 184 N.E.3d 745, 754 (Mass. 2022).

60. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018). Notably, the *Carpenter* Court explained how society at one time did not expect law enforcement to be able to track every movement of an individual's car. *Id.* This logic applies the same to tracking individuals themselves. Prior to the digital era, society did not expect law enforcement to have the ability to secretly track the movements of individuals. *Id.*

61. *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).

62. *See* United States v. Jones, 565 U.S. 400, 403–04 (2012) (finding that the government's use of a GPS tracking device on a suspect's vehicle for twenty-eight days constituted a search within the meaning of the Fourth Amendment).

shooting or terrorist event that would justify a tower dump. Regardless of the reason, law enforcement should be prohibited from such unrestricted access to a cell phone user's personal information through the use of tower dumps over an extended period of time.

II. AUTOMATIC LICENSE PLATE READERS

ALPRs are devices that use "high-speed cameras designed to capture a photograph of each and every passing license plate, combined with software that analyzes those photographs to identify the license plate number."[63] Law enforcement uses both their own ALPR devices and devices owned by vendors that have contracts with law enforcement.[64] These contracts allow officers to "access . . . private databases containing scans from private ALPRs and from other local and federal law enforcement agencies."[65] The U.S. Supreme Court has never addressed whether a warrant is required for law enforcement to obtain historical ALPR data.[66] However, some appellate courts have started deciding cases on this very issue.

The Ninth Circuit has held that a defendant lacked standing to challenge law enforcement's warrantless accumulation of ALPR data to determine where the defendant went after he kept a rental car past its return date.[67] The Massachusetts Supreme Judicial Court found that a limited use of ALPRs in a specific location did not violate a defendant's reasonable expectation of privacy.[68] Notably, the Massachusetts court implied that an extended use of ALPRs to constantly monitor someone's movements with more than four cameras, in more than one location, would violate a defendant's reasonable expectation of privacy.[69]

States have different rules for how long a specific piece of ALPR data can be stored. New Hampshire mandates that data on a vehicle that is not

63. AM. CIV. LIBERTIES UNION, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 4 (July 2013).

64. Ángel Díaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, BRENNAN CTR. FOR JUST. (Sept. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations#:~:text=Law%20enforcement%20use%20of%20ALPR,and%20federal%20law%20enforcement%20agencies [https://perma.cc/H4YB-G9FW].

65. *Id.*

66. *Id.*

67. United States v. Yang, 958 F.3d 851, 859 (9th Cir. 2020).

68. Commonwealth v. McCarthy, 142 N.E.3d 1090, 1106 (Mass. 2020).

69. *See id.* ("While we cannot say precisely how detailed a picture of the defendant's movements must be revealed to invoke constitutional protections, it is not that produced by four cameras at fixed locations on the ends of two bridges.").

associated with a crime be deleted in three minutes.[70] Arkansas requires that the data be deleted after 150 days.[71] ALPR data in California must be deleted after sixty days if it is not related to a felony case.[72] Georgia mandates that ALPR data be deleted after thirty months unless it is related to a "law enforcement purpose."[73] This means that the state in which an individual drives determines how long their personal information is stored.

Law enforcement having unfettered access to a long term, searchable, organized database containing photographs of individuals driving on a highway is concerning. Specifically, these images reveal the vehicle make and model, the license plate number, and the vehicle's location on a certain date and time.[74] In other words, the database creates a mosaic of the driver's movements. As courts have recognized, an unlimited record of vehicle movements can be intrusive,[75] which is why time limits make sense. If this type of information gathering is turned into targeted, individualized surveillance, the question is whether it violates the *Katz* standard and the mosaic theory. When the gathering of information becomes the action of law enforcement searching an ALPR database for a specific driver's movements, such gathering violates those standards.

Even though the collection and storage of images in ALPR databases is not a search, when law enforcement accesses the database to identify and track the movements of a specific driver, a search does occur. First, using ALPRs for this individualized surveillance implicates a subjective expectation of privacy, as it creates the potential for a permeating police state and permits law enforcement to track the daily movements of any driver they target.[76] ALPRs allow agencies to collect images of vehicles as they travel on specific roads and highways, revealing a driver's

---

70. Dave Davies, *Surveillance and Local Police: How Technology Is Evolving Faster Than Regulation*, NPR (Jan. 27, 2021, 12:51 PM), https://www.npr.org/2021/01/27/961103187/surveillance-and-local-police-how-technology-is-evolving-faster-than-regulation [https://perma.cc/6CNS-PY6J].

71. ARK. CODE ANN. §§ 12-12-1804(a) (2023).

72. *Automated License Plate Readers: State Statutes*, NAT'L CONF. OF STATE LEGISLATURES (Feb. 3, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx [https://perma.cc/8UFC-7X2V]; CAL. VEH. CODE § 2413(b) (West 2022).

73. *Automated License Plate Readers: State Statutes*, *supra* note 72; *see also* GA. CODE ANN. § 35-1-22(b) (2022).

74. *ALPR FAQs*, IACP (Aug. 8, 2018), https://www.theiacp.org/resources/alpr-faqs#:~:text=ALPR%20systems%20typically%20capture%20the,unit%20that%20captured%20the%20image [https://perma.cc/HQ5G-4C3N].

75. *See* United States v. Jones, 565 U.S. 400, 403–04 (2012) (holding that the police conducted a search within the meaning of the Fourth Amendment by using a GPS tracking device on a vehicle for twenty-eight days and collecting more than two thousand pages of data).

