Note

Somebody's Tracking Me: Applying Use Restrictions to Facial Recognition Tracking

*Matthew E. Cavanaugh**

> A person does not surrender all Fourth Amendment protection by venturing into the public sphere.
>
> –Chief Justice John Roberts, *Carpenter v. United States*

> The future of surveillance is a future of use restrictions.
>
> –Orin Kerr

INTRODUCTION

In the very near future, the technology will be in place for all public movements to be recorded. As you walk down the street, a network of cameras will capture your movements and be able to identify you from your facial features. Facial-recognition-capable cameras will watch from shop windows, from telephone poles, and from body cameras worn by patrolling police officers. Every person will carry at least one such camera with them on their phone.

All of this data will be fed into centralized databases, where it can be stored indefinitely. At any time, the police will be able to enter your name into a database and review a log of every place your face has been recorded, including precisely how long you stayed there.[1] They will also be able to query a particular location for the names of anyone whose face was recorded there, including yours. They can do so on a

* J.D. Candidate 2021, University of Minnesota Law School. I would like to thank Professor Alan Rozenshtein for his thoughts and feedback throughout the Note-writing process. I would also like to thank the staff and editors of the *Minnesota Law Review* for their editorial work on this Note, especially Sarah Nelson and Melanie Griffith. Finally, I would like to thank Kelsey Goergen for her encouragement and support.

1. *See* Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 540–42 (2017) (describing combination of surveillance cameras and storage for later access).

hunch, and without constitutional oversight, because none of this constitutes a search under the Fourth Amendment.[2]

This future is closer than you may think. It is largely in place in China[3] and is rapidly progressing in the United States. Cities across the country are constructing massive networks of cameras equipped with facial recognition technology, with little oversight governing its use.[4] This detection apparatus is compounded by social media—in January 2020, the *New York Times* reported that police departments across the country are using Clearview, an app that enables its users to identify a person by comparing their face to a database of three billion photos compiled from Facebook, LinkedIn, and other social media.[5]

Rapid advances in technology in the twentieth century led to a growth in state surveillance power that was mostly unchecked by the courts. However, in 2018, the Supreme Court indicated a new approach to technological surveillance in the landmark decision *Carpenter v. United States*.[6] There, the Court held that the acquisition of seven days of cell-site location information (CSLI) records by police constituted a search.[7]

While *Carpenter* is a step in the right direction, constitutional gaps remain. One such issue is the distinction between how data is collected and how it is used, which has not been explicitly recognized

2. *See infra* Part II.B.

3. *See, e.g.*, Emily Feng, *How China Is Using Facial Recognition Technology*, NPR (Dec. 16, 2019, 4:24 PM), https://www.npr.org/2019/12/16/788597818/how-china-is-using-facial-recognition-technology [https://perma.cc/N5LX-3B7H] (describing Chinese facial recognition-powered surveillance apparatus that tracks individuals and groups them by ethnicity); *see also* Ross Andersen, *The Panopticon Is Already Here*, ATLANTIC (Sept. 2020), https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197 [https://perma.cc/NG4P-6V46] (describing China's extensive use of facial recognition to monitor its Uighur population); Richard Van Noorden, *The Ethical Questions that Haunt Facial-Recognition Research*, NATURE (Nov. 18, 2020), https://www.nature.com/articles/d41586-020-03187-3 [https://perma.cc/J6P2-PPXH] (same).

4. *See infra* Part I.B.

5. *See* Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/8DMW-73FD]; *see also* Ryan Mac, Caroline Haskins & Logan McDonald, *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, WalMart, and the NBA*, BUZZFEED NEWS (Feb. 27, 2020, 3:43 PM), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement [https://perma.cc/B4RW-GBR9]. Note that, at the time of this writing, Clearview and its use are surrounded by questions, both legal and otherwise.

6. 138 S. Ct. 2206 (2018).

7. *Id.* at 2217 n.3.

by the courts. The concept of use restrictions attempts to address this gap. Use restrictions are grounded in the idea that in a digital world, how data is *used* raises a distinct (and potentially more important) Fourth Amendment issue than how the data was acquired.[8] This Note argues that the Fourth Amendment limits the ability of law enforcement to track the population by using the fruits of facial recognition technology and that the courts should employ use restrictions to protect this right.

This Note proceeds in three Parts. Part I begins by describing how facial recognition technology works, how it can be used to track people, and the ongoing development of sophisticated networks of cameras and databases across the United States that will make such tracking possible. Part I concludes with an overview of how Fourth Amendment jurisprudence has developed alongside changing technology and policing methods in recent years, leading to the introduction of a new mode of analysis presented in *Carpenter*.

Part II argues that facial recognition tracking is a dangerous threat to liberty. It begins with a discussion of the effects of police surveillance on individuals and populations and explains why Fourth Amendment restraints on state power are distinct from concerns about a more general erosion of privacy. Part II then argues that both the collection of data and the use of that data can constitute potential Fourth Amendment searches and that even if facial identification is not considered a search, the aggregation of multiple points of identification to provide location information should be. Part II concludes by arguing that the unbridled use of a surveillance apparatus to track individuals' movements violates the Fourth Amendment right to be free from unreasonable searches.

Part III argues for a way forward through applying the Fourth Amendment to the use of facial recognition tracking based on the principles stated in *Carpenter*. Part III argues that (1) the use of seven days of aggregated facial recognition data constitutes a search under *Carpenter* and (2) any aggregation of such data should be considered a Fourth Amendment search. Part III argues that this approach strikes the proper balance between individual rights and society's broader interests and concludes by considering how this approach might interact with the reasonableness requirement of the Fourth Amendment.

8. *See* Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 50–53 (1995) (arguing that law enforcement's use of certain kinds of lawfully acquired information should be governed by the Fourth Amendment).

I. FACIAL RECOGNITION TECHNOLOGY, SURVEILLANCE AND POWER, AND THE FOURTH AMENDMENT

This Part provides an overview of facial recognition technology, how it can be used to track people, and how courts have struggled to apply the Fourth Amendment to surveillance technologies. It begins by describing the mechanics of facial recognition technology and how that technology can be used by law enforcement. It then describes the growth of a network of cameras equipped with facial recognition technology in American cities, as well as the large databases that enable the matching of a person's image to their identity. This Part concludes by describing the ongoing struggle of Fourth Amendment jurisprudence to reckon with the meaning of a "reasonable expectation of privacy" in the face of rapidly changing technology, culminating with *Carpenter v. United States*.

A. FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology is a computer process that uses artificial intelligence and machine learning to identify an individual by their facial features.[9] It is one of a series of technologies known as "biometrics," which use some physiological or behavioral characteristic to identity a person.[10] At a high level, facial recognition can be understood as a computer generating probabilities that an image of a person matches an image in a database.[11]

1. The Mechanics of Facial Recognition

The facial recognition process works as follows. First, an algorithm converts photos or images of human faces (called "probe

9. *See* Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, 34 CRIM. JUST. 9, 9–10 (2019). For an overview of the mechanics of the technology, see generally HANDBOOK OF FACE RECOGNITION (Stan Z. Li & Anil K. Jain eds., 2005) (describing the mechanics of pattern recognition broadly and facial recognition specifically).

10. *See* LISA S. NELSON, AMERICA IDENTIFIED 1 (2011) (providing an overview of biometrics and defining biometric technologies as "automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic").

11. *See generally The Complete Guide to Facial Recognition Technology*, PANDA SEC. (Oct. 11, 2019), https://www.pandasecurity.com/mediacenter/panda-security/facial-recognition-technology [https://perma.cc/ENB5-MYLC] (providing a comprehensive explanation of the facial recognition process); Adam Geitgey, *Machine Learning Is Fun! Part 4: Modern Face Recognition with Deep Learning*, MEDIUM (July 24, 2016), https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78 [https://perma.cc/2S99-DGA3] (describing machine learning process for facial recognition).

photos"[12]) to a numerical code, called a faceprint. Importantly, a probe photo can come from anywhere—it can be an image the system captures in real-time, a photograph taken in the past, or an image of a person pulled from their social media page.[13] The facial features analyzed by a facial recognition system include "nodal points," which are distinguishable landmarks on an individual's face.[14] Because any given individual has around eighty nodal points, facial recognition programs are able to use each individual's face to assign that individual a unique identifying number.[15]

Once the probe photo becomes a number, the next step is for the algorithm to match that number against a database of photos, i.e., codes, to generate a probability that the probe photo is the person in the database.[16] For facial recognition technology to effectively identify an individual, the system must have access to a database of photos to compare against the probe photo.[17] Each photo in the database is converted to a unique value (a "template") using the same process that creates a numerical value for probe photos.[18] Then, an algorithm compares the two values, resulting in a similarity or "match" score that estimates the probability that the photos are of the same person.[19]

12. *See* Hamann & Smith, *supra* note 9, at 10. For one example of this terminology being used by a law enforcement agency, see U.S. DEP'T OF HOMELAND SEC., FACE RECOGNITION POLICY DEVELOPMENT TEMPLATE (2017) (referring to "probe photos" throughout the document).

13. *See, e.g.*, PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., ONGOING FACE RECOGNITION VENDOR TEST (FRVT) PART 2: IDENTIFICATION 2 (2018) (describing probe photos as including "reasonably well-controlled live portrait photos" as well as "more unconstrained photos" including "webcam images . . . photojournalism and amateur photographer photos . . . and faces cropped from surveillance-style video clips"). For a discussion of probe photos coming from police body cameras, see generally JENNIFER LYNCH, FACE OFF: LAW ENFORCEMENT USE OF FACE RECOGNITION TECHNOLOGY 4–6 (2020). A probe photo can even be based on a lookalike. *See* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. L. CTR. ON PRIV. & TECH. (May 2019), https://www.flawedfacedata.com [https://perma.cc/NQA9-8DUK] (describing the use of a web image of Woody Harrelson as a probe photo when the detective thought the suspect resembled Harrelson).

14. *See The Complete Guide to Facial Recognition Technology*, *supra* note 11.

15. *Id.*

16. NELSON, *supra* note 10, at 39.

17. *See id.* ("The extracted features are compared against the stored [database] templates to generate match scores . . . ."); Van Noorden, *supra* note 3.

18. *See* NELSON, *supra* note 10, at 38; *see also* SEC. INDUS. ASS'N, FACE FACTS: DISPELLING COMMON MYTHS ASSOCIATED WITH FACIAL RECOGNITION TECHNOLOGY 2, https://www.securityindustry.org/wp-content/uploads/2019/06/facial-recognition-20193.pdf [https://perma.cc/6TD2-WKJ9].

19. NELSON, *supra* note 10, at 39; *see also* SEC. INDUS. ASS'N, *supra* note 18.

The rate at which facial recognition systems are able to accurately match a probe photo to a database photo is rapidly improving through the use of artificial neural networks, also known as machine learning.[20] These networks are self-improving; the more photos they are able to access, and the more times they go through the matching process, the more accurate they become.[21]

Despite these improvements, facial recognition is still an imperfect technology—it can falsely identify a person who should have been accepted ("false acceptance") or reject a person who should have been identified ("false rejection").[22] Of particular concern, facial recognition is more likely to misidentify minorities[23] and women.[24] For example, in 2018, Amazon's Rekognition[25] incorrectly identified twenty-eight members of the United States Congress as other people who had previously been arrested for a crime.[26] The incorrect matches were

20. *See* Oleksii Kharkovyna, *An Intro to Deep Learning for Face Recognition*, MEDIUM (June 26, 2019), https://towardsdatascience.com/an-intro-to-deep-learning-for-face-recognition-aa8dfbbc51fb [https://perma.cc/FJ8X-2SQZ] (explaining deep learning and how it is used by facial recognition); *see also* GROTHER ET AL., *supra* note 13 ("The major result of the evaluation is that massive gains in accuracy have been achieved in the last five years (2013–2018) and these far exceed improvements made in the prior period (2010–2013).").

21. *See* Kharkovyna, *supra* note 20.

22. *See* NELSON, *supra* note 10, at 40–41.

23. *See* Natasha Singer & Cade Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html [https://perma.cc/3DGX-T4AN]; *see also* Garvie, *supra* note 13 (describing general biases in facial recognition).

24. This is largely attributable to the fact that these populations are underrepresented in photo databases. *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. OF MACH. LEARNING RSCH. 1–15 (2018).

25. Amazon advertises its Rekognition software as "provid[ing] highly accurate facial analysis and facial search capabilities that you can use to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases." *See Amazon Rekognition*, AMAZON, https://aws.amazon.com/rekognition [https://perma.cc/9LSA-MFCR]. Its customers include the NFL, CBS, and National Geographic. *Id.* Amazon has faced criticism and pressure from investors over its role in the facial recognition market. *See* Natasha Singer, *Amazon Faces Investor Pressure over Facial Recognition*, N.Y. TIMES (May 20, 2019), https://www.nytimes.com/2019/05/20/technology/amazon-facial-recognition.html [https://perma.cc/53C7-5WNX]. In June 2020, Amazon placed a one-year moratorium on police use of its Rekognition software. *See* Karen Weise & Natasha Singer, *Amazon Pauses Police Use of Its Facial Recognition Software*, N.Y. TIMES (June 10, 2020), https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html [https://perma.cc/HD7A-TKVL].

26. Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (July 26, 2018, 8:00 AM), https://www.aclu.org/blog/

disproportionately people of color.[27] This problem underlies one of the common critiques of facial recognition today—that it is not accurate enough to use in policing.[28] Although databases are becoming more representative and accuracy is improving,[29] the concerns described throughout this Note are exacerbated for both minorities and women. A full exploration of these issues is beyond the scope of this Note, but they are at the forefront of the broad concerns posed by facial recognition technology.

2. Types of Facial Recognition, Including Facial Identification and Face Tracking

Facial recognition technology can be used in many different ways by a broad range of actors in society.[30] Professor Andrew Ferguson defines the four main types of facial recognition used for law enforcement purposes as (1) face surveillance, (2) face identification, (3) face tracking, and (4) face verification.[31] "Face surveillance" refers to the

privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [https://perma.cc/V3U7-VVGX].

27. *Id.*

28. *See, e.g.*, Garvie, *supra* note 13; Buolamwini & Gebru, *supra* note 24, at 2; Davide Castelvecchi, *Is Facial Recognition Too Biased To Be Let Loose?*, NATURE (Nov. 18, 2020), https://www.nature.com/articles/d41586-020-03186-4 [https://perma.cc/CDS2-5CT8]; Tawana Petty, *Defending Black Lives Means Banning Facial Recognition*, WIRED (July 10, 2020), https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition [https://perma.cc/J2GG-768E].