76. Yash Dattani, *Big Brother Is Scanning: The Widespread Implementation of ALPR Technology in America's Police Forces*, 24 VAND. J. ENT. & TECH. L. 749, 764 (2022).

movements on public roads.[77] Not only does this information provide a log of a driver's movements but it can also reveal intimate details of a driver's location or whereabouts at any specific time.[78] Justice Sotomayor even explained that giving law enforcement the ability to create a precise, comprehensive record of a person's movements threatens reasonable expectations of privacy.[79] Specifically, she stated, "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of her familial, political, professional, religious, and sexual associations."[80] Although Justice Sotomayor was writing about the use of GPS, her analysis can also apply to personal location data obtained through use of ALPRs. The major difference is that a GPS is attached to a car while an ALPR is not. But the resulting tracking information can result in the same location data. This is the type of intimate information that the mosaic theory prohibits. Notably, the Supreme Court has stated, "A person *does not surrender all Fourth Amendment protections* by venturing into the public sphere. To the contrary, 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[81]

Further, law enforcement has not always had this surveillance technology. Until the advent of ALPRs, law enforcement did not have the technology to gather a vast amount of information about every driver on a highway at a given location, date, and time. They also lacked the ability to obtain specific information on the location of drivers from months or years prior to their investigation. Now, that is possible. Although some states restrict ALPRs,[82] there is no Supreme Court determination that constant ALPR surveillance is an intrusion. The mosaic theory could well apply to continuous surveillance through ALPRs, depending on the facts. As it stands now, there is no consistent national policy on ALPRs.

---

77. *Id.* at 769.

78. *Id.* at 774.

79. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

80. *Id.* at 415.

81. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting Katz v. United States, 389 U.S. 347, 351–52 (1967)) (emphasis added) (brackets in original).

82. *See, e.g.*, ME. STAT. tit. 29-A, § 2117-A (2022) (explaining that ALPRs are prohibited except when used by law enforcement in Maine to "provid[e] public safety, conduct[] criminal investigations and ensur[e] compliance with local, state and federal laws"); MD. CODE ANN., PUB. SAFETY § 3-509(c) (LexisNexis 2022) (setting forth specific procedures for law enforcement in Maryland to follow in using ALPRs); VT. STAT. ANN. tit. 23, § 1607(c)(1)(A) (2022) ("Deployment of ALPR equipment by Vermont law enforcement agencies is intended to provide access to law enforcement reports of wanted or stolen vehicles and wanted persons and to further other legitimate law enforcement purposes. Use of ALPR systems by law enforcement officers and access to active data are restricted to legitimate law enforcement purposes.").

III. SOCIAL MEDIA

Seventy-two percent of Americans use at least one form of social media.[83] Social media allows users to share in real time what they are doing, where they are located, and how they are feeling while making new friends online. Unfortunately, this shared information has also become a treasure trove for law enforcement investigations. Seventy-three percent of law enforcement agencies believe "social media helps solve crimes more quickly."[84] Much of this information is available without a warrant.[85]

The third-party doctrine allows law enforcement to obtain information on social media sites without a warrant.[86] The doctrine states that when people voluntarily give information to third parties like banks, Internet service providers, and phone companies, they have no reasonable expectation of privacy in the information they provide.[87] However, with the evolving technologies in the digital era, the broad application of this doctrine is outdated and ignores the realities of contemporary society.

The logic of this doctrine was questioned as early as 1979. In fact, Justice Thurgood Marshall criticized this doctrine in his dissent in *Smith v. Maryland*: "Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[88] Justice Sotomayor also expressed her frustrations with the doctrine in her *United States v. Jones* concurrence and argued that it is time to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[89] Justice Sotomayor also went on to say that the third-party doctrine was "ill-suited" for the digital era because individuals share a "great deal of information about themselves

---

83. *Social Media Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/social-media/ [https://perma.cc/2DTF-UKAV].

84. LEXISNEXIS, SOCIAL MEDIA USE IN LAW ENFORCEMENT: CRIME PREVENTION AND INVESTIGATIVE ACTIVITIES CONTINUE TO DRIVE USAGE 3 (2014), https://centerforimprovinginvestigations.org/wp-content/uploads/2018/11/2014-social-media-use-in-law-enforcement-pdf.pdf [https://perma.cc/8TNF-JC5K].

85. *See id.* at 8 ("Social media information used to help establish probable cause for a search warrant continues to be widely accepted.").

86. *See id.* (explaining that social media information can be gathered by law enforcement before obtaining a search warrant, in order to establish probable cause); *see also* Harvey Gee, *Last Call for the Third-Party Doctrine in the Digital Age After Carpenter?*, 26 B.U. J. SCI. & TECH. L. 286, 288 (2020) (emphasizing that, by relying on the third-party doctrine, the government can "liberally glean the most intimate details" from communicative content, including social media messages).

87. THOMPSON II, *supra* note 55.

88. Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting).

89. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

to third parties in the course of carrying out mundane tasks."[90] Justice Sotomayor explained the dangers of the third-party doctrine in the digital age perfectly. Technology dominates all aspects of modern life. Individuals surrender vast amounts of personal information to third parties in the course of a normal day, but that surrender should not be considered a waiver of Fourth Amendment rights.