29. *See* Castelvecchi, *supra* note 28 (describing "significant improvement" in face-recognition accuracy). IBM is working to create a more diverse database, and some researchers allege that improved algorithms have accuracy rates for African Americans that are equal to that of Caucasians. *See* Krishnapriya K.S., Kushal Vangara, Michael C. King, Vítor Albiero & Kevin Bowyer, Characterizing the Variability in Face Recognition Accuracy Relative to Race (Apr. 2019) (unpublished manuscript), https://arxiv.org/ftp/arxiv/papers/1904/1904.07325.pdf [https://perma.cc/DX82-C2RC]; *see also* GROTHER ET AL., *supra* note 13.

30. *See* Sharon Nakar & Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 B.U. J. SCI. & TECH. L. 88, 96 (2016) (describing "the many and broad uses" of facial recognition including "security, commerce, social media, personal use, and even for religious purposes" (footnotes omitted)). Note that, at the time of this writing, facial recognition surveillance has been deployed around the world to track the spread of the novel coronavirus. *See* Natasha Singer & Chloe Sang-Hun, *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, N.Y. TIMES (Apr. 17, 2020), https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html [https://perma.cc/U4GN-MCU9]; Antoaneta Roussi, *Resisting the Rise of Facial Recognition*, NATURE (Nov. 18, 2020), https://www.nature.com/articles/d41586-020-03188-2 [https://perma.cc/X6M9-MFLB].

31. *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1116–28 (2021). Note that face verification, which is generally

generalized monitoring of a public space.[32] Face identification matches a particular person (individualized suspicion is present).[33] Facial recognition tracking, or "face tracking,"[34] combines the two—it describes the practice of obtaining information about an individual's movements using aggregated data obtained via facial identification.[35]

There are basic similarities between tracking with CSLI and facial recognition tracking. Just as cell phone providers can store information about a person's location,[36] facial recognition tracking could enable law enforcement or third parties to track a person's whereabouts based on where their face appears.[37] The key distinction between facial recognition tracking and other uses of facial recognition is the locational component—it is not simply identifying a person at one point in time, but instead is identifying a person at multiple points and aggregating those points to create a record of movements. This tracking can be done in real-time (as one's face appears in front of a camera at various points) or retrospectively (by aggregating stored images of captured movements).

In thinking about how facial recognition tracking works, it is helpful to understand the concept of the "data life cycle."[38] Data is generated in myriad ways, from making a phone call to visiting a website to crossing the path of a camera. Once generated, data can then be collected, stored, and analyzed.[39] "Use" occurs when any action is taken

used to confirm that a person is who they say they are, is not relevant to the issues discussed in this Note.

32. *Id.* at 113.

33. *Id.* at 117.

34. Throughout this Note, the terms "face tracking" and "facial recognition tracking" are used to refer to the use of facial recognition data to produce information about that person's movements.

35. *Id.* at 120.

36. *See* NAT'L ASS'N OF CRIM. DEF. LAWS. & SAMUELSON L. TECH. & PUB. POL'Y CLINIC AT U.C. BERKELEY, CELL PHONE LOCATION TRACKING (2016), https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf [https://perma.cc/5WVX-JPZV].

37. *See* Jens-Martin Loebel, *Is Privacy Dead?—An Inquiry into GPS-Based Geolocation and Facial Recognition Systems*, IFIP INT'L CONF. ON HUM. CHOICE & COMPUTS. 338, 343 (2012) (describing the mechanics of how facial recognition and GPS location systems can be used together). A service that allows employers to use facial recognition to track the location and movements of its employees is already being advertised. *See* FINDD, https://www.findd.io [https://perma.cc/8AZR-C2R5].

38. *See* WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 325 (2016) (describing the "life cycle of data" consisting of collection, processing and use, storage, and disclosures).

39. *Id.*

using the collected data, including a query of the data.[40] In the case of facial recognition tracking, data is collected when a camera captures and stores a person's image. It is used for facial recognition tracking when those points are aggregated and viewed by a human operator. That use can occur immediately following collection or at a later date.

Facial recognition tracking can reveal an individual's movements and thus a great deal of information about them.[41] For this reason, facial recognition tracking is a tremendously powerful surveillance tool, particularly in the hands of law enforcement. There are two key components necessary for facial recognition tracking to move from theory to reality: extensive networks of cameras and databases of faces. The next Section describes how each of these elements are rapidly developing, providing the tools necessary for facial recognition tracking to become widespread in the near future.

B. CAMERA-FILLED CITIES AND BILLION-PERSON DATABASES: AN AMERICAN DRAGNET

This Section describes the rapid growth of a facial recognition-powered surveillance apparatus in the United States. It begins by providing an overview of the cities and police departments that have been most active in deploying sophisticated networks of cameras. It then turns to the databases that are necessary for this system to be effective. This apparatus is already being used by law enforcement to identify suspects and investigate leads.[42] As it continues to grow and the scope of surveillance expands, the aggregation of location data will enable the creation of records of a person's physical movements.

1. Facial Recognition-Enabled Camera Networks Around the United States

A 2019 Georgetown Center on Privacy and Technology report describes a rapidly developing surveillance system in the United

40. *See* Rebecca Lipman, *Protecting Privacy with Fourth Amendment Use Restrictions*, 25 GEO. MASON L. REV. 412, 413 (2018).

41. *See* Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 626 (2016) ("[T]he insight provided by [location data] into individuals' lives is profound.").

42. *See* Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/JKR6-GQ6S]; Alex Hern, *What Is Facial Recognition – and How Do Police Use It?*, GUARDIAN (Jan. 24, 2020, 9:39 AM), https://www.theguardian.com/technology/2020/jan/24/what-is-facial-recognition-and-how-do-police-use-it [https://perma.cc/BBT5-EFLH] (discussing police capability to track and pinpoint individuals using facial recognition technology).

States.[43] The report focuses on the surveillance practices of Detroit and Chicago, noting that similar systems are developing in New York City, Orlando, and Washington, DC.[44] These systems as they exist today are comprised of extensive networks of cameras equipped with facial recognition[45] and massive databases powered by the public and private sectors.[46]

In 2017, the city of Detroit entered into a three-year contract to license a real-time video surveillance system equipped with facial recognition technology.[47] This system "provides continuous screening and monitoring of live video streams" throughout the city.[48] Detroit is able to implement an advanced face surveillance system in part because of Project Green Light, a partnership between the city and local businesses that began in 2016.[49] The program, which installed more than five hundred high-definition cameras throughout Detroit, was initially confined to businesses open late at night, but has expanded in recent years into other businesses as well as community centers.[50] Many of these cameras are now equipped with facial recognition

43. *See generally* Clare Garvie & Laura M. Moy, *America Under Watch*, GEO. L. CTR. ON PRIV. & TECH. (May 16, 2019), https://www.americaunderwatch.com [https://perma.cc/W79E-WVJ6] (describing the state of facial recognition surveillance in American cities).

44. *See id.*

45. Although facial recognition technology can be applied to an image captured by any camera, cameras equipped with facial recognition allow for real-time use. *See* Jon Schuppe, *Facial Recognition Gives Police a Powerful New Tracking Tool. It's Also Raising Alarms.*, NBC NEWS (July 30, 2018, 3:08 AM), https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936 [https://perma.cc/W4HT-LFB4] (describing the advancement of real-time facial recognition systems); Ava Kofman, *Real-Time Face Recognition Threatens To Turn Cops' Body Cameras into Surveillance Machines*, INTERCEPT (Mar. 22, 2017), https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn-cops-body-cameras-into-surveillance-machines [https://perma.cc/T2SH-XF3F] (same).

46. *See* Gregory Barber & Tom Simonite, *Some US Cities Are Moving into Real-Time Facial Surveillance*, WIRED (May 17, 2019, 7:00 AM), https://www.wired.com/story/some-us-cities-moving-real-time-facial-surveillance [https://perma.cc/T4DL-CST4].

47. Garvie & Moy, *supra* note 43 (citing CITY OF DETROIT, CONTRACT NO. 6000801, PROFESSIONAL SERVICES CONTRACT BETWEEN CITY OF DETROIT, MICHIGAN AND DATAWORKS PLUS (2017)).

48. *Id.*

49. *See* Juleyka Lantigua-Wlliams, *Using a Green Light To Bring Crime to a Stop*, ATLANTIC (May 19, 2016), https://www.theatlantic.com/politics/archive/2016/05/project-green-light/483300 [https://perma.cc/X8JU-MBSC] (describing Project Green Light initiative where business owners paid to have surveillance cameras that are monitored by police installed at their business).

50. *See id.*; Garvie & Moy, *supra* note 43.

capability.[51] That capability may soon be attached to police officers and drones as well—the Detroit Police Department's stated policy is that it "may connect the face recognition system to *any* interface that performs live video, including cameras, drone footage, and body-worn cameras."[52] Despite its implications for surveillance in the city, the adoption of facial recognition does not appear to have been subjected to any public discussion. The Detroit Police Department has downplayed its significance and the program is not mentioned on the Project Green Light webpage.[53]

Detroit is just one example; there are many more. Chicago, which is equipped with more than twenty thousand cameras, has also been at the forefront of implementing facial recognition technology into policing, first applying for a grant from the Department of Homeland Security in 2009.[54] Orlando pulled plans for a facial recognition system after it was the subject of widespread public backlash.[55] New York City has had a facial recognition system in place since 2011 and has plans to install facial recognition cameras at bridges and tunnels.[56] The city

51. Garvie & Moy, *supra* note 43.

52. *Id.* (quoting CRIME INTEL. UNIT, DETROIT POLICE DEP'T, STANDARD OPERATING PROCEDURE § 8: FACIAL RECOGNITION (2019)).

53. George Hunter, *Project Green Light To Add Facial Recognition Software*, DET. NEWS (Oct. 30, 2017, 11:52 AM), https://www.detroitnews.com/story/news/local/detroit-city/2017/10/30/detroit-police-facial-recognition-software/107166498 [https://perma.cc/W24J-NZJL] ("'This isn't some super-secret piece of technology,' [Assistant Police Chief James] White said."); *Project Green Light Detroit*, CITY DET., https://detroitmi.gov/departments/police-department/project-green-light-detroit [https://perma.cc/G7V5-XVLK] (omitting any mention of facial recognition).

54. Garvie & Moy, *supra* note 43. Since 2016, Chicago has had a contract in place with DataWorksPlus that allows it to monitor these cameras using real-time facial recognition. *See id.* In November 2016, the Chicago Police Department responded to an ACLU request by stating that it "does not use facial recognition technology in real-time situations." *Id.* (citing Letter from Charise Valente, Gen. Couns., Chi. Police Dep't, to Karen Sheley, Dir., Police Pracs. Project, Roger Baldwin Found. of ACLU, Inc. (Nov. 10, 2016) (on file with author)).

55. *See Facial Recognition Pilot Program*, CITY ORLANDO, https://www.orlando.gov/Initiatives/Facial-Recognition-Pilot-Program [https://perma.cc/U3AU-M4GQ] (announcing that Orlando ended its pilot facial recognition program); *see also* Davey Alba, *With No Laws To Guide It, Here's How Orlando Is Using Amazon's Facial Recognition Technology*, BUZZFEED NEWS (Oct. 30, 2018), https://www.buzzfeednews.com/article/daveyalba/amazon-facial-recognition-orlando-police-department [https://perma.cc/Z8C5-FW2Q] (describing Orlando's use of facial recognition technology).

56. *See* Joseph Goldstein & Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database*, N.Y. TIMES (Aug. 1, 2019), https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html [https://perma.cc/FXM6-RW2E] (noting that New York City has had some version of facial recognition in place since 2011). The state of New York has already attempted to use facial recognition to identify motorists, and though that program failed, the state

installed a vast network of cameras as part of its "Domain Awareness System," which gives police warrantless access to footage for up to thirty days.[57] In 2018 Washington, D.C., itself equipped with a vast network of cameras, began experimenting with facial recognition security systems at the White House and other federal buildings.[58] In 2015, the Baltimore Police Department used a facial recognition program called Geofeedia to identify protesters based on their social media profiles.[59] In May 2020, as protests unfolded in Minneapolis following the death of George Floyd, BuzzFeed News reported that the Minneapolis Police had contracted with Clearview to employ the use of facial recognition technology.[60] This list could continue on; a search for local governments employing facial recognition reveals that this is happening all over America, in small towns as well as large cities.[61]

In addition to these networks of fixed cameras, some police departments around the country are experimenting with the possibility of body-worn cameras equipped with facial recognition technology.[62]

has plans to try again. *See* Paul Berger, *MTA's Initial Foray into Facial Recognition at High Speed Is a Bust*, WALL ST. J. (Apr. 7, 2019, 9:00 AM), https://www.wsj.com/articles/mtas-initial-foray-into-facial-recognition-at-high-speed-is-a-bust-11554642000 [https://perma.cc/9EJB-MWZ2].

57. *See* Chris Francescani, *NYPD Expands Surveillance Net To Fight Crime as Well as Terrorism*, REUTERS (June 21, 2013), https://www.reuters.com/article/usa-ny-surveillance/nypd-expands-surveillance-net-to-fight-crime-as-well-as-terrorism-idINL2N0EV0D220130621 [https://perma.cc/FBZ6-Y54C].

58. *See* Jon Schuppe, *Secret Service Tests Facial Recognition Surveillance System Outside the White House*, NBC NEWS (Dec. 4, 2018, 11:43 AM), https://www.nbcnews.com/news/us-news/secret-service-tests-facial-recognition-surveillance-system-outside-white-house-n943536 [https://perma.cc/5ART-2U2T] (describing the White House's testing of facial recognition technology).

59. *See* Letter from ACLU to U.S. Dep't of Just. (Oct. 18, 2016) (asserting that an ACLU investigation found that Baltimore PD had used facial recognition to monitor protestors in the riots following Freddie Gray's death); *see also* GEOFEEDIA, BALTIMORE COUNTY POLICE DEPARTMENT AND GEOFEEDIA PARTNER TO PROTECT THE PUBLIC DURING FREDDIE GRAY RIOTS, https://congress.gov/116/meeting/house/109521/documents/HHRG-116-GO00-20190522-SD012.pdf [https://perma.cc/7GW5-8J5H] (promotional document advertising that its facial recognition services were used by Baltimore PD following Freddie Gray's death).

60. *See* Caroline Haskins & Ryan Mac, *Here Are the Minneapolis Police's Tools To Identify Protesters*, BUZZFEED NEWS (May 29, 2020), https://www.buzzfeednews.com/article/carolinehaskins1/george-floyd-protests-surveillance-technology [https://perma.cc/SY2X-ESMB].