Nonetheless, courts continue to hold that individuals have no reasonable expectation of privacy in their social media posts. A New York court held that a Twitter user had no reasonable expectation of privacy in his tweets.[91] The U.S. District Court for the Southern District of New York found that law enforcement can constitutionally access a Facebook user's private profile through friends' profiles.[92] The court noted that having more secure privacy settings on a profile may reflect users' intent to protect their personal information, providing some constitutional protections.[93] The Connecticut Supreme Court suggested that posting personal information on social media waives any expectation of privacy in that information.[94] The Pennsylvania Court of Common Pleas held that communications on social media are not protected: "[N]o person choosing MySpace or Facebook as a communications forum could reasonably expect that his communications would remain confidential, as both sites clearly express the possibility of disclosure."[95] The U.S. District Court for the Northern District of Ohio held that the Fourth Amendment did not protect defendants from law enforcement adding them as friends on music sites to gather evidence.[96] The U.S. District Court of New Jersey held that a defendant's privacy rights were not

90. *Id.*

91. *See* People v. Harris, 949 N.Y.S.2d 590, 593 (N.Y. Crim. Ct. 2012) ("There can be no reasonable expectation of privacy in a tweet sent around the world.").

92. *See* United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) ("Where Facebook privacy settings allow viewership of postings by 'friends,' the Government may access them through a cooperating witness who is a 'friend' without violating the Fourth Amendment.").

93. *Id.* at 525.

94. *See* State v. Bruhl, 138 A.3d 868, 878 n.10 (Conn. 2016) ("The Appellate Court reasoned that the Facebook posts had to be exhibited in a 'public place,' . . . in order to be publicly exhibited . . . . [T]he Appellate Court concluded that to be publicly exhibited, the Facebook posts had to be accessible by the general public, and not only to 'Tasha Moore's' friends. Because we conclude that the trial court reasonably could have concluded that the posts were accessible to the general public on the facts of the present case, we need not decide whether a Facebook post that is accessible only to a user's network of friends is publicly exhibited . . . . We leave that question for another day.").

95. McMillen v. Hummingbird Speedway, Inc., No. 113-2010, 2010 WL 4403285 (Pa. Com. Pl. Sept. 9, 2010) (trial order op.).

96. United States v. Sawyer, 786 F. Supp. 2d 1352, 1356–57 (N.D. Ohio 2011).

violated when an officer followed the defendant on Instagram and discovered incriminating evidence.[97]

In evaluating law enforcement's access to social media, it is important to determine if an individual takes actions that demonstrate a desire to limit access to their information. For example, when a social media user chooses a private profile, that action can be an expression of an expectation of privacy.[98] In *Commonwealth v. Carrasaquillo*, the court evaluated whether the defendant had a reasonable expectation of privacy in a video he posted on Snapchat.[99] A law enforcement officer used a randomly generated username and requested to be Carrasaquillo's friend on Snapchat.[100] Carrasaquillo added the officer, and the officer recorded a video Carrasaquillo posted, which was later used against him at trial.[101] The court ultimately concluded that Carrasaquillo did not have a subjective expectation of privacy because he did not know what his privacy settings were and because he accepted more requests than those of people he knew.[102] The court also explained that there may be a subjective expectation of privacy in social media posts if the user has taken actions to "purposefully engage[] in conduct aimed at ensuring privacy."[103] Clearly, Carrasaquillo's actions were not taken to ensure his privacy.

Based on the logic of *Carrasaquillo*, a user who takes specific, intentional steps to protect their personal information can establish an expectation of privacy. For instance, a person may take intentional steps to program privacy settings to prevent Facebook friends from sharing their statuses or pictures.[104] In other platforms, individuals can also express an intent to protect their privacy. An individual can prevent their tweets from getting retweeted or can prevent their Instagram post from being shared by other profiles and limit viewing to specific people. There are not yet Supreme Court precedents on these various privacy options, but there is a reasonable argument that personal conversations, even if

97. United States v. Gatson, No. 13-705, 2014 WL 7182275, at *22 (D. N.J. Dec. 16, 2014), *aff'd*, 744 F. App'x 97 (3d Cir. 2018).

98. *See Meregildo*, 883 F. Supp. 2d at 525 ("[P]ostings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected.").

99. Commonwealth v. Carrasquillo, 179 N.E.3d 1104, 1108 (Mass. 2022).

100. *Id.* at 1110.

101. *Id.* at 1120.

102. *Id.* at 1117.

103. *Id.*

104. *See* United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) (explaining that Facebook users may "decide to keep their profiles completely private, share them only with 'friends' or more expansively with 'friends of friends,' or disseminate them to the public at large" and that because the defendant "maintained a Facebook profile in which he permitted his Facebook 'friends' to view a list of all of his other Facebook 'friends,'" the government did not violate the Fourth Amendment by viewing the defendant's profile through his friend's profile).

conducted over social media, can be limited. There are longstanding expectations of privacy in conversation and association[105]—two things that are prominent features of social media. Capturing social media posts can be highly intrusive. The nature of social media does not usually manifest a desire for privacy, but it can. If posts allow for large numbers of observers, it is difficult to argue that the user has a reasonable expectation of privacy. But intentional privacy limits may provide arguments against warrantless access. There is something disquieting about a law enforcement officer creating a fake profile to gain access to a social media profile.

Notably, the mosaic theory also provides some guidance. As a reminder, there are three concerns to consider when applying the mosaic theory to potential searches by law enforcement: how much of someone's public movement is revealed, the nature of the information revealed, and whether law enforcement could obtain this information using traditional techniques.[106] It is undeniable that a law enforcement officer looking at someone's social media profile is able to see a detailed mosaic of that person's life. In fact, part of social media posting involves sharing where a user has been—implicating the first concern of the mosaic theory. Social media allows law enforcement to see a great deal of someone's public movement by browsing photograph location tags, status updates, and location pins. Additionally, people share their thoughts on religion, politics, and current events on social media. They post photographs of family, for birthdays, and while on vacation. All of this information is very intimate in nature. Finally, social media provides law enforcement with an unprecedented amount of information on users—information that would never be achieved through traditional law enforcement techniques.