61. For a dynamic, interactive map showing the use of facial recognition surveillance throughout the country, see BAN FACIAL RECOGNITION, https://www.banfacialrecognition.com/map [https://perma.cc/T77S-8VM7] (showing that law enforcement's use of facial recognition is widespread).

62. *See Police Body Worn Cameras: A Policy Scorecard*, UPTURN (Nov. 2017), https://www.bwcscorecard.org [https://perma.cc/69ES-WL2P] (listing police

A full consideration of the benefits and drawbacks of body-worn cameras as a policy matter is beyond the scope of this Note.[63] But the possibility of equipping these cameras with facial recognition technology adds a further dimension to the potential of the surveillance apparatus discussed here.[64]

This omnipresent network of cameras may seem chilling in its own right, but it is only a part of this story. The second part, discussed next, is the rise of massive databases that provide the identifying data necessary to turn a face into a name.

2. From Mugshots to Facebook: You're Probably in a Database

Once a facial recognition system has created a template and algorithmic representation of a person's face, it needs something to match that template to.[65] This is where databases enter the equation. There is no shortage of such databases in America.[66]

Each of the cities described above uses databases as part of the facial recognition process. In Detroit, the program is authorized to

departments that have adopted body cameras). In October 2019, California passed the Body Camera Accountability Act (AB 1215), banning the use of facial recognition technology in police-worn body cameras for three years. *See* Bryan Anderson, *New Law Bans California Cops from Using Facial Recognition Tech on Body Cameras*, SACRAMENTO BEE (Oct. 8, 2019), https://www.sacbee.com/news/politics-government/capitol-alert/article235940507.html [https://perma.cc/JYY4-BQFD]; *Breaking: California Senate Passes AB 1215, Blocking Face Recognition on Police Body Cameras*, MEDIAJUSTICE (Sept. 11, 2019), https://mediajustice.org/news/breaking-california-senate-passes-ab-1215-blocking-face-recognition-on-police-body-cameras [https://perma.cc/SH5N-KD36].

63. For a consideration of the privacy implications of police worn body cameras, see generally Kelly Freund, Note, *When Cameras Are Rolling: Privacy Implications of Body-Mounted Cameras on Police*, 49 COLUM. J.L. & SOC. PROBS. 91 (2015).

64. *See generally* Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933 (2016) (discussing the Fourth Amendment implications of police worn body cameras with a particular emphasis on their potential for creating a retrospective record); Katelyn Ringrose, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns*, 105 VA. L. REV. ONLINE 57 (2019).

65. *See* Hamann & Smith, *supra* note 9, at 10 (describing how such matches are made).

66. *See* Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org [https://perma.cc/8R36-HCV5] (describing the various types of databases used in conjunction with facial recognition); Cade Metz, *Facial Recognition Tech Is Growing Stronger, Thanks to Your Face*, N.Y. TIMES (July 13, 2019), https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html [https://perma.cc/LMG2-5LZB] (describing growth of databases).

search the city's database of 500,000 mug shot photos as well as Michigan's Statewide Network of Agency Photos, which includes driver's license photos.[67] Chicago uses its database of seven million mug shots.[68] In August 2019, the *New York Times* reported that the New York City Police Department had loaded "thousands of arrest photos of children and teenagers into a facial recognition database" and used those photos to make arrests years later.[69]

Through the FBI, the federal government maintains its own photograph database: the Next Generation Interface-Interstate Photo System (NGI-IPS).[70] The Interstate Photo System (IPS) is the portion of that database that contains photos searchable by facial recognition technology.[71] Local, state, tribal, and federal law enforcement agencies are all authorized to use the NGI-IPS.[72] Searchable photos include those submitted by both criminal and civil authorities—in 2015 criminal and non-criminal data were linked together as part of a "one-identity system."[73]

67. Garvie & Moy, *supra* note 43, at 1.A ("An Expensive, Expandable Face Surveillance System").

68. *Id.* at 2.

69. Goldstein & Watkins, *supra* note 56.

70. The NGI-IPS is one part of the broader Next Generation Identification system (NGI) that includes other types of biometric data, like iris scans and fingerprints, which may have been collected as part of an arrest or for non-criminal reasons (e.g., state licenses requirements). Each biometric identifier (photo) is linked to personal information. LYNCH, *supra* note 13, at 13. Since 2010, the FBI has been replacing the previous system, the Integrated Automated Fingerprint Identification System (IAFIS) with the NGI. U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-579T, FACE RECOGNITION TECHNOLOGY: DOJ AND FBI HAVE TAKEN SOME ACTIONS TO ENSURE PRIVACY AND ACCURACY, BUT ADDITIONAL WORK REMAINS 2 (2019). In 2017, the FBI issued a rule exempting the NGI system from the Privacy Act. Privacy Act of 1974; Implementation, 82 Fed. Reg. 35,651, 35,651 (Aug. 1, 2017) (codified at 28 C.F.R. pt. 16) (exempting NGI from the Privacy Act "to avoid interference with the Department[of Justice]'s law enforcement and national security functions and responsibilities of the FBI").

71. LYNCH, *supra* note 13, at 13.

72. *Id.* at 2. When using the NGI-IPS, a local, state, or federal agency submits a probe photo obtained during an investigation. The FBI then uses an automated facial recognition process to compare the probe photo against the NGI-IPS system. The system returns a gallery of two to fifty individuals whose photos are routed back to the requesting agency. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 70, at 3. Note that the NGI-IPS also allows text-based searching based on demographics including race. ERNEST J. BABCOCK, FBI, PRIVACY IMPACT ASSESSMENT FOR THE NEXT GENERATION IDENTIFICATION (NGI) INTERSTATE PHOTO SYSTEM 2 (2015).

73. *See* BABCOCK, *supra* note 72, at 3 (explaining the process by which civil photos may be connected to the Criminal Identity Group for searching); 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, 275 (2014–2015) ("The NGI expands the data by allowing more mug shot photos per profile, photo and biometric data from

Facial recognition databases are not limited to the formal, relatively regulated sphere of government agencies, however. In January 2020, the *New York Times* reported that Clearview, a private company, had built a database of more than three billion photos it obtained from scraping images posted on Facebook, Instagram, and other social media websites, in apparent violation of the terms of service of each of the host sites.[74] This is merely the latest iteration of an ongoing theme—facial recognition vendors have long sought to improve their algorithms by feeding them large collections of photos.[75] Facebook, which at one point claimed to possess the world's largest facial recognition dataset,[76] was recently sued by a class of persons in Illinois who claimed that its storage of their facial data violated the Illinois Biometric Information Privacy Act.[77] The size, scope, and sources of these databases suggests that if you own a driver's license, passport, or have posted your picture on the Internet, you're probably in a database, whether you like it (or even know it) or not.

This vast network of cameras and matching photo databases suggests that the United States is rapidly moving towards a society where merely appearing in public could mean being recorded, identified, and

civil submissions, facial features for use in FRT searches, and photos of scars and tattoos.").

74. Hill, *supra* note 5.

75. *See* Olivia Solon, *Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent*, NBC NEWS (Mar. 17, 2019, 10:25 AM), https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921 [https://perma.cc/9F3M-HQ2F] (describing the popular practice of facial recognition researchers and proprietors of using publicly available photos from various online sites to refine facial recognition algorithms).

76. *See* Natasha Singer, *Facebook's Push for Facial Recognition Prompts Privacy Alarms*, N.Y. TIMES (July 9, 2018), https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html [https://perma.cc/5RZM-UY8J] (noting the Facebook researchers' work was on "the largest facial dataset to-date" (quoting YANIV TAIGMAN, MING YANG & MARC'AURELIO RANZATO, DEEPFACE: CLOSING THE GAP TO HUMAN-LEVEL PERFORMANCE IN FACE VERIFICATION 1 (2014))).

77. 740 ILL. COMP. STAT. 14/1 (2019); Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019). The Ninth Circuit held that the class had standing to sue Facebook. *Id.* at 1272–73 ("In its recent Fourth Amendment jurisprudence, the Supreme Court has recognized that advances in technology can increase the potential for unreasonable intrusions into personal privacy. . . . [W]e conclude that an invasion of an individual's biometric privacy rights 'has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.'" (quoting Spokeo, Inc. v. Robins, 1363 S. Ct. 1540, 1549 (2016))). Following this ruling, Facebook settled with the class for $550 million. *See* Natasha Singer & Mike Isaac, *Facebook To Pay $550 Million To Settle Facial Recognition Suit*, N.Y. TIMES (Jan. 29, 2020), https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html [https://perma.cc/3YXL-TVGP].

tracked. This looming surveillance dragnet poses a significant threat to the Fourth Amendment right to be free from unreasonable government searches. With this in mind, the next Section provides an overview of how the modern Supreme Court has grappled with issues of government surveillance and technology.

C. FOURTH AMENDMENT JURISPRUDENCE, USE RESTRICTIONS, AND THE *CARPENTER* SHIFT

This Section describes how the Supreme Court's approach to searches under the Fourth Amendment has shifted in response to changing technology. The first portion describes the traditional reasonable expectation of privacy test and its subsequent application to various types of searches. Then, this Section discusses how the Court has applied new methods of scrutiny to the use of sophisticated technologies. This Section ends with a discussion of the culmination of these trends in the 2018 case *Carpenter v. United States*, where the Court recognized a Fourth Amendment right to an expectation of privacy in the whole of one's physical movements.[78]

1. The Reasonable Expectation of Privacy

The Supreme Court focuses its Fourth Amendment analysis first on the issue of whether a search or seizure has occurred.[79] If it determines that a search or seizure has not occurred, the Fourth Amendment does not apply and the analysis ends. Generally, the Court determines whether a search occurred through the use of the "reasonable expectation of privacy" test.[80]

The "reasonable expectation of privacy" analysis is rooted in the 1967 case *Katz v. United States*, where the FBI used a recording device to monitor Charles Katz's conversations held in a telephone booth.[81] Justice Harlan, writing in concurrence, set out a two-pronged analysis

78. 138 S. Ct. 2206 (2018).

79. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31 (2001) (describing the "antecedent question" of whether a search has occurred).

80. As established in the landmark case *Katz v. United States*, 389 U.S. 347 (1967).

81. *Id.* at 348. FBI agents suspected that Charles Katz was involved in an illegal gambling enterprise. *Id.* at 354. They knew that Katz regularly used a particular telephone booth, so they attached a recording device to the booth. *Id.* That device yielded conversations where Katz communicated wagers, and the agents used those recordings against Katz at trial, where he was convicted. *Id.* at 348. The Supreme Court then granted certiorari and reversed, finding that Katz's Fourth Amendment rights had been violated. *Id.* at 359.

to determine whether a search occurred.[82] The test outlines that "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."[83] The Court has fully adopted this reasoning into authoritative law.[84] Under this analysis, if the police violate a person's expectation of privacy that society is prepared to recognize as reasonable, then a search has occurred. The Court then turns to the question of whether that search was "reasonable," which generally means that it requires a warrant.[85]

Significantly, the *Katz* test has traditionally provided very little protection for activities that a person carries out in the public sphere. Indeed, in *Katz* itself, the Court noted that "[w]hat a person knowingly exposes to the public, even in his own home or office is not a subject of Fourth Amendment protection."[86] The Court has applied this reasoning broadly.[87]

As technology evolved to allow new types of investigative methods, however, the Court began to question some of its earlier

82. *Id.* at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

83. *Kyllo*, 533 U.S. at 31–33.

84. *See, e.g.*, *id.* at 33 (attributing this description to Justice Harlan's "oft-quoted concurrence").

85. *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) ("Although the 'ultimate measure of the constitutionality of a governmental search is "reasonableness,"' our cases establish that warrantless searches are typically unreasonable . . . ." (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652–53 (1995))); Kentucky v. King, 563 U.S. 452, 459–60 (2011) (discussing presumptive unreasonableness of warrantless searches and exceptions to the warrant requirement). There is a maze of exceptions and special cases where the warrant requirement does not apply. Though these are beyond the scope of this Note, the tendency of the Court to avoid labeling something a search as a way of avoiding the warrant requirement is discussed *infra* at note 336.

86. *Katz*, 389 U.S. at 351.

87. In *Cardwell v. Lewis*, the Court held that a car traveling on public roads had no expectation of privacy because it "travels public thoroughfares where both its occupants and its contents are in plain view." 417 U.S. 584, 590 (1974). The Court extended this reasoning in *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986), where it upheld the use of an aerial mapping camera on grounds that it was merely an enhancement of the naked eye. In *Florida v. Riley*, 488 U.S. 445 (1989), police flew a helicopter over the defendant's greenhouse and looked through missing roof panels to observe his marijuana grow operation. Echoing the reasoning in *Dow Chemical*, the Court held that there was no reasonable expectation of privacy because the "police may see what may be seen 'from a public vantage point where [they have] a right to be.'" *Id.* at 449 (quoting California v. Ciraolo, 476 U.S. 207, 213 (1986)).

assumptions. In *United States v. Knotts*, it held that the monitoring of a beeper placed in a container of chemicals leading police to the owner's rural cabin did not invade a legitimate expectation of privacy because the vehicle traveled over public roads.[88] The Court noted, however, that the possibility of "dragnet-type law enforcement practices" in the future may require a different constitutional analysis.[89] In *Dow Chemical v. United States*, the Court acknowledged that police surveillance with improved technology could represent an unreasonable search.[90] This language was a harbinger of things to come, as the Court would eventually be forced to confront highly sophisticated methods of surveillance that had moved from the realm of speculation to reality.

2. "Digital Is Different"—the Supreme Court Seeks To Modernize the Fourth Amendment

As new technologies have expanded government surveillance power, both scholars and courts have grappled with questions of whether and how traditional Fourth Amendment jurisprudence should change. In recent years, as the Supreme Court has been confronted with digital technologies that have expanded police surveillance capabilities, it has responded by expanding the means through which a Fourth Amendment search can occur.

The Supreme Court has indicated its goal of "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[91] The struggle to maintain this balance has been described as the "equilibrium-adjustment theory" of the Fourth Amendment.[92] As advances in surveillance technology have provided

88. 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

89. *Id.* at 284 ("[I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.").

90. *Dow Chemical*, 476 U.S. at 238 ("It may well be, as the Government concedes, that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant.").

91. United States v. Jones, 565 U.S. 400, 406 (2012) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

92. *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011). This understanding of the Fourth Amendment recognizes that the role of the Court is to adjust Fourth Amendment standards as technology changes in order to maintain a relatively constant balance between the individual and the state. As the technology underpinning or inhibiting surveillance develops, judges must strike a balance. On the one hand, they fear that the unchecked

law enforcement with novel ways of gathering information about members of the public, the application of traditional Fourth Amendment doctrine to those practices has resulted in significant gaps in constitutional protection.[93]

The concept of use restrictions was introduced in 1995 by Professor Harold Krent as an attempt to bridge one such gap between historical Fourth Amendment analyses and the constitutional issues posed by modern technology.[94] Use restrictions apply Fourth Amendment scrutiny to the way that data is used, even after it has been legally collected. Professor Krent argued that Fourth Amendment doctrine did not properly consider the reasonableness of how the government used information after it had been lawfully seized, even though such use implicated interests protected by the Fourth Amendment.[95] At the time, Professor Krent noted that his argument was out of touch with current doctrine, instead grounding his points in theoretical and historical bases.[96] But today, Professor Krent's ideas look prescient, as a series of recent cases suggests that the Court is determined to adjust its Fourth Amendment doctrine to remain relevant in the digital age.

The Court began to signal potential changes in its Fourth Amendment analysis for digital search methods in *United States v. Jones*,[97] where it held that the use of a Global Positioning System (GPS) to track a vehicle through public streets was a search within the meaning of the Fourth Amendment.[98] Justice Scalia, writing for the majority, sidestepped the underlying surveillance issues in the case by deciding for

expansion of government power will lead to a dystopian state. But they also fear that too much limitation on government power will lead to anarchy. Equilibrium-adjustment is a "judicial instinct" to balance the competing concerns. *Id.* at 488.

93. *See* Donohue, *supra* note 41, at 612 ("Fourth Amendment doctrine has long struggled with how to integrate new technologies into the private/public distinction. Perhaps nowhere are its failings clearer than in the realm of location tracking."). For a broader description of the various technologies that have led to this erosion, see generally *id.* at 581–631.

94. *See* Krent, *supra* note 8, at 51 ("My thesis is that the reasonableness of a seizure extends to the uses that law enforcement authorities make of property and information even after a lawful seizure.").

95. *Id.*

96. *See id.* at 51 n.14 (noting that the article does not directly address the Court's then current definition of seizure).

97. 565 U.S. 400 (2012); *see also* Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 1 (2012) (describing *Jones* as a "giant step into the modern age").

98. *Jones*, 565 U.S. at 404.

Jones under a property-rights theory of the Fourth Amendment, noting that the *Katz* "reasonable expectations" test did not encompass the entirety of Fourth Amendment analysis.[99] The majority emphasized the importance of "assur[ing] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[100] Despite taking a property-based approach in deciding the facts of the case, the Court signaled its awareness of the constitutional problems posed by modern surveillance methods by noting: "It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[101]

Jones is a landmark Fourth Amendment case, however, because of its two concurrences by Justices Sotomayor and Alito, which attempted to answer precisely such a question.[102] These concurrences, joined by a total of five members of the Court, established that a "shadow majority" of the Court was concerned by growing surveillance capabilities and the inability of its traditional Fourth Amendment jurisprudence to address them.[103]

Justice Sotomayor rejected Justice Scalia's narrow focus on property rights.[104] She noted that the GPS monitoring used in the case "generates 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."[105] The government can continue to access this data, "alter[ing] the relationship between citizen and government in a way that is inimical to democratic society."[106] Justice Sotomayor argued that these surveillance capabilities should be accounted for in the reasonable expectation test and analysis, and that the proper question is "whether people reasonably expect that their movements will be recorded and aggregated in a manner

99. *Id.* at 406 ("But we need not address the Government's contentions, because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation.").

100. *Id.* (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

101. *Id.* at 412.

102. *Id.* at 413 (Sotomayor, J., concurring); *id.* at 418 (Alito, J., concurring in the judgment).

103. *See, e.g.*, Laura Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 506–08 (2012) (describing the five Justices joining the Alito and Sotomayor concurrences as the "shadow majority").

104. *Jones*, 565 U.S. at 414 (Sotomayor, J., concurring).

105. *Id.* at 415 (citing People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

106. *Id.* at 416 (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[107] The concerns described in Justice Sotomayor's concurrence comprise one of the pillars of *Carpenter*, where the Court recognized that an individual has a reasonable expectation of privacy in the whole of their physical movements.[108]

Justice Alito wrote a separate concurrence where he highlighted problems with the majority's property-based analysis, calling it "highly artificial."[109] He also noted that the reasonable expectation of privacy test is imperfect and that technology can change society's expectations.[110] Justice Alito agreed that the "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted" was the proper goal, but rejected the majority's theory that "any technical trespass that led to the gathering of evidence" constituted a search.[111] This too foreshadowed an important part of the *Carpenter* analysis.[112] Justice Alito concluded with a discussion of the unique privacy problems presented by cell phones, a preview of problems the Court would confront directly just two years later.[113]

In 2014, the shadow majority was joined by the rest of the court in the unanimous decision *Riley v. California*.[114] In *Riley*, the Court held that a warrant was required for police to search information on the cell phone of an individual who had been arrested.[115] Applying a

107. *Id.*

108. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018). Some commentators have argued that Justice Sotomayor's reasoning in *Jones* was an application of the "mosaic theory" of the Fourth Amendment. *See, e.g.*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (describing and criticizing the mosaic theory).

109. *Jones*, 565 U.S. at 419 (Alito, J., concurring in the judgment).

110. *Id.* at 427 ("But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.").

111. *Id.* at 420.

112. *Carpenter*, 138 S. Ct. at 2217 ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment))).

113. *Jones*, 565 U.S. at 428–29 (Alito, J., concurring in the judgment).

114. 573 U.S. 373 (2014).

115. *Id.* at 386. The Court noted that searches in the criminal context generally required a warrant, and in the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement. *Id.* at 382. At issue in *Riley* was whether one such exception, searches "incident to arrest," should include searches of cell phones. *Id.* at 385.

reasonableness balancing test, the Court dismissed arguments that such searches were necessary to protect officer safety or the destruction of evidence when compared with their intrusiveness into a person's privacy interests.[116]

Chief Justice Roberts, who authored *Riley*, wholeheartedly embraced the notion that digital is different.[117] He famously dismissed the government's efforts to analogize a comprehensive search of a cell phone's contacts to other permissible searches as "like saying a ride on horseback is materially indistinguishable from a flight to the moon."[118] Chief Justice Roberts emphasized that cell phones deserved unique protection because they contained the "privacies of life."[119] This meant that they were subject to special protection because the point of the Fourth Amendment was to protect certain kinds of information from government access.[120] *Riley* confirmed what *Jones* suggested—the Court was determined to breathe new life into its Fourth Amendment jurisprudence to ensure its relevance in the digital age. But the exact contours of the new doctrine were uncertain. The next Subsection discusses the 2018 case *Carpenter v. United States*, where some, but not all, of those questions were answered.

3. A New Approach—the *Carpenter* Shift

In 2018, the Court decided the landmark case *Carpenter v. United States*.[121] In that case, the Court held that the government conducts a Fourth Amendment search when it "accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements."[122] *Carpenter* has spawned a wealth of scholarship and debate. Professor Orin Kerr calls the decision "a blockbuster for the Digital Fourth Amendment" that shows the Court is "on a new path."[123] Professor Paul Ohm writes that "*Carpenter* works a series of revolutions in Fourth Amendment law, which are likely to guide the evolution of

116. *Id.* at 386–98.

117. *See* Henderson, *supra* note 64, at 951 ("So, while *Riley* perhaps left things unanswered that it could have addressed, it made very clear that when it comes to the Fourth Amendment, digital is different.").

118. *Riley*, 573 U.S. at 393.

119. *Id.* at 410 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

120. *Id.* ("The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.").

121. 138 S. Ct. 2206 (2018).

122. *Id.* at 2211.

123. Orin S. Kerr, *The* Carpenter *Shift*, *in* THE DIGITAL FOURTH AMENDMENT (forthcoming) (manuscript at 1), https://ssrn.com/abstract=3301257.

constitutional privacy in this country for a generation or more."[124] To be sure, *Carpenter* left many questions unanswered.[125] But it signaled that the Court has embraced new modes of analysis to ensure that the Fourth Amendment remains relevant in the digital age.[126]

In *Carpenter*, cell-site location information (CSLI) was used to place Timothy Carpenter at the scene of a series of robberies of electronics stores in Detroit.[127] Based on tips from an accomplice, the prosecutors in the case applied for two court orders under the Stored Communications Act[128] to obtain CSLI from Carpenter's phone over a four-month period in 2011, when the robberies occurred.[129] Federal magistrate judges granted these requests and ordered Carpenter's cell phone carriers to turn over his records, which they did.[130] As a result of these records, the government obtained 12,898 location points cataloging Carpenter's movements.[131]

Carpenter moved to suppress the records on Fourth Amendment grounds because they had been obtained without a warrant supported by probable cause.[132] The district court denied the motion.[133] At trial, the CSLI obtained from the records was used to place Carpenter at the scene of the crimes.[134] Carpenter was convicted on nearly all counts and sentenced to over one hundred years in prison.[135] The Sixth Circuit affirmed, and the Supreme Court granted certiorari.[136]

124. Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 358 (2019).

125. As the Court itself noted, "we 'do not begin to claim all the answers today.'" *Carpenter*, 138 S. Ct. at 2220 n.4 (quoting *id.* at 2268 (Gorsuch, J., dissenting)).

126. *Id.* at 2219 ("The Government's position fails to contend with the *seismic shifts in digital technology* that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years." (emphasis added)).

127. *Id.* at 2212–13.

128. 18 U.S.C. §§ 2701–2713. 18 U.S.C. § 2703 designates procedures law enforcement must follow to obtain user data from a third party.

129. *Carpenter*, 138 S. Ct. at 2212. Cell-site location information is produced when cell phones continuously connect to nearby cell towers. *Id.* at 2211. The data is collected by cell phone providers for their own use. *Id.* at 2212.

130. *Id.*

131. *Id.*

132. *Id.*

133. *Id.*

134. *Id.* at 2213.

135. *Id.*

136. *Id.*

The Supreme Court reversed.[137] The majority began by noting that the "basic purpose of [the Fourth Amendment] is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials" and "property rights are not the sole measure of Fourth Amendment violations."[138] It described two basic guideposts for the Fourth Amendment: "First, that the Amendment seeks to secure 'the privacies of life' against 'arbitrary power.' Second, and relatedly, that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'"[139] The majority noted the importance of these considerations in applying the Fourth Amendment to innovative surveillance methods and referenced *Kyllo v. United States* and *Riley v. California* as examples of taking this approach.[140]

The majority noted that *Carpenter* sat at the intersection of two lines of cases and began with the first: "a person's expectation of privacy in his physical location and movements."[141] It described the holdings of *Knotts* and *Jones* and how they differed based on the scope of surveillance at issue.[142] The majority then described the second issue: it has typically distinguished "between what a person keeps to himself and what he shares with others."[143]

137. *Id.* at 2223.

138. *Id.* at 2213 (first quoting Camara v. Mun. Ct., 387 U.S. 523, 528 (1967); and then quoting Soldal v. Cook Cnty., 506 U.S. 56, 64 (1992)).

139. *Id.* at 2214 (first quoting Boyd v. United States, 116 U.S. 616, 630 (1886); and then quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

140. *Id.* In *Kyllo*, the Court held that the use of a thermal imaging device to detect heat radiating from a person's home was a search. 533 U.S. 27, 34–35 (2001). One could argue that this case also was a part of the broader "digital is different" shift described in Part I.C.2, but its focus on the home as a unique source of Fourth Amendment protection adds a degree of complexity that is unhelpful to the broader discussion here.

141. *Carpenter*, 138 S. Ct. at 2215.

142. *Id.* (comparing "rudimentary tracking" in *United States v. Knotts*, 460 U.S. 276 (1983), with "more sophisticated surveillance").

143. *Id.* at 2216. This is the third-party doctrine. *See id.* ("We have previously held that 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.' That remains true 'even if the information is revealed on the assumption that it will be used only for a limited purpose.'" (first quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979); and then quoting United States v. Miller, 425 U.S. 435, 443 (1976))). The third-party doctrine has been widely criticized as unjustly limiting Fourth Amendment protection. *See, e.g.*, DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 102–10 (2011) (arguing that defense of the third-party doctrine boils down to arguing that there should be no Fourth Amendment protection for "digital dossiers"); Ohm, *supra* note 124, at 362 nn.32–33 (citing criticisms of third-party doctrine).

The Court noted that the challenge in front of it was "how to apply the Fourth Amendment to a new phenomenon."[144] It declined to extend the third-party doctrine to cover CSLI, including direct government surveillance alongside third-party surveillance in the prohibition.[145] The Court then held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[146] This expansion of the expectation of privacy to the whole of one's movements shows a willingness of the Court to adjust its traditional doctrine when applying the Fourth Amendment to modern surveillance methods.

Carpenter signals a subtle but important shift in the theory underlying the *Katz* test. *Carpenter* leaves *Katz* intact—the reasonable expectation of privacy concept remains a guiding principle in determining whether a search has occurred for Fourth Amendment purposes.[147] But *Carpenter* expands the realm of what a person can reasonably expect to be private to include certain kinds of information. Indeed, *Carpenter* suggests that the relevant question in determining whether a Fourth Amendment search occurred can be whether the nature of the information at issue is itself protected from unwarranted government scrutiny under the Fourth Amendment.[148] Whereas previously the test was about how the police interacted with physical places and things (also known as "means analysis"),[149] *Carpenter* asks whether a technology or police practice is potentially so revealing that

144. *Carpenter*, 138 S. Ct. at 2216.

145. *Id.* at 2217. This limitation of the third-party doctrine is significant in its own right. Like *Carpenter* more broadly, its full implications remain to be seen. *See* Harvey Gee, *Last Call for the Third-Party Doctrine in the Digital Age After* Carpenter*?*, 26 B.U. J. SCI. & TECH. L. 286, 288–89 (2020) (arguing that *Carpenter* should be understood as a rebuke of the third-party doctrine).

146. *Carpenter*, 138 S. Ct. at 2217.

147. *See id.* at 2214 n.1 ("Neither party has asked the Court to reconsider *Katz* in this case.").

148. *Carpenter* embraces the "informational security" theory of the Fourth Amendment. *See* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 604 (2017) (defining "informational security" as "personal information that is secured in some manner from governmental intrusion"). Ferguson notes that the theory of informational security is built on a broad array of scholarship from constitutional and privacy scholars. *See id.* at 605 nn.304–05 (describing informational security literature).