Ultimately, the protection of social media disclosures may well be decided around the evolution of the third-party doctrine in the digital age. As it stands, social media is a vast unprotected trove of personal information that law enforcement can easily access without a warrant. A rethinking of the third-party doctrine in the digital era may serve to create the best protections from social media intrusions by law enforcement.

IV. GEOFENCING

Geofencing is a "location-based service in which an app or other software uses GPS, RFID, Wi-Fi or cellular data to trigger a pre-programmed action when a mobile device or RFID tag enters or exits a virtual boundary set up around a geographical location, known as a

105. *See Carrasquillo*, 179 N.E.3d at 1114 ("Government surveillance of [social media] activity therefore risks chilling the conversational and associational privacy rights that the Fourth Amendment . . . seek[s] to protect.").

106. Commonwealth v. Perry, 184 N.E.3d 745, 758 (Mass. 2022).

geofence."[107] When law enforcement is unable to identify a suspect for a potential crime, officers can obtain a geofence warrant to get valuable location information from certain apps.[108] These warrants are different from search warrants. To obtain a geofence warrant, a law enforcement officer only needs to provide a specific place and time to a judge. Once that officer obtains judicial approval, companies will conduct searches of their databases to provide a list of cell phone numbers that were in that specific location at that specific time.[109]

Zachary McCoy, a University of Florida student, learned first-hand how law enforcement's use of geofencing warrants can lead officers to identifying a suspect, and in his case, the wrong suspect. In March 2019, McCoy was riding his bike in Gainesville, Florida, and tracking his ride on RunKeeper, a Google fitness app.[110] Months later, in January 2020, Google emailed McCoy and notified him that his data was being released to law enforcement because he had become a suspect in a burglary.[111] McCoy became a suspect after law enforcement obtained his location information from Google through a geofencing warrant.[112] McCoy ultimately fought to keep Google from releasing his personal information and won.[113]

Many states have allowed law enforcement to use geofence warrants to gain large amounts of personal location information.[114] These warrants "rely on the vast trove of location data that Google collects from Android users—approximately 131.2 million Americans—and anyone who visits a Google-based application or website from their phone, including Calendar, Chrome, Drive, Gmail, Maps, and YouTube, among others."[115] This is extremely concerning as most Americans use at least one Google

107. Sarah K. White, *What Is Geofencing? Putting Location to Work*, CIO (Nov. 1, 2017), https://www.cio.com/article/288810/geofencing-explained.html [https://perma.cc/5QPT-82MA]. RFID stands for radio-frequency identification.

108. Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2509 (2021) [hereinafter *Geofence Warrants*].

109. *Id.*

110. *Id.* at 2508.

111. *Id.*

112. Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect*, NBC NEWS (Mar. 7, 2020, 6:22 AM), https://www.nbcnews.com/news/us-news/google-tracked-his-buke-ride-past-burglarized-home-made-him-n1151761 [https://perma.cc/Z5ZN-TAF5].

113. *Id.*

114. *Geofence Warrants*, *supra* note 108 (stating that Arizona, Florida, Maine, Minnesota, New York, North Carolina, Texas, Virginia, Washington, D.C., Wisconsin, and other states have embraced the use of "sweeping geofence warrants").

115. *Id.* at 2512.

application: YouTube.[116] In fact, between 2017 and 2018, law enforcement's request for geofenced information from Google increased 1,500%, and it increased 500% between 2018 and 2019.[117] While Google is the most common corporation to receive these requests, Apple, Snapchat, Lyft, and Uber also receive them.[118]

Google has attempted to protect some of this information by implementing a three-step plan to prohibit "overly broad requests" from being fulfilled.[119] The first step Google takes is searching its location history database and producing an anonymized list of accounts, which contains "relevant coordinate, timestamp, and source information—present during the specified timeframe in one or more areas."[120] Next, law enforcement informs Google regarding which accounts it wants additional information on.[121] Finally, Google will provide "account-identifying information, such as first names, last names, and email addresses" of those users.[122]

It is harder to argue that an individual has an expectation of privacy in the *anonymized* account information that Google provides to law enforcement than when Google provides identifiable personal information. At that point, the Fourth Amendment becomes relevant for the following reasons, in accordance with the mosaic theory.

First, geofencing reveals the locations of any individuals in a given area at a given time.[123] Once that information is targeted toward a certain user, law enforcement knows when that individual was in a public space, allowing officers to have a better understanding of someone's public movements. Second, as explained above, after a simple request, law enforcement can obtain personal information on any anonymized account that may be deemed suspicious or that is in a suspicious location, turning this massive search of anonymized accounts into an investigation into a single individual.[124] This personal information contains highly intimate

116. *See* Brooke Auxier & Monica Anderson, *Social Media Use in 2021*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/ [https://perma.cc/293B-7SUA] (finding that eighty-one percent of Americans report that they use YouTube).

117. Cullen Seltzer, *Google Knows Where You've Been. Should It Tell the Police?*, SLATE (May 16, 2022, 11:04 AM), https://slate.com/technology/2022/05/google-geofence-warrants-chatrie-location-tracking.html [https://perma.cc/65JR-EFXE]. "In 2019, Google received about 9,000 geofence requests." *Id.*

118. *Geofence Warrants*, *supra* note 108, at 2512–13.

119. *Id.* at 2515.

120. *Id.*

121. *Id.*

122. *Id.*

123. Seltzer, *supra* note 117.

124. *Geofence Warrants*, *supra* note 108, at 2514–15.

content and includes email addresses, first names, and last names of users, at minimum.