149. *See* Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1343 (2002) ("[T]he Court's approach focuses on the means employed by government, and has been described by Melvin Gutterman as the 'means model' or what I choose to call 'means analysis.'").

it violates a reasonable expectation in what the police can do.[150] Rather than asking whether a government action violates a reasonable expectation of privacy in a person's tangible *things*, *Carpenter* asks "whether a prior limit on government power has been lifted."[151] For practical purposes, the problem in *Carpenter* was not how the police obtained the CSLI records, but rather the nature of the records themselves.

The Court described three factors that should be considered to determine whether a search has occurred based on the nature of the data to be searched: (1) its "depth, breadth, and comprehensive reach"; (2) "the inescapable and automatic nature of its collection"; and (3) its "deeply revealing nature."[152]

The first factor "refers to the detail and precision of the information stored," as well as its size and scope.[153] Professor Kerr suggests that this factor implies that "records must be of a kind and nature that generally could not be collected in a pre-digital age."[154] This factor continues the trend of recognition from the Roberts Court that digital technologies are sufficiently different than their predecessors to warrant a new approach.[155]

150. *See Carpenter*, 138 S. Ct. at 2218–19 (discussing how revealing CSLI data can be and holding that by accessing Carpenter's CSLI, the government invaded Carpenter's reasonable expectation of privacy as to the entirety of his movements); Kerr, *supra* note 123, at 6 ("*Carpenter* signals a new kind of expectation of privacy test, one that focuses on how much the government can learn about a person regardless of the place or thing from which the information came.").

151. Kerr, *supra* note 123, at 8.

152. *Carpenter*, 138 S. Ct. at 2223; *see* Ohm, *supra* note 124, at 370. The discussion here is based on Professor Ohm's distillation of the factors but, as he notes, there is likely to be some disagreement among scholars about how exactly these factors should be defined. *Id.*; *see, e.g.*, Kerr, *supra* note 123, at 16–26 (asserting that the *Carpenter* factors are records created digitally, without meaningful voluntary choice, that reveal "the privacies of life"). But note that these differences are relatively minor and do not meaningfully change the assertions in this Note.

153. Ohm, *supra* note 124, at 372–76. Ohm defines depth as "the detail and precision of the information stored." *Id.* at 372 (citing *Carpenter*, 138 S. Ct. at 2218). He defines breadth as referring to time, both in terms of collection frequency and storage time. *Id.* Finally, he considers comprehensive reach as "the number of people tracked in the database." *Id.* at 373.

154. Kerr, *supra* note 123, at 16.

155. Ohm, *supra* note 124, at 399 (describing the majority's "deep and abiding belief in the exceptional nature of the modern technological era"). Professor Ohm notes Chief Justice Roberts's emphasis on the sheer power, scale, and speed of modern technological changes. *Id.* at 401–03.

The second factor "considers the extent to which the data subject assumed the risk of revealing the information at issue."[156] The *Carpenter* majority quoted *Riley*, noting that cell phones are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[157] At its core, this factor asks whether the records were "created without the subject's meaningful voluntary choice."[158]

The third factor, which considers the "deeply revealing nature" of a given set of information, suggests that some information deserves inherent protection.[159] This factor is an explicit extension of principles described in *Jones* and *Riley*, that the "privacies of life" deserve special protection from government access.[160] This factor is the most revolutionary of the three because it considers the nature of the information at issue rather than how it was obtained.[161]

Carpenter is also noteworthy because it specifically addressed some of the Fourth Amendment problems that arise with the use of sophisticated surveillance methods.[162] The Court acknowledged that "[a] majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements."[163] In other words, there is an important distinction between observing a person once versus chronicling their movements over time.[164] This has implications for surveillance by any method but is particularly salient for comprehensive surveillance technologies like facial recognition tracking.

The Court also noted that "[a] person does not surrender all Fourth Amendment protection by venturing into the public

156. *Id.* at 376–78.

157. *Carpenter*, 138 S. Ct. at 2220 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

158. Kerr, *supra* note 123, at 20.

159. Ohm, *supra* note 124, at 371–72.

160. *Riley*, 573 U.S. at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)); *see* United States v. Jones, 565 U.S. 400, 414–15 (2012) (Sotomayor, J., concurring).

161. Ohm, *supra* note 124, at 372 ("[T]his factor focuses exclusively on an analysis of the intrinsic nature of the information itself, divorced from any consideration of what the police had to do to obtain it, the company's incentives for gathering it, or what the individual could have done to prevent it."). Note that the exact contours of this factor remain unsettled, although this Note argues that location data should be considered per se deeply revealing. *See infra* Part III.

162. *Carpenter*, 138 S. Ct. at 2216–19.

163. *Id.* at 2217 (first citing *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment); and then citing *id.* at 415 (Sotomayor, J., concurring)).

164. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

sphere."[165] This statement casts serious doubt on the doctrine that there is per se no reasonable expectation of privacy in public spaces. At the very least, it affirms that law enforcement's access to a piece of data is not shielded from Fourth Amendment scrutiny solely because it was collected in a public space.

It is true that in *Carpenter* the records at issue were possessed by a third party, and the case was significant for its implications for the third-party doctrine.[166] But the Court noted that its reasoning applied to direct government surveillance as well.[167]

In sum, during the last decade the Supreme Court has repeatedly shown its willingness to apply practical standards to its Fourth Amendment analysis to ensure that the capabilities of modern technologies do not eliminate Fourth Amendment protections. This Note argues that to protect the Fourth Amendment principles recognized in *Carpenter*, courts should analyze the use of facial recognition technology to track an individual's movements as a search under the Fourth Amendment.

II. COMPREHENSIVE FACIAL TRACKING FUNDAMENTALLY ALTERS THE RELATIONSHIP BETWEEN CITIZEN AND STATE

This Part shows why facial recognition tracking is a threat to liberty and the Fourth Amendment. It begins by discussing the effects of state surveillance on people and society and argue that the Fourth Amendment is meant to protect individual liberty as well as privacy. Then, this Part argues that modern constitutional oversight must consider the use of data as well as its collection in determining whether a Fourth Amendment search occurred. It argues that facial recognition tracking implicates the Fourth Amendment even if facial identification does not. This Part concludes by arguing that law enforcement's unbridled use of facial recognition tracking threatens the Fourth

165. *Carpenter*, 138 S. Ct. at 2217.

166. *Id.* at 2220 ("We therefore decline to extend *Smith* and *Miller* to the collection of CSLI. Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection.").

167. *Id.* at 2217 ("Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, [this rule applies]."); *see also* Ohm, *supra* note 124, at 392 ("*Carpenter*'s reasoning should apply even when third parties are not involved. Its multi-factor test focuses most of its attention on the quality of the database alone, so it should apply even to databases compiled directly by the government.").

Amendment right to be free from "a too permeating police surveillance" and demands a constitutional response.[168]

A. THE EFFECTS OF POLICE SURVEILLANCE AND A CONSIDERATION OF FOURTH AMENDMENT PURPOSE

In an effort to illustrate the potential ramifications of comprehensive police surveillance via facial recognition tracking, this Section shows why surveillance is harmful and why considerations of liberty, not just privacy, should be central to Fourth Amendment analysis.

1. Somebody's Watching Me—the Harms of Surveillance

"Surveillance" is a broad term used to describe the general phenomenon of being watched.[169] People generally do not like being watched, and there is evidence that surveillance can affect behavior.[170] Similarly, surveillance can be understood as limiting a person's choices and thus their freedom.[171] Scholars such as Alan Westin have described these effects as destroying the comfort that public spaces can provide.[172] Even the mere possibility of surveillance can affect people. In his theory of the "panopticon," the philosopher Jeremy Bentham argued that the knowledge that one *might* be under surveillance can have the same effects as certainty that one is under surveillance.[173] Surveillance can also lead to effects on behavior, including

168. United States v. Di Re, 332 U.S. 581, 595 (1948).

169. Privacy scholar Professor Daniel Solove defines surveillance as "the watching, listening to, or recording of an individual's activities." DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 104 (2009). Philosopher Helen Nissenbaum prefers the phrase "monitoring and tracking" because she argues that surveillance implies a "set of political assumptions." *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT 22 (2010). This Note focuses on the concept of surveillance of people, a phenomenon that is related to but distinct from *dataveillance*, a term that describes the surveillance of information. *See id.* at 23. Dataveillance is the subject of a broad scholarship and is beyond the scope of this Note. *See, e.g.*, *id.* at 23–25.

170. *See* SHOSHANA ZUBOFF, IN THE AGE OF THE SMART MACHINE: THE FUTURE OF WORK AND POWER 344–45 (1988) (describing "anticipatory conformity," the phenomenon of people adjusting their behavior to preemptively conform to authority).

171. SOLOVE, *supra* note 169, at 30. This is philosopher Stanley Benn's personhood theory of privacy. *Id.* Solove describes how the theory has been adopted by the U.S. Supreme Court in its right to privacy decisions including *Griswold v. Connecticut*, 381 U.S. 479 (1965), *Eisenstadt v. Baird*, 405 U.S. 438 (1972), and *Roe v. Wade*, 410 U.S. 113 (1973). *Id.*

172. ALAN F. WESTIN, PRIVACY AND FREEDOM 31 (1967) ("Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas.").

173. JEREMY BENTHAM, PANOPTICON; OR, THE INSPECTION-HOUSE 23 (1791). The panopticon is a prison made up of a ring of cells with a guard tower at its center. *Id.* at 5–

self-censorship, conformity, and inhibition.[174] Taken together, these effects make surveillance a powerful tool for social control.[175]

Police surveillance can also be used in other undesirable ways. For example, in Britain, surveillance has been used "to enforce social conformity."[176] An investigative report of Britain's surveillance system describes the use of a system of CCTVs to police loitering and public drunkenness rather than focusing solely on the types of violent crimes one might envision when thinking about the potential benefits of police surveillance.[177] In other words, surveillance results in the policing of public spaces to keep out unwanted characters—something far different than protection from violent crimes.[178] This resembles Foucault's anticipation of modern society as a kind of "super panopticon" where constant surveillance acts to ensure conformity.[179]

Surveillance does not necessarily have to come from the state, but its effects are more significant when it does. Surveillance by the state

6. The guard can see into the cells, but the prisoners cannot see into the tower. *Id.* The prisoners know they may be under surveillance at any given moment, but they do not know when. *See id.* at 23; *see also* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 240 (2002). Although the panopticon is generally described by its physical terms, it is interesting to note that Bentham intended the panopticon as a broader political project with a focus on the dynamics between members of a society. *See* Greg Elmer, *Panopticon—Discipline—Control*, *in* ROUTLEDGE HANDBOOK OF SURVEILLANCE STUDIES 22 (Kirstie Ball, Kevin D. Haggerty & David Lyon eds., 2012). Michel Foucault expounded on Bentham's idea when he noted, "He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power . . . he becomes the principle of his own subjection." MICHEL FOUCAULT, DISCIPLINE AND PUNISH 195–229 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977).

174. *See* Terence C. Burnham & Brian Hare, *Engineering Human Cooperation*, 18 HUM. NATURE 88, 99 (2007) (finding people altered their behavior when aware of an image of a robot with human eyes); *see also* SOLOVE, *supra* note 169, at 108 (suggesting that too much surveillance can adversely dampen human behavior); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013) ("Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas.").

175. SOLOVE, *supra* note 169, at 108.

176. Slobogin, *supra* note 173, at 248 (quoting Jeffrey Rosen, *A Watchful State*, N.Y. TIMES MAG. (Oct. 7, 2001), https://www.nytimes.com/2001/10/28/magazine/l-a-watchful-state-797944.html [https://perma.cc/V4GM-69Y4]).

177. Jeffrey Rosen, *A Watchful State*, N.Y. TIMES MAG. (Oct. 7, 2001), https://www.nytimes.com/2001/10/28/magazine/l-a-watchful-state-797944.html [https://perma.cc/V4GM-69Y4]. "CCTVs" are closed-circuit televisions, a form of video surveillance. *See id.*

178. *See* Slobogin, *supra* note 173, at 248–49.

179. FOUCAULT, *supra* note 173; *see also* ZUBOFF, *supra* note 170, at 344–45 (suggesting that anticipatory conformity occurs when people accept that they are being watched and adapt to it).

is distinct from surveillance by some other entity, like a nosy neighbor, for two main reasons. Most significantly, the state has the ability to punish.[180] Because people want to avoid punishment, they are more careful in their interactions with the state than they otherwise might be.[181] As state surveillance capabilities increase, this unnaturally inhibited behavior comes to dominate more of one's life.

Similarly but more subtly, the effects of surveillance are amplified when a person believes not only that she is under observation, but that her actions are susceptible to use by a bureaucracy.[182] In other words, people become more inhibited in their behaviors because they are unsure of the range of potential consequences for those behaviors in the hands of an institution as powerful and bureaucratic as the government. Technology scholar Bruce Schneier echoes these concerns in his argument that "[u]biquitious surveillance means that anyone could be convicted of lawbreaking, once the police set their minds to it."[183] The idea of "perfect" enforcement of the law may sound superficially attractive, but it becomes less so as one considers its full implications.[184]

Governments have long sought to track and monitor the citizenry—both the concept of authority figures watching others and the feeling that it is wrong have ancient roots.[185] But the rise of modern

180. Bentham argued that surveillance was particularly pernicious when conducted by an authority with the ability to punish. *See* BENTHAM, *supra* note 173, at 29–30; *see also* Slobogin, *supra* note 173, at 247.

181. *See* Elmer, *supra* note 173, at 25 (describing mechanics of "disciplinary society," including coercion through surveillance).

182. *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1154 (2002) (describing a problem that occurs when people know information that is collected about them may be used in various, unknown ways by authorities); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1189 (2002) (describing the threat posed by "inadvertence, carelessness, and mindlessness of bureaucracy") [hereinafter Solove, *Access and Aggregation*]; *see also* Richards, *supra* note 174 (describing the chilling of civil liberties and an increase in the power of the state as two distinct effects of state surveillance).

183. BRUCE SCHNEIER, DATA AND GOLIATH 92 (2015). *See generally* EMILY BAXTER, WE ARE ALL CRIMINALS (2017) (arguing that virtually everyone has committed crimes over the course of their lives).

184. Professor Woodrow Hartzog calls this the "suffocating restraint of the relentless, perfect enforcement of the law." Woodrow Hartzog, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 [https://perma.cc/4TP6-5RGH].