Finally, geofencing technology allows law enforcement to obtain information that it normally would not be able to obtain through traditional law enforcement techniques like speaking to witnesses who were at the scene.[125] Law enforcement has not always had the ability to effortlessly obtain personal, identifying details about a person's whereabouts through the Internet, but geofencing provides them with this ability. In other words, geofencing now provides law enforcement with the ability to aggregate information on a person's whereabouts over a period of time, creating a mosaic of their life.

V. CLOSED-CIRCUIT TELEVISION

CCTV cameras that record activity in real time are in use across the world for security and law enforcement purposes. The U.S. Justice Department conducted a survey in 2001 indicating that sixty-three percent of participants say CCTV helps in criminal investigations, fifty-four percent say CCTV helps gather evidence, and twenty percent say CCTV helps in crime prevention.[126] Fifty million CCTV cameras are stationed throughout the United States as of 2020.[127]

Courts have started to establish when law enforcement's use of CCTV cameras constitutes a search. If CCTV covers public spaces, and the camera records activity in public, there is generally no broad expectation of privacy.[128] But there are exceptions. For example, in *United States v. Moore-Bush*, a federal judge granted a defendant's motion to suppress CCTV video footage of the defendant and her mother.[129] The CCTV camera was placed on an utility pole outside of the defendant and her mother's home, and the camera filmed their movement for eight months.[130] The camera could pan to numerous parts of the property, and

125. *Id.* at 2515–18.

126. Laura J. Nichols, *Use of CCTV/Video Cameras in Law Enforcement, Executive Brief*, U.S. DEP'T OF JUST., https://www.ojp.gov/ncjrs/virtual-library/abstracts/use-cctvvideo-cameras-law-enforcement-executive-brief [https://perma.cc/AXY7-PX3U] (last visited Mar. 17, 2023).

127. Sidney Fussell, *When Private Security Cameras Are Police Surveillance Tools*, WIRED (Aug. 11, 2020, 3:27 PM), https://www.wired.com/story/private-security-cameras-police-surveillance-tools/ [https://perma.cc/NP7Z-R5C9].

128. United States v. Knotts, 460 U.S. 276, 277 (1983).

129. United States v. Moore-Bush, 381 F. Supp. 3d 139, 141 (D. Mass. 2019), *rev'd*, 36 F.4th 320 (1st Cir. 2022). Although the district court's decision in *Moore-Bush* was reversed, other courts have applied the district court's reasoning to support similar decisions. *See, e.g.*, People v. Tafoya, 494 P.3d 613, 615, 621 n.8 (Colo. 2021) (holding that "police use of [a] pole camera to continuously video surveil Tafoya's fenced-in curtilage for three months, with the footage stored indefinitely for later review, constituted a warrantless search in violation of the Fourth Amendment" and explaining that the reversal of *Moore-Bush* did not change the court's decision).

130. *Moore-Bush*, 381 F. Supp. 3d at 141.

it could zoom in on activities occurring on the property.[131] Through this footage, law enforcement created a searchable log of the family's activities in and around their home.[132] The government did not have a warrant before it installed this camera, and it could not show probable cause for this surveillance.[133] The government argued that the video taken from the pole did not constitute a search under the Fourth Amendment.[134] The district court judge disagreed.[135]

The judge stated that there were two "basic guideposts" to shape society's understanding of an unreasonable search: "First, that the [Fourth] Amendment seeks to secure the 'privacies of life' against 'arbitrary power.' Second . . . that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'"[136] The court found that the defendant and her mother's actions of living in a residential neighborhood and in a house obstructed by a large tree showed "that they did not subjectively expect to be surreptitiously surveilled with meticulous precision each and every time they or a visitor came or went from their home."[137] The court also found the expectation to be reasonable based on *Carpenter*, stating that they had a reasonable expectation of privacy in their movements and their visitor's movements around the house for eight months.[138] The court also noted that those alive during the creation of the Fourth Amendment would be outraged if they discovered law enforcement "had managed to collect a detailed log of when a home's occupants were inside and when visitors arrived and whom they were."[139]

The *Moore-Bush* decision draws a logical line. When law enforcement uses CCTV to conduct twenty-four-hour surveillance of a home, that action constitutes an unreasonable search.[140] CCTV targeted at a home seems to be a clear overreach under the Fourth Amendment. Not only is the target specific, but also the continuous nature reeks of permeating surveillance. As the *Carpenter* Court explained, in drafting the Fourth

131. *Id.* The camera could not see into the home, but it could see license plates of vehicles that came and went from the home. *Id.*

132. *Id.* at 149–50.

133. *Id.* at 142.

134. *Id.*

135. *Id.* at 150.

136. *Moore-Bush*, 381 F. Supp. 3d at 142.

137. *Id.* at 144.

138. *Id.* at 146.

139. *Id.* at 148.

140. *See* People v. Tafoya, 490 P.3d 532, 542 (Colo. App. 2019) (finding that the police violated the Fourth Amendment when they used a video camera on a utility pole to continuously surveil defendant's house for three months), *aff'd*, 494 P.3d 613 (Colo. 2021). The Colorado appellate court nevertheless noted that "many of the courts to address the issue have concluded that continuous, long-term video surveillance of a private home via a non-trespassory pole camera does *not* constitute a 'search' under the Fourth Amendment." *Id.* at 538 (emphasis added).