185. *See* NELSON, *supra* note 10, at 28 ("For as long as there have been systems of identification, there have also been persistent concerns regarding the consequences to those individuals who are identified."). Edward Higgs argues that the dynamics of mass surveillance long predate industrial society, citing early English records such as the

industrial societies and systems of government have changed the dynamics of surveillance practices.[186] As smaller units of social organization have been replaced by massive governments and more efficient, industrialized systems, concerns about surveillance that were once confined to person-to-person practices like "Peeping Toms" gave way to the dystopian visions of Orwell's *1984* and Huxley's *Brave New World*.[187] This change was driven by the development of ever more efficient surveillance systems.[188] The development of panvasive surveillance technologies like facial recognition tracking is a continuation of this trend.[189] But while the steady erosion of individual liberty due to surveillance technology may seem inevitable, it is not. The relationship between citizen and state is a legal, rather than technological, issue and is addressed directly in the Bill of Rights.

2. The Fourth Amendment Is a Limitation on Government Power

The founders of the United States were weary of an overly powerful government and embraced the concept of limited government to protect individual liberty.[190] This Subsection argues that the Fourth Amendment should be understood not just as a protection of privacy but as a protection of liberty alongside the rest of the Bill of Rights. This context suggests that courts should be particularly sensitive to surveillance systems that threaten individual liberty, like facial recognition tracking.

The Fourth Amendment, like the rest of the Bill of Rights, is a limitation on government power in order to protect individual

Domesday Book of 1086 as attempts to organize and monitor the population. EDWARD HIGGS, THE INFORMATION STATE IN ENGLAND 2–3 (2004). For a more contemporary overview, see SCHNEIER, *supra* note 183, at 62–77.

186. David Lyon, Kevin D. Haggerty & Kirstie Ball, *Introducing Surveillance Studies*, *in* ROUTLEDGE HANDBOOK OF SURVEILLANCE STUDIES, *supra* note 173, at 1; *see also* Toni Weller, *The Information State*, *in* ROUTLEDGE HANDBOOK OF SURVEILLANCE STUDIES, *supra* note 173, at 58.

187. See SOLOVE, *supra* note 169, at 107, for a discussion of "Peeping Toms," which originated from a folktale dating back to 1050. For two twentieth-century narratives of what a future totalitarian surveillance society could look like, see GEORGE ORWELL, 1984 (1949), and ALDOUS HUXLEY, BRAVE NEW WORLD (1932).

188. *See* Weller, *supra* note 186.

189. "Panvasive surveillance" is a term coined by Professor Christopher Slobogin to define surveillance technologies that are "pervasive, and are often invasive, [but] their defining characteristic is their *pan*vasiveness—the fact that they affect so many people, most of them innocent of any wrongdoing." *See* Christopher Slobogin, *Rehnquist and Panvasive Searches*, 82 MISS. L.J. 307, 308 (2013).

190. Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1265–66 (2016).

liberties.[191] In other words, the Fourth Amendment should be understood as pertaining to power, and scholars have argued that the Court's focus on privacy has diluted that purpose.[192] There is support for this assertion in the history of the Fourth Amendment: it was written as a response to general warrants during the colonial period, which permitted their holder full discretion to search a person's home and effects.[193] The Founders implemented the Amendment so that there would be some check on government power to arbitrarily search the citizenry.[194]

The Fourth Amendment should thus be understood as a protection of the people's authority to determine how much the government can learn about them.[195] The focus on privacy in Fourth Amendment jurisprudence has diluted this purpose because it fails to distinguish between the government and private actors.[196] Given the purpose of the Fourth Amendment, the permissiveness of state surveillance as a constitutional matter should be understood as a distinct issue from the privacy one may or may not enjoy from other members of the

191. Slobogin, *supra* note 97, at 11 ("The entire Bill of Rights, from the First Amendment's guarantees of speech and association through the Eighth Amendment's prohibition on cruel and unusual punishment, is meant to protect liberty and dignity against governmental abuse of power.").

192. *See, e.g.*, Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303, 303–04 (2010) (arguing that the Fourth Amendment "seeks to protect the political liberties of the sovereign 'People'"); Ku, *supra* note 149, at 1326 ("The Fourth Amendment protects power not privacy."); *see also* United States v. Martinez-Fuerte, 428 U.S. 543, 554 (1976) (asserting that the Fourth Amendment protects against "arbitrary and oppressive interference by enforcement officials").

193. *See* Donohue, *supra* note 190 (describing the English and colonial background in which the Fourth Amendment was developed); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (detailing how the Fourth Amendment was historically connected to property rights and physical intrusion); 2 LEGAL PAPERS OF JOHN ADAMS 142–44 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965) (stating that general warrants violate "the freedom of one's house").

194. *See* Ku, *supra* note 149, at 1326 (arguing that the Fourth Amendment is about power rather than privacy and describing its role as a bulwark against government authority). Ku argues that the Fourth Amendment should be read alongside the rest of the Constitution as a means of defining and limiting governmental power. *Id.* at 1337 ("[A] primary goal of the Fourth Amendment is the same as that of the entire Constitution—to define and limit governmental power.").

195. *See id.* at 1326 ("[T]he amendment is best understood as a means of preserving the people's authority over government—the people's sovereign right to determine how and when government may intrude into the lives and influence the behavior of its citizens.").

196. Justice Black predicted this in his dissent in *Katz v. United States*. 389 U.S. 347, 374 (1967) (Black, J., dissenting) ("The history of governments proves that it is dangerous to freedom to repose such powers [linking Fourth Amendment to 'privacy'] in courts.").

public.[197] When a person on the street knows too much about you, it can range from an annoyance to a potentially serious problem. When law enforcement knows too much about you, it can put you in prison.[198]

This is not to suggest that considerations of privacy should have no role in Fourth Amendment jurisprudence. Rather, it is to say that the Fourth Amendment does not apply only to actions carried out in private life.[199] As the ability of law enforcement to surveil and record public spaces increases, the reasoning that activities carried out in those spaces are per se not Fourth Amendment searches makes less and less sense.[200]

Traditional Fourth Amendment law has determined whether a search occurred based on where and how the fruits of a search were *collected*.[201] This focus on the methods of collection, rather than the use of the information itself, has diluted the effectiveness of the Fourth Amendment as a limitation on government power. In the past, this conflation of the collection and use of information was unimportant, because there was little difference between the two. But as technology has changed the methods and capabilities of surveillance, the flaws of a singular focus on collection have become glaringly apparent.[202]

197. Ku, *supra* note 149, at 1369 ("[W]hether members of the public may invade our privacy does not answer the question of whether government may."). This approach also diminishes the strength of the argument that the government should be able to freely surveil society because "privacy is dead." *See, e.g.*, Calvin C. Gotlieb, *Privacy: A Concept Whose Time Has Come and Gone*, *in* COMPUTERS, SURVEILLANCE, AND PRIVACY 156 (David Lyon & Elia Zureik eds., 1996) (arguing that people do not really value privacy); Christopher Mims, *Privacy Is Dead. Here's What Comes Next*, WALL ST. J. (May 6, 2018, 8:00 AM), https://www.wsj.com/articles/privacy-is-dead-heres-what-comes-next-1525608001 [https://perma.cc/YZ7T-LJGG].

198. *See Carpenter*, 138 S. Ct. at 2214 ("[T]he Amendment seeks to secure 'the privacies of life' against 'arbitrary power.' . . . [A] central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" (first quoting Boyd v. United States, 116 U.S. 616, 630 (1886); and then quoting United States v. Di Re, 332 U.S. 581, 595 (1948))); David Alan Sklansky, *Too Much Information: How Not To Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1088 (2014) (arguing that lack of anonymity is a distinct issue from freedom from police surveillance).

199. *See Carpenter*, 138 S. Ct. at 2217 ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere.").

200. *See supra* note 93 and accompanying text (discussing advancing surveillance technology).

201. *See* SOLOVE, *supra* note 169, at 110 (describing Fourth Amendment doctrine's historical focus on where surveillance takes place); *see also* Slobogin, *supra* note 97, at 6 (describing the focus on property concepts in Fourth Amendment analysis).

202. *See, e.g.*, Donohue, *supra* note 41, at 613 ("Locational data, collected in bulk, yields deep insight into individuals' lives.").

B. FOURTH AMENDMENT SEARCHES CAN OCCUR AFTER DATA IS COLLECTED

This Section argues that Fourth Amendment searches can occur throughout the data life cycle, including at the point of use as well as the point of collection. Although Fourth Amendment scrutiny has typically focused on the collection stage, emergent technologies have allowed for data to be used in new ways that should also be considered searches. Facial recognition tracking is one such use. Facial recognition tracking is distinct from facial identification, which is a use of data that is unlikely to be considered a Fourth Amendment search. Because facial recognition tracking aggregates multiple points of data about a person to reveal information of a deeply revealing nature, it should be considered a Fourth Amendment search, which courts can recognize through employing use restrictions.

1. Searches Can Occur Throughout the Data Life Cycle

Recall that the "data life cycle" refers to the multiple points of the process through which human operators interact with data.[203] Traditionally, Fourth Amendment law (and data law more broadly)[204] has focused on the collection phase of the data cycle by limiting the ability of law enforcement to collect information about a person.[205] But as bulk data collection has become easier and cheaper, the way that data is used must also be scrutinized.

Historically, collection was limited by human senses.[206] Collecting massive amounts of data was simply too costly to be a regular occurrence, as the Court emphasized in *Carpenter*.[207] This meant that

203. *See* MCGEVERAN, *supra* note 38; *supra* notes 38–40 and accompanying text.

204. *See* MCGEVERAN, *supra* note 38, at 327–28.

205. *See* discussion *supra* Part I.C; *see also supra* note 87 (citing cases applying the *Katz* test); Lipman, *supra* note 40, at 440 ("The Court's Fourth Amendment doctrines are currently built around regulating collection . . . [.]").

206. *See* Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law*, *in* THE FUTURE OF THE CONSTITUTION 3 (2011) ("In [the past], surveillance systems were simple. The 'system' was really just a person. The person would listen or watch. If he saw something notable, he would tell others about it.").

207. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("[Employing traditional surveillance methods] 'for any extended period of time was difficult and costly and therefore rarely undertaken.'" (quoting United States v. Jones, 565 U.S. 400, 429 (2014) (Alito, J., concurring))); *see also* Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents out of* United States v. Jones, 123 YALE L.J.F. 335, 341–50 (2014) (attempting to quantify the reduced costs in various methods of surveillance); Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1375 (2004) ("But one of the hallmarks of new surveillance technologies is the degree to which they lower the costs, both in time and expense, of round-the-

practical and logistical limitations served as effective protections of Fourth Amendment rights. Additionally, there was not a meaningful distinction between collection and use—the difficulty of collecting information served as an effective proxy for protecting the use of information, and once something was obtained by police, they were not able to garner additional information from how they used it. Thus, the use of information was more or less controlled by regulating its collection.[208]

Today, however, data can be collected in broad, sweeping ways that are not subject to human or cost constraints.[209] For example, the NSA famously attempted to create a database of all phone calls made on the Verizon network in its bulk metadata program.[210] Indeed, it is becoming increasingly possible to collect data on everyone, all the time.[211] That data can then be stored and accessed indefinitely, as well as analyzed for further insights.[212] The network of surveillance cameras described in Part I is another example of this type of data collection. With enough storage capacity, such a network could be used to store the entirety of its recordings, which could then be accessed at any time. Because this level of collection leads to enormous new surveillance capabilities, it also creates new Fourth Amendment liabilities.

The regulation of data collection, while important, does not fully protect Fourth Amendment rights in the modern day.[213] Collection and use are distinct components of the modern surveillance process, and each of these phases can raise Fourth Amendment concerns, as scholars have recognized.[214] The use of information threatens harms

clock monitoring."). *See generally* Lipman, *supra* note 40 (describing how the limitations on how police can use evidence have changed).

208. As Professor Orin Kerr puts it: "The government cannot misuse evidence if it does not have it in the first place." Kerr, *supra* note 206, at 4.

209. *See, e.g.*, Sklansky, *supra* note 198, at 1085–87 (describing pervasiveness of various forms of surveillance in modern society).

210. Henderson, *supra* note 64, at 940–44.

211. *Id.* at 935–36 (describing how "technology increasingly permits capture of almost all information").

212. *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1468 (2000) (explaining the distinction between technologies that enable data gathering and the organization and analysis of that data).

213. *See* Donohue, *supra* note 41, at 628 ("[T]o the extent that the Fourth Amendment analysis hinges on an initial determination at the moment of collection, it does not provide for a later interest to arise as the volume of information expands.").

214. *See* Krent, *supra* note 8, at 51 ("[T]he reasonableness of a seizure extends to the uses that law enforcement authorities make of property and information even after lawful seizure."); Kerr, *supra* note 206, at 4 ("There are now four basic stages of

to Fourth Amendment protections that are distinct from those caused by the collection of that information. Protecting the information itself from government searches requires that a Fourth Amendment analysis be applied to its use. Indeed, in some cases, like facial recognition tracking, the use of information may result in constitutional harm even if the information was legally collected.

2. Facial Tracking Should Be Considered a Search Even If Facial Identification Is Not

Recall that "facial identification" refers to the use of facial recognition technology to identify someone.[215] This is distinct from facial tracking, which uses multiple points of facial identification to chronicle a record of a person's movements.[216] Though some have argued that facial identification should itself be considered a Fourth Amendment search, it is most likely sufficiently analogous to existing modes of policing that have been found constitutional to not be considered a search. However, because location aggregation is deeply revealing, facial recognition tracking raises Fourth Amendment harms that facial identification does not. As a result, facial recognition tracking should be considered a Fourth Amendment search.

a. Facial Identification Is Unlikely To Be Considered a Search

Rightfully recognizing the surveillance capabilities of facial recognition technology, some scholars argue that facial identification should be considered a Fourth Amendment search.[217] However, this is unlikely to be the case under current doctrine. First, the police do have some right to surveil public spaces.[218] While others have argued for a

computer-based surveillance systems: 1) data collection, 2) data manipulation by a machine, 3) human disclosure, and 4) public disclosure.").

215. *See* discussion *supra* notes 30–37 and accompanying text.

216. *Id.*

217. *See, e.g.*, Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1595 (2017); Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 411 (2014); Elizabeth Snyder, Note, *"Faceprints" and the Fourth Amendment: How the FBI Uses Facial Recognition Technology To Conduct Unlawful Searches*, 68 SYRACUSE L. REV. 255, 257–58 (2018); Claudia Cuador, Comment, *From Street Photography to Face Recognition: Distinguishing Between the Right To Be Seen and the Right To Be Recognized*, 41 NOVA L. REV. 237, 240 (2017).

218. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."); 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(g) (6th ed. 2020) (describing law allowing police to surveil public); *see also* United States v. Dionisio, 410 U.S. 1, 14 (1973) ("No person can have a reasonable expectation that others

right to anonymity under the Constitution,[219] this is not consistent with the historical origins of the Fourth Amendment or its modern jurisprudence.[220] This likely remains true even following *Carpenter*; while *Carpenter* shifts the *Katz* test, it is unlikely that *Carpenter* stands for the proposition that the police cannot identify a person in public, even through the use of sophisticated technology.[221]

Second, identifying a person at a single point is unlikely to yield information of a "deeply revealing nature"[222] that exposes the "privacies of life."[223] These problems arise through the aggregation of a person's location at multiple points in time, not necessarily from any one point. This is the "whole of their physical movements" that is protected in *Carpenter*.[224] It is difficult to see how the identification of a person, even with a substantially enhanced tool like facial recognition, is sufficiently different from existing, constitutionally permissible police methods to constitute a Fourth Amendment search.[225] As the Massachusetts Supreme Court observed in a 2020 case: "It is an entirely ordinary experience to drive past a police officer in a cruiser

will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world."); *supra* note 87 and accompanying text (presenting cases where police surveillance of public spaces was permitted). *But see* Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 62–63 (2014) (arguing that the Court should reexamine its doctrine that the Fourth Amendment does not provide protection in public areas). Note also that there may be special circumstances or locations (such as a public protest, voting center, or other politically sensitive locations) where identification using facial recognition technology is considered a search for Fourth Amendment purposes. *See, e.g.*, Julian R. Murphy, *Chilling: The Constitutional Implications of Body-Worn Cameras and Facial Recognition Technology at Public Protests*, 75 WASH. & LEE L. REV. ONLINE 1, 6 (2018). Further exploration of these ideas is beyond the scope of this Note.

219. *See, e.g.*, Brown, *supra* note 217; Slobogin, *supra* note 173.

220. *See* Brown, *supra* note 217, at 417–20 (describing lack of anonymity at the time of the American Revolution).

221. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018); Katz v. United States, 389 U.S. 347 (1967).

222. *Carpenter*, 138 S. Ct. at 2223.

223. Boyd v. United States, 116 U.S. 616, 630 (1886).

224. *Carpenter*, 138 S. Ct. at 2217.

225. *See* United States v. Knotts, 460 U.S. 276, 282 (1983) ("Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."). *But see* State v. Muhammad, 451 P.3d 1060, 1071 (Wash. 2019) (demonstrating the argument that they are different in kind, not just degree, in finding that a one-time "ping" of a cell phone to determine its location using CSLI was a search under the Fourth Amendment).

observing traffic on the side of the road, and, of course, an officer may read or write down a publicly displayed license plate number."[226]

An application of these principles to an instance of real-life identification helps to illustrate the point. In 2017, police pulled a man over following a high-speed chase but were unable to identify him.[227] Officers took a photo of the man and used facial recognition to compare it to a large database, revealing his identity.[228] Though this is the type of comprehensive technology contemplated by *Carpenter*, and his inclusion in the database may well have been involuntary, this type of identification does not result in deeply revealing information. It is analogous to identifying someone from memory or based on their fingerprints. As a result, this type of identification probably does not implicate the Fourth Amendment under the current doctrine.

Thus, this Note operates under the assumptions that the collection of facial recognition data and facial identification through the use of that data are unlikely to be considered Fourth Amendment searches. While a deeper exploration of the constitutional issues posed by facial identification is beyond the scope of this Note, the appropriate solution to that problem is likely to be legislative rather than judicial.[229]

b. Facial Recognition Tracking Should Be Considered a Search

Facial recognition tracking, however, reveals an additional layer of information about a person. Because this information—a record of a person's movements—is deeply revealing, facial recognition

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

227. *See* Valentino-DeVries, *supra* note 42.

228. *Id.*

229. In a representative democracy, the appropriate forum for a comprehensive determination of the role facial recognition should play in society is through the representatives of the people. Legislatures are politically accountable and thus more suited to decide policy questions that require balancing trade-offs. They also are institutionally suited for fact-finding in a way that the courts are not. Article III requires that the courts decide cases or controversies, meaning they are limited to the facts of the case in front of them. This is a poor way to make broad policy. *See, e.g.*, *Facial Recognition Technology: (Part 1) Its Impact on Our Civil Rights and Liberties: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. 5 (2019) (written testimony of Professor Andrew Guthrie Ferguson) [hereinafter *Hearing*]. Justice Alito has been the leading voice on the Court for the position that comprehensive regulation should come from the legislature. *See Carpenter*, 138 S. Ct. at 2261 (Alito, J., dissenting) ("Legislation is much preferable to the development of an entirely new body of Fourth Amendment caselaw for many reasons, including the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope.").

tracking should be considered a search. The primary reason that the use of facial recognition tracking raises its own set of harms is due to the phenomenon of aggregation—the aggregation of location data reveals additional information about the person.[230] Various forms of technology, including facial recognition, allow government entities to legally collect vast troves of data which can then be stored for later use and analysis.[231] Once collected, this data can be aggregated. Because it can reveal trends and patterns, aggregated data allows for "a qualitatively more complete picture of that individual to be drawn."[232] Professor Daniel Solove calls this the "aggregation problem."[233] The aggregation of data yields additional information—the whole is greater than the sum of its parts.[234] This is the power of big data.

Facial recognition tracking is a means of learning information about a person through the aggregation of data. It combines data points of a person's location based on the appearance of their face at that location. Each point, in theory, could have been legally collected. However, when the points are aggregated, the data provides a much more complete picture of a person's life.[235] Identifying a person standing outside of an office building will reveal their name. But the aggregation of data showing them arriving at that building each morning and leaving each night reveals additional information about them—they probably work there. Aggregating data showing that person

230. *See* Donohue, *supra* note 41, at 626–27 (describing how location data provides "profound" insight into individuals' private lives).

231. *See* Lipman, *supra* note 40, at 441 ("[A facial recognition camera network] could allow law enforcement to search for any individual, anywhere in a city, going back for weeks or months, depending on how much cheap data storage the city invested in."); Blitz, *supra* note 207 ("But one of the hallmarks of new surveillance technologies is the degree to which they lower the costs, both in time and expense, of round-the-clock monitoring.").

232. *See* Ferguson, *supra* note 148, at 574–75.

233. *See* Solove, *Access and Aggregation*, *supra* note 182, at 1185 ("Viewed in isolation, each piece of our day-to-day information is not all that telling; viewed in combination, it begins to paint a portrait about our personalities. The aggregation problem arises from the fact that the digital revolution has enabled information to be easily amassed and combined.").

234. *See* Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 21 (2020); *see also* Kerr, *supra* note 206, at 8 ("[C]omputer surveillance and modern camera surveillance tend to work by gathering more information that is less invasive per datum, and then manipulating it through electronic methods to yield important information that normally would be obtainable only through more invasive surveillance techniques."); Donohue, *supra* note 41, at 628 ("The value of aggregated information changes when there is more of it.").

235. *See* Donohue, *supra* note 41 ("Locational tracking shows where you go, what you do, and who you are with when you do so.").

leaving the office building and data showing them at a Planned Parenthood, a synagogue, or a political event reveals even more information.

The Court has struggled with its response to the problems of data aggregation.[236] In *Jones*, it indicated awareness that it was addressing a Fourth Amendment issue of a different nature than in previous cases. Justice Sotomayor's concurrence specifically noted that it was aggregation that gave rise to the harms in that case.[237] Recall Professor Krent's 1995 argument that use restrictions were one such solution to this problem.[238] Writing twenty-three years later, Rebecca Lipman argued that the Court has been moving towards use restrictions doctrinally and should now do so explicitly.[239]

This Note sees *Carpenter* as signaling tacit agreement from the Court.[240] Rather than focusing solely on collection, which asks whether the police properly obtained information, *Carpenter* broadened judicial scrutiny of what the police can *do*, holding that individuals have a reasonable expectation of privacy in certain types of information.[241] Thus, instead of constantly adjusting its collection-based doctrine to advancing technology, the Court moved to impose protections on certain types of information itself—information that is "deeply revealing."[242] This is the basis for the third *Carpenter* factor. The exact point at which this occurs remains unclear,[243] but the Court

236. *See supra* note 108 and accompanying text.

237. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (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." (emphasis added)).

238. *See* Krent, *supra* note 8.

239. *See generally* Lipman, *supra* note 40 (arguing that the Court has considered how law enforcement uses information in its Fourth Amendment analysis but has been reluctant to say so openly). Lipman argues that a use restriction-based approach to the Fourth Amendment is the most effective way to ensure its relevance going forward, and that the Court should openly embrace such an approach.

240. Lipman mentions *Carpenter* but does not read it this way. She argues that it was significant for the third-party doctrine but did not apply to direct government surveillance. *See id.* at 446. I disagree with Lipman based on both the text of *Carpenter* itself as well as the interpretations of other scholars. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy . . . ."); *see also* Ohm, *supra* note 124.

241. *See Carpenter*, 138 S. Ct. at 2218–19; *see also* Kerr, *supra* note 123, at 6–7.

242. *Carpenter*, 138 S. Ct. at 2223.

243. *See infra* Part III.A.2.

has indicated its awareness that the use of data through aggregation can pose constitutional concerns.

In embarking on this shift the Court continued the natural progression of the reasoning it had previously applied in *Jones* and *Riley*.[244] Modern surveillance methods give police new tools and represent new threats to the Fourth Amendment.[245] Digital technologies can transform police practices because they are a paradigm shift.[246] And people have some reasonable expectation of privacy in what the government can learn about them, even in public.[247] In a computerized age of vast digital libraries, protection of this right requires restrictions on how police can *use* data in addition to restrictions on how they can collect it.

The surveillance apparatus described in Part I collects facial recognition data which can then be aggregated and used by police.[248] The collection of this data at any particular point is unlikely to be considered a search for the purposes of the Fourth Amendment under current doctrine.[249] But because the use of these aggregated data to track a person present independent Fourth Amendment concerns, that use should be analyzed as an independent search.[250]

Technological and political trends indicate that the United States is rapidly moving towards a future where facial recognition tracking systems can be accessed and used as a mass surveillance tool.[251] The next Section describes how these practices and intended practices are indicative of the broader problem at issue: the Fourth Amendment

244. *See* United States v. Jones, 565 U.S. 400 (2012); Riley v. California, 573 U.S. 373 (2014); *supra* Part I.B.2.

245. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (describing Fourth Amendment threats from novel forms of surveillance).

246. *Riley*, 573 U.S. at 393 (describing the assertion that searches of all data stored on a cell phone is "materially indistinguishable" from searches of physical items "is like saying a ride on horseback is materially indistinguishable from a flight to the moon").

247. *See Carpenter*, 138 S. Ct. at 2217; *cf. Riley*, 573 U.S. at 400 ("[T]he fact that a search in the predigital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery.").

248. *See supra* Part I.B; *infra* Part II.C.

249. *See supra* note 218 and accompanying text; *see also* United States v. Dionisio, 410 U.S. 1, 14 (1973) ("No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world.").

250. *See* Lipman, *supra* note 40, at 456 ("[T]he Court should find that certain uses are Fourth Amendment searches in their own right that can be analyzed for reasonableness independently of their antecedent collection.").

251. *See* LAW ENF'T IMAGING TECH. TASK FORCE, LAW ENFORCEMENT FACIAL RECOGNITION USE CATALOG (2019) (describing current uses of facial recognition technology).

right to be free from "too permeating a police surveillance" is violated by the unregulated use of facial recognition tracking.[252]

C. UNBRIDLED USE OF FACIAL RECOGNITION TRACKING VIOLATES THE FOURTH AMENDMENT

The growing facial recognition infrastructure and rapidly improving tracking capabilities described in Part I indicate that, in the near future, law enforcement will be capable of freely tracing the movements of every person in a systematic, computerized fashion.

Like CSLI, the aggregation of facial recognition data will enable the creation of a comprehensive record capable of revealing the whole of a person's movements.[253] But unlike with cell phones, which one can choose not to use (or, in some cases, to turn off CSLI), a person appearing in public does not have the option of not showing their face.[254] Once this system is in place, individual location data will be accessible at will by law enforcement for a variety of purposes.[255]

Law enforcement agencies are likely to use such powers broadly—in fact, they are already signaling their intention to do so. For example, the Detroit Police Department includes in its facial recognition policy that face recognition information is authorized to "investigate and/or corroborate tips and leads."[256] This broad prerogative would enable officers to surveil a wide range of regular activity with no warrant and no knowledge on the part of the person being watched. The same document cites the Department's right to "connect the face recognition system to any interface that performs live video, including cameras, drone footage, and body-worn cameras."[257]

252. *See Carpenter*, 138 S. Ct. at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

253. *See* Hern, *supra* note 42.

254. For an interesting report on the burgeoning business of providing people with clothing that can elude facial recognition, see John Seabrook, *Adversarial Man*, NEW YORKER (Mar. 16, 2020). However, facial recognition is improving in its ability to identify masked faces. *See Face Recognition Software Shows Improvement in Recognizing Masked Faces*, NAT'L INST. STANDARDS & TECH. (Dec. 1, 2020), https://www.nist.gov/news-events/news/2020/12/face-recognition-software-shows-improvement-recognizing-masked-faces [https://perma.cc/FFJ6-SKK9].

255. *See* Garvie et al., *supra* note 66 (describing how facial recognition can alter policing methods).

256. *See* CRIME INTEL. UNIT, DETROIT POLICE DEP'T, STANDARD OPERATING PROCEDURE § 8: FACIAL RECOGNITION 8.2(c)(v) (2019).

257. *Id.* at 8.5(c).

Federal agencies are also eager to make use of facial recognition tracking.[258] The FBI already uses facial recognition technology in active investigations[259] and has also expressed its desire to use face tracking to "track people's movements to and from 'critical events.'"[260] Other federal agencies, including the Department of Homeland Security, the Transportation Security Administration, and Immigration and Customs Enforcement are also using facial recognition technology in their operations.[261] Although these operations appear to be currently limited to facial identification, there is no reason to believe that they would not expand to include facial tracking in the future in the absence of further legal protection.

Thus, pending federal legislation, it is likely that in many places in the United States, law enforcement's use of facial recognition to identify people will soon be the norm. Given the rate at which facial

258. *See* KIMBERLY J. DEL GRECO, SEARCH ANNIVERSARY: THE NEXT 40 YEARS: FUTURE TRENDS IN LAW ENFORCEMENT 6 (2009) (describing FBI's goal of using biometric data to "[r]eveal movement patterns").