Amendment, the Framers sought to prevent a "too permeating police" state.[141] Allowing law enforcement to have unlimited access to monitor a home and who visits it permits the permeating police surveillance that the Court warned of, and it provides an intimate look into the home—a constitutionally protected area. In sum, a subjective expectation of privacy exists when residents have taken specific actions to ensure their home will not be "surreptitiously surveilled with meticulous precision."[142]

Society expects privacy at home and is prepared to recognize it as reasonable. There is a long history of Supreme Court cases stating that the most protected sphere of privacy for an individual is their home.[143] Additionally, constant CCTV monitoring of a home reveals a deeply intimate mosaic of an individual's private life. First, it tracks the movement of all residents of a home and of all visitors of a home.[144] It also reveals extremely intimate information concerning private family life[145]—religion, political affiliations, and health, to name a few. Finally, it allows law enforcement to use cameras to get a closer look at a home that they otherwise would not be able to see into through traditional law enforcement techniques.[146] Arguably, law enforcement's use of CCTV to

141. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

142. *Moore-Bush*, 381 F. Supp. 3d at 150.

143. *See* Mapp v. Ohio, 367 U.S. 643, 660 (1961) (holding that the Fourth Amendment is made applicable to the states through the Due Process Clause, such that state residents are protected from unreasonable searches and seizures in their home by state police); Chimel v. California, 395 U.S. 752, 768 (1969) (establishing that the warrantless search of an individual's entire home is unconstitutional under the Fourth Amendment); Payton v. New York, 445 U.S. 573, 576 (1980) ("[T]he Fourth Amendment . . . prohibits the police from making a warrantless and nonconsensual entry into a suspect's home in order to make a routine felony arrest."); Kyllo v. United States, 533 U.S. 27, 34 (2001) ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use."); Florida v. Jardines, 569 U.S. 1, 11–12 (2013) ("The government's use of trained police dogs to investigate the home and its immediate surroundings is a 'search' within the meaning of the Fourth Amendment.").

144. *See* Brief of Amici Curiae Elec. Frontier Found. et al. in Support of Petitioner at 16, Tuggle v. United States, 142 S. Ct. 1107 (2022) (No. 21-541) ("[C]onstant and secret long-term surveillance makes it possible to learn intimate details about the lives of everyone in the household. For example, the police could identify everyone who visits the home by tracking the license plate of every car that parks in the driveway.").

145. *See, e.g.*, *id.* ("[Police] could deduce whether the occupants were expecting a baby, merely by the large boxes delivered to the home, and whether the occupants later lost that baby, by those same boxes being returned.").

146. *See id.* at 14–15 ("Although 'lawful conventional surveillance techniques,' such as a stakeout, might allow police to watch a suspect's activities for limited periods from public vantage points, digitally enabled surveillance is 'ever alert,' and its 'memory is nearly infallible.'").

monitor a home over any period of time is a search that requires a warrant.[147]

Additionally, the Fourth Amendment could be implicated when a public CCTV camera identifies a person on footage through law enforcement's use of facial recognition software.[148] Once an image has been captured by CCTV or otherwise, facial recognition technology can be used to personally identify an individual.[149] Then that image may be used to track multiple other images.[150] Applications like Clearview software say they have billions of images from the Internet and other locations.[151] Interestingly, Clearview has been limited in certain locations such as Canada and Australia.[152] Law enforcement frequently uses facial recognition, and some public opinion polls indicate that Americans think it is a good way to stop crime.[153] However, the combination of broad

147. Notably, the general surveillance of a public space through CCTV footage may not have the same protections. Additionally, modern technology can make CCTV monitoring even more dangerous with insect-size drones. In fact, a micro air vehicle, also called the bug drone, is being developed for future use by the U.S. Military for "in-the-open surveillance, aerial swarm operations, and battlefield situational awareness." Bruce Crumley, *Bug Off: US Military Planning Winged, Insect-like Microdrone*, DRONEDJ (June 18, 2021, 4:26 AM), https://dronedj.com/2021/06/18/bug-off-us-military-planning-winged-insect-like-microdrone/ [https://perma.cc/Z8DJ-EJ27]. Another danger of CCTV is the way it interacts with facial recognition technology. A single image of a person on a public street taken by a CCTV camera can be put into a facial recognition database, and large amounts of personal data can be gathered. *Facial Recognition: Who's Tracking You in Public?*, CONSUMER REPS. (Dec. 30, 2015), https://consumerreports.org/privacy/facial-recognition-who-is-tracking-you-in-public1-a7157224354/ [https://perma.cc/6N68-9KB8].

148. Theodore Claypoole, *A Clear Solution to Police Surveillance Creep: Warrants Needed for Biometric Analysis*, AM. BAR ASS'N (Aug. 3, 2020), https://www.americanbar.org/groups/business_law/publications/blt/2020/08/police-surveillance/ [https://perma.cc/P4G8-67JH].

149. *See* Benedict, *supra* note 12, at 854 ("This technology attempts to match one image of a face against a collection of facial images.").

150. *See id.* ("[L]aw enforcement agencies use [facial recognition technology] to try to match an image of a suspect against databases of driver's license photos or mugshots. Some [facial recognition technology] databases contain images gathered from social media or other sources without the consent of those photographed.").

151. *Company Overview*, CLEARVIEW AI, https://www.clearview.ai/ [https://perma.cc/JR4M-SZ77] (last visited Mar. 18, 2023).

152. *Announcement: Clearview AI Ordered to Comply with Recommendations to Stop Collecting, Sharing Images*, OFF. OF PRIV. COMM'R OF CANADA (Dec. 14, 2021), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/ [https://perma.cc/4GWS-THRN]; Byron Kaye, *Australia Says U.S. Facial Recognition Software Firm Clearview Breached Privacy Law*, REUTERS (Nov. 3, 2021), https://www.reuters.com/business/cop/australia-says-us-facial-recognition-software-firm-clearview-breached-privacy-2021-11-03/ [https://perma.cc/AEL9-YZXM].

153. Lee Rainie et al., *Public More Likely to See Facial Recognition Use by Police as Good, Rather Than Bad for Society*, PEW RSCH. CTR. (Mar. 17, 2022), https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-

CCTV surveillance, individual facial recognition, and gathering of other images with AI can create what reasonably can be termed a permeating surveillance state. One example is the proposed use of Amazon's Rekogniton software program in Orlando, Florida; the program uses CCTV, facial recognition, and AI to aide law enforcement.[154]

VI. STINGRAYS

A Stingray is a tool used by law enforcement to collect cell phone data.[155] These devices are able to "mimic cell phone towers and send out signals to trick cell phones in the area into transmitting their locations and identifying information. When used to track a suspect's cell phone, they also gather information about the phones of countless bystanders who happen to be nearby."[156] To note, Stingrays and tower dumps share similarities. However, Stingrays can gather a larger volume of cellphone data over an extended period of time.[157] States vary on whether Stingrays can be used without a warrant, but in 2015, the Department of Justice announced a new policy that requires federal agents to obtain a search warrant before using a Stingray.[158] While the federal government has taken an encouraging step in preventing warrantless police surveillance,

---

than-bad-for-society/ [https://perma.cc/K39L-YNQ4]; Geoff Kohl, *Extensive New Poll Finds Most Americans Support Facial Recognition*, SEC. INDUS. ASS'N (Oct. 7, 2020), https://www.securityindustry.org/2020/10/07/extensive-new-poll-finds-most-americans-support-facial-recognition/ [https://perma.cc/85NX-RM44].

154. Rekognition is a program that Amazon and the city of Orlando considered implementing that would conduct real-time facial recognition on a city-wide basis. The information generated by the software would be available to law enforcement. *See* Dawn Kawamoto, *Orlando Police to Launch Round of Two Facial Recognition Testing*, GOV'T TECH., https://www.govtech.com/public-safety/orlando-police-to-launch-round-two-of-facial-recognition-testing.html [https://perma.cc/X7LP-APJK] (last visited Mar. 18, 2023). Fortunately, Rekognition is no longer being piloted for use by Orlando police. *See* Nick Statt, *Orlando Police Once Again Ditch Amazon's Facial Recognition Software*, VERGE (July 18, 2019, 8:30 PM), https://www.theverge.com/2019/7/18/20700072/amazon-rekognition-pilot-program-orlando-florida-law-enforcement-ended [https://perma.cc/3UYN-2TCR].

155. Zetter, *supra* note 1.

156. *Stingray Tracking Devices: Who's Got Them?*, AM. CIV. LIBERTIES UNION (Nov. 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them#:~:text=Stingrays%2C%20also%20known%20as%20%22cell,their%20locations%20and%20identifying%20information [https://perma.cc/YKG9-MA4V].

157. ADAM BATES, CATO INST., STINGRAY: A NEW FRONTIER IN POLICE SURVEILLANCE 5 (2017).

158. U.S. DEP'T OF JUST., DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY *passim* (2015), https://www.justice.gov/opa/file/767321/download [https://perma.cc/SLM3-QWRD]; *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, U.S. DEP'T OF JUST. (Sept. 3, 2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators [https://perma.cc/GM24-BMXM].

we cannot overlook that prior to this 2015 order, federal agents were using Stingrays without a warrant since 1995.[159]

Some states do require law enforcement to obtain a warrant before using a Stingray. Those states are Washington, D.C.,[160] Florida,[161] New York,[162] California,[163] Maryland,[164] Virginia,[165] Minnesota,[166] Utah[167] and Washington.[168] However, all other states allow the warrantless use of Stingrays to gather information on potential suspects.

United States v. Ellis specifically evaluated the use of Stingray surveillance to determine whether the warrantless search and seizure of historical cell phone records revealing CSLI violates the Fourth Amendment.[169] Law enforcement used a Stingray to locate and arrest Ellis for shooting a police officer.[170] Ellis argued that the use of a Stingray to locate him constituted a warrantless search.[171] The district court ultimately concluded that Ellis had a reasonable expectation of privacy in his real-time cell location, stating "cell phone users have an expectation of privacy in their cell phone location in real time and that society is prepared to recognize that expectation as reasonable."[172] The court continued to say that cell phone users have "an even stronger privacy

159. *STINGRAYS: The Most Common Surveillance Tool the Government Won't Tell You About*, AM. CIV. LIBERTIES UNION N. CAL. (June 24, 2014), https://www.aclunc.org/publications/stingrays-most-common-surveillance-tool-government-wont-tell-you-about [https://perma.cc/FBB3-CYRN].

160. Jones v. United States, 168 A.3d 703, 717 (D.C. 2017).

161. Ferrari v. Florida, 260 So. 3d 295, 307 (Fla. 4th DCA 2018); Florida v. Sylvestre, 254 So. 3d 986, 992 (Fla. 4th DCA 2018).

162. N.Y. CIV. LIBERTIES UNION, MEMORANDUM: WARRANT REQUIREMENT FOR THE USE OF STINGRAYS IN NEW YORK 1 (2015), https://www.nyclu.org/sites/default/files/memo_stingrayuse_NY_201508_final.pdf [https://perma.cc/3NGP-9GQ4].

163. Cyrus Farivar, *California Cops, Want to Use a Stingray? Get a Warrant, Governor Says*, ARS TECHNICA (Oct. 8, 2015, 7:32 PM), https://arstechnica.com/tech-policy/2015/10/california-governor-signs-new-law-mandating-warrant-for-stingray-use/#:~:text=On%20 Thursday%2C%20California%20Governor%20Jerry,intercept%20calls%20and%20text%20messages [https://perma.cc/425J-G73Z].

164. State v. Andrews, 134 A.3d 324, 346–47 (Md. App. Ct. 2016).

165. VA. CODE ANN. § 19.2-70.3 (2022).

166. MINN. STAT. § 626A.28(3) (2022).

167. 2022 Utah Laws 77-23c-101.1.

168. WASH. REV. CODE § 9.73.260(1)–(6) (2022). The provisions require law enforcement to request an ex parte order authorizing the use of the device. *See id.* § 9.73.260(3)–(4). The request must include the type of data being collected, and law enforcement must take "all steps necessary" to permanently delete any information or metadata collected from any party not specified in the court order. *See id.* § 9.73.260(3), (6)(c). Additionally, law enforcement must delete the data from the target within thirty days if there is no longer probable cause to support the belief that such data is evidence of a crime. *See id.* § 9.73.260(6)(c).

169. United States v. Ellis, 270 F. Supp. 3d 1134, 1144 (N.D. Cal. 2017).

170. *Id.* at 1139.

171. *Id.*

172. *Id.* at 1145.

interest in real time location information associated with their cell phones, which act as a close proxy to ones' actual physical location because most cell phone users keep their phones on their person or within reach."[173]

Today, there is an actual subjective expectation of privacy in real-time location information from cell phones gathered over a period of time by law enforcement. As of 2022, seventy-seven percent of Americans own cell phones.[174] In other words, seventy-seven percent of the American population carries a device that can be accessed by a Stingray at any moment. This is concerning because, as the *Riley v. California* Court explained, "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet."[175] This allows law enforcement to build a mosaic of an individual's life, contributing to a permeating surveillance state.

This expectation in real-time location information from cell phones over a period of time is one society is prepared to recognize as reasonable. Law enforcement can use a Stingray to continuously monitor an individual's movements, and that data can be compiled to create a vast database of location information, tracking the public and private movements of individuals.[176] Additionally, the information from Stingrays provides a "precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[177] Further, the information gathered is information that law enforcement would not usually have access to if they relied on traditional police surveillance techniques, as it would take weeks or months to gather the same kind of information from interviewing witnesses or subpoenaing camera footage from businesses. Therefore, law enforcement's use of Stingrays constitutes unreasonable searches that should require warrants.

CONCLUSION

The technologies discussed above all raise concerns that law enforcement's use of data-gathering technologies and AI can create a permeating police surveillance state. New technologies must be subjected to the *Katz* test. First, the individual must have an actual, subjective

173. *Id.*

174. Deyan Georgiev, *67+ Revealing Smartphone Statistics for 2022*, TECHJURY (Feb. 26, 2022), https://techjury.net/blog/smartphone-usage-statistics/#gref [https://perma.cc/7UQQ-AJWN].

175. Riley v. California, 573 U.S. 373, 394 (2014).

176. Jones v. United States, 168 A.3d 703, 708 n.7 (D.C. 2017).

177. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

expectation of privacy in the information obtained by law enforcement.[178] Second, the violation must violate society's reasonable expectation of privacy.[179] An individual's reasonable expectation of privacy is violated through the use of these surveillance tools when a search yields data that is objectively intrusive. Surveillance is considered objectively intrusive based on the type of information or locations obtained, the intimate nature of the information that would be otherwise unknowable, and the aggregate of information that creates a detailed and intrusive mosaic of an individual's life.[180]

We cannot say that law enforcement's initial investigation using location-based technologies and other technologies available to investigate or prevent a criminal activity requires a search warrant. However, when technologies are combined to produce a comprehensive surveillance of all citizens, limitations are necessary. Also, when a general investigation converts to a specific investigation on an individual, the use of these technologies becomes a critical issue because they reveal a great deal of personal, intimate, and private intrusive information that law enforcement would not otherwise be able to access. To note, law enforcement does have databases like CODIS, which provide information about individuals.[181] However, the Authors' objection is to the government's use of technology to profile every citizen—an earmark of a surveillance state. Legislatures have already taken steps to limit some of these technologies, especially Stingrays, but there are not enough protections in place. In fact, private corporations like Clearview have databases to aid law enforcement with facial recognition.[182] There must be a policy that draws the line on the government gathering information on citizens, who may or may not have committed a crime. These policies are the best way to prevent the permeating surveillance society the Fourth Amendment was intended to protect us from.

The sum of tower dumps, ALPRs, social media, geofencing, CCTV, Stingrays, and AI provide the potential for collecting, analyzing, and creating a dossier without a warrant that then justifies a warrant. The new technology creates an information matrix that rivals or exceeds the abilities of the "thought police" from George Orwell's *1984* or the "precogs" from Philip K. Dick's *The Minority Report*. We have the Fourth Amendment for a reason. The Supreme Court has stated that "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to

178. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

179. *Id.*

181. Commonwealth v. Perry, 184 N.E.3d 745, 757–58 (Mass. 2022).

181. *See Frequently Asked Questions on CODIS and NDIS*, *supra* note 15 (explaining that CODIS is a database that agencies can use to access DNA records).

182. *Company Overview*, *supra* note 151.

'assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[183] In this Article, the Authors have provided guidance for where the courts can establish protections for individuals and their information. Additionally, the Authors have found that *Kyllo* is obsolete when new technologies are becoming publicly available so rapidly,[184] and the Authors have argued that the third-party doctrine must be limited in this new digital age. Further, a search warrant must be required when law enforcement's investigations become targeted and intrusive. There is a realm of privacy and individuality that must be protected from the government unless the government shows a good reason to intrude—that is, obtaining a warrant. The speed of technological innovation has outpaced the law, and it is time to draw a line.

183. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting Kyllo v. United States, 533 U.S. 27 (2001)) (brackets in original).

184. *See supra* note 30.