259. The FBI does so through its Facial Analysis, Comparison, and Evaluation (FACE) Services Unit. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 70, at 3. FACE Services uses the NGI-IPS system as well as separate databases maintained by the State Department and various state governments, which contain photos obtained for noncriminal purposes, including driver's license and visa applicant photos. *Id.* In all, more than 641 million photos were available to the FACE Services program as of 2018, including passport and driver's license photos. *See also* Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches [https://perma.cc/JB6Z-HNEN].

260. LYNCH, *supra* note 13, at 20 (citing RICHARD W. VORDER BRUEGGE, FBI, FACIAL RECOGNITION AND IDENTIFICATION INITIATIVES 5 (2010)). For a comprehensive overview of the FBI's use of facial recognition as of 2012, see generally Donohue, *supra* note 103, at 425–51.

261. U.S. DEP'T OF HOMELAND SEC., DHS/TSA/PIA-046, PRIVACY IMPACT ASSESSMENT FOR THE TRAVEL DOCUMENT CHECKER AUTOMATION USING FACIAL RECOGNITION (2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-046-tdcautomationusingfacialrecognition-january2018.pdf [https://perma.cc/EK6Q-PS6F]; *see also* Bill Chappell, *ICE Uses Facial Recognition To Sift State Driver's License Records, Researchers Say*, NPR (July 8, 2019), https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers-sa [https://perma.cc/4ADW-P88Z]; Catie Edmonson, *ICE Used Facial Recognition To Mine State Driver's License Databases*, N.Y. TIMES (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html [https://perma.cc/B26P-XF4N]; Jon Porter, *US Facial Recognition Will Cover 97 Percent of Departing Airline Passengers Within Four Years*, VERGE (Apr. 18, 2019), https://www.theverge.com/2019/4/18/18484581/us-airport-facial-recognition-departing-flights-biometric-exit [https://perma.cc/M9ZT-GPCZ] (reporting that the Department of Homeland Security has said that it plans to use facial recognition on 97% of airline passengers by 2022).

recognition technology is advancing, it is also likely that today's capabilities represent only the tip of a surveillance iceberg. It will soon be possible to query a person's name against a database containing records of the movements of full populations, giving the user the ability to build a profile of a person based on their movements.[262] Such capabilities give the user immense power over the movement, location, and association of citizens.[263] This is true for any user, but *especially* the government.[264]

Facial recognition tracking (and other comprehensive surveillance methods) also creates wholly novel threats to security. As a surveillance apparatus matures, its focus shifts from the detection of crime to its *prevention*, with a focus on "predicting future risky behaviors and/or people."[265] Such predictions could even be based on a person's mental or emotional state rather than their actions.[266] These

262. *Hearing*, *supra* note 229 ("One potential form of face surveillance is the ability to search stored footage from networked surveillance cameras. . . . The resulting scans could map the location of individuals at any point they are identified by a camera." (footnote omitted)).

263. *See* Hartzog, *supra* note 184; Garvie et al., *supra* note 66.

264. *See infra* Part II.B.

265. Ayse Ceyhan, *Surveillance as Biopower*, *in* ROUTLEDGE HANDBOOK OF SURVEILLANCE STUDIES, *supra* note 173, at 43. This algorithmic approach is also known as preemptive or predictive policing. For an excellent summary of the dangers of this preemptive approach to policing, see generally ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017). *See also* CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION 101–03 (2016) (arguing that preemptive policing is reactive and diverts focus away from improving social problems). Chicago is already using algorithms to predict violent crimes. *See* John Buntin, *Social Media Transforms the Way Chicago Fights Gang Violence*, GOV'T TECH. (Sept. 30, 2013), https://www.govtech.com/public-safety/Social-Media-Transforms-the-Way-Chicago-Fights-Gang-Violence.html [https://perma.cc/T3HX-CE4E]. Predictive policing has also been used in Rochester, Minnesota. *See* Maya Rao, *Rochester Hopes Predictive Policing Can Steer Juveniles away from Crime*, STAR TRIB. (Oct. 24, 2014), https://www.startribune.com/rochester-police-plan-to-target-at-risk-teens-raises-concerns/280385202 [https://perma.cc/P3XN-7NTU]. Aziz Huq argues that predictive policing exacerbates the racial imbalances in the criminal justice system. *See* Aziz Z. Huq, *Racial Inequality in Algorithmic Criminal Justice*, 68 DUKE L.J. 1043 (2019). For one pop-culture depiction of a world that employs predictive policing, see MINORITY REPORT (20th Century Fox & Dreamworks Pictures 2002).

266. For example, Amazon Rekognition boasts its ability to not only identify individuals but also analyze their sentiments. *See* Ranju Das, *Amazon Rekognition Announces Real-Time Face Recognition, Support for Recognition of Text in Image, and Improved Face Detection*, AWS: AWS MACH. LEARNING BLOG (Nov. 21, 2017), https://aws.amazon.com/blogs/machine-learning/amazon-rekognition-announces-real-time-face-recognition-support-for-recognition-of-text-in-image-and-improved-face-detection [https://perma.cc/6TKH-5SQ5] ("With this improvement, you can accurately capture demographics and analyze sentiments for all faces in group photos,

uses of the surveillance system are initially presented as social goods, or ways to protect citizens from themselves and one another.[267] Such systems tend to keep growing, justifying their expansion through the promise of ever-greater security.[268] And of course, they are always susceptible to human abuses and biases.[269] The end result is a vast expansion in state power at the expense of individual liberty.

The comprehensive surveillance power enabled by facial recognition tracking is the essence of "too permeating police surveillance."[270] It enables the government to know who is present at sensitive events like public protests, religious gatherings, or political rallies.[271] But more than that, it simply reinvents the boundaries between citizen and state—everything you do and everywhere you go becomes subject to state inspection and scrutiny.[272] This type of

crowded events, and public spaces such as airports and department stores."); *see also* Seabrook, *supra* note 254 (describing "smart retail" applications that can "harvest demographic information from customers' faces, . . . track and measure 'dwell time,'" and assign "sentiment scores" to faces).

267. *See* Weller, *supra* note 186, at 59 (describing perception of state surveillance as beneficial).

268. *See* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1371 (2004) ("[H]istory . . . shows the temptation of surveillance systems to justify an ever-increasing scope of activity . . . ."); Richards, *supra* note 174, at 1945. Professor Richard Sobel argues that this trade-off ultimately leads to a less secure society. *See* Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37, 38 (2002) ("Because the centralization and monitoring of personal information increases the likelihood of abuses, the power gained by the government to misuse this information typically outweighs their supposed benefits and degrades political and personal identity.").

269. Human use of data also gives rise to additional harms, including an increased likelihood of bias and discrimination. Modern surveillance occurs in three phases: identification, correlation, and discrimination, and the latter two are done by humans. *See* Bruce Schneier, *We're Banning Facial Recognition. We're Missing the Point.*, N.Y. TIMES (Jan. 20, 2020), https://www.nytimes.com/2020/01/20/opinion/facial-recognition-ban-privacy.html [https://perma.cc/5XXR-KAMB]. Correlation involves sorting the population into groups, which naturally leads to discrimination based on those groups. *See* Richards, *supra* note 174, at 1956–58 (citing some of the more notorious instances of this phenomenon, including the sorting of Japanese-Americans during World War II). Although these types of harms are not necessarily Fourth Amendment violations, they are included here as further examples of the potential harms of government surveillance that arise from the use of data.

270. *See* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

271. Gianluca Mezzofiore, *Facial Recognition Could Soon Be Used To Identify Masked Protestors*, MASHABLE (Sept. 11, 2017), https://mashable.com/2017/09/11/facial-recognition-masks-protesters [https://perma.cc/WR9G-MLLN]; *see also* Hartzog, *supra* note 184.

272. *See* James B. Rule, *"Needs" for Surveillance and the Movement To Protect Privacy*, *in* ROUTLEDGE HANDBOOK OF SURVEILLANCE STUDIES, *supra* note 173, at 70 (arguing

arbitrary power is precisely the type of infringement on individual autonomy that is anathema to the American conception of separation between state and individual that the Bill of Rights was written to protect.[273]

It is important to note that facial recognition is very likely to have some role to play in current and future policing.[274] Facial recognition technology is an extremely powerful tool that will improve policing and protect law enforcement officers.[275] Some uses of facial recognition, like identification, are unlikely to violate the Fourth Amendment.[276] And it is encouraging that some departments have adopted procedures governing their use of the technology.[277] But the Supreme Court has rejected the assertion that police departments are free to

that facial recognition and other comprehensive surveillance technologies change what it means to appear in public).

273. *See generally* Ku, *supra* note 149 (arguing that the primary purpose of the Fourth Amendment was protecting the people from government power); *supra* Part I.B.

274. *See, e.g.*, Craig McCarthy, *NYPD Pushes Back Against Facial Recognition Ban*, N.Y. POST (Feb. 2, 2020, 2:20 PM), https://nypost.com/2020/02/02/nypd-pushes-back-against-facial-recognition-ban [https://perma.cc/QA8W-CQ8K] ("Facial recognition is exploding in the private sector, whether or not the Senate wants to ban it for police, which is asinine in my perspective, the private sector is going to develop and use it. It's here and it's going to expand and that's the reality of it." (quoting former police commissioner Bill Bratton)).

275. For example, in 2017 the FBI used facial recognition to identify and arrest a member of its Ten Most Wanted list. *See* Ryan Lucas, *How a Tip—and Facial Recognition Technology—Helped the FBI Catch a Killer*, NPR (Aug. 21, 2019, 5:01 AM), https://www.npr.org/2019/08/21/752484720/how-a-tip-and-facial-recognition-technology-helped-the-fbi-catch-a-killer [https://perma.cc/TC65-YHPC] (describing FBI's use of facial recognition technology to capture gang member Walter Yovany-Gomez). Police departments consistently praise facial recognition as a powerful tool that will protect the public. *See, e.g.*, DHS SCI. & TECH. DIRECTORATE, MOBILE BIOMETRICS (2014), https://www.dhs.gov/sites/default/files/publications/Mobile%20Biometrics_0.pdf [https://perma.cc/VF46-J79J] (asserting facial recognition and other mobile biometric identifiers will protect police and solve previously unsolved crimes); James O'Neill, *How Facial Recognition Makes You Safer*, N.Y. TIMES (June 9, 2019), https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html [https://perma.cc/E5K9-3N46] (discussing how police can utilize facial recognition software to identify criminals without violating people's rights).

276. *See* LAFAVE, *supra* note 218.

277. *See Police Body Worn Cameras: A Policy Scorecard*, *supra* note 62 (listing police departments that have enacted guidelines for biometrics including facial recognition).

regulate themselves.[278] The Court is responsible for determining the constitutional floor.[279]

The Supreme Court has indicated its goal of "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[280] A Fourth Amendment analysis that does not consider police use of a comprehensive record of individual movements to be a "search" is fundamentally at odds with this approach, because such use represents a tremendous increase in government power over the individual.[281] In light of that, if the Fourth Amendment is to remain relevant to contemporary life, it must have a role to play here.[282] *Carpenter*'s new questions and modes of analysis show that the Court agrees.[283] The next Part argues that the proper way to ensure Fourth Amendment protections for comprehensive movement data like facial recognition tracking is by analyzing the use of that data as a search.

III. THE WAY FORWARD—APPLYING USE RESTRICTIONS TO FACIAL RECOGNITION DATA

This Part argues that to protect the Fourth Amendment, courts should apply the factors described in *Carpenter* to the use of facial

278. *E.g.*, Riley v. California, 573 U.S. 373, 382 (2014) (describing the importance of judicial oversight to the "often competitive enterprise of ferreting out crime" (quoting Johnson v. United States, 333 U.S. 10, 14 (1948))).

279. *See generally* Aziz Z. Huq, *Fourth Amendment Gloss*, 113 NW. U. L. REV. 701 (2019) (arguing that the Court looks to police practices in determining constitutional floor).

280. United States v. Jones, 565 U.S. 400, 406 (2012) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)). Professor Kerr describes the struggle to maintain this balance as the "equilibrium-adjustment theory" of the Fourth Amendment. *See* Kerr, *supra* note 206. This understanding of the Fourth Amendment recognizes that the role of the Court is to adjust Fourth Amendment standards as technology changes in order to maintain a relatively constant balance between the individual and the state. As the technology underpinning or inhibiting that surveillance develops, judges must strike a balance. On the one hand, they fear that the unchecked expansion of government power will lead to a dystopian state. But they also fear that too much limitation on government power will lead to anarchy. The equilibrium-adjustment theory is their attempt to solve this problem.

281. *See* Ku, *supra* note 149, at 1331 ("[T]he decision to allow law enforcement to use emerging surveillance technologies is effectively a decision to expand government power at the expense of the public's privacy and security.").

282. *See* Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?*, *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE (Jeffery Rosen & Benjamin Wittes eds., 2011) (arguing that the Court must impose use restrictions to ensure that the Fourth Amendment remains relevant to modern life).

283. *See supra* Part I.C.

recognition tracking data to determine whether a Fourth Amendment search occurred. Accessing more than seven days of tracking data should be considered a search under current law,[284] but this Note argues that to protect the privacies of life, courts should treat any use of facial recognition to aggregate location data as a search. This Part concludes by arguing that a use-based approach to facial recognition technology can protect the constitutional rights of citizens while respecting the separation of powers and providing law enforcement with clear guidelines.

A. APPLYING *CARPENTER* TO THE USE OF FACIAL RECOGNITION TRACKING SHOWS SUCH USE SHOULD BE CONSIDERED A SEARCH

This Section argues that the application of *Carpenter* to the use of facial recognition tracking indicates that such use should be considered a search for Fourth Amendment purposes. *Carpenter* broadens the Fourth Amendment reasonable expectation of privacy test to include whether society reasonably expects the police to have access to certain types of information—namely, information that reveals the whole of a person's physical movements.[285] The use of aggregated facial recognition data implicates this factor in a way that its collection does not. To ensure the integrity of this constitutionally protected information, courts should apply a Fourth Amendment search analysis to the use of facial recognition tracking data.[286]

1. Applying *Carpenter* to the Aggregation of Movements Using Facial Recognition Databases

Recall that *Carpenter* provided three factors that guided its determination that accessing CSLI constituted a search: (1) its "depth, breadth, and comprehensive reach"; (2) "the inescapable and automatic nature of its collection"; and (3) its "deeply revealing nature."[287] These factors are the key to determining whether law enforcement's use of a particular set of data should be treated as a search under the Fourth Amendment. This Subsection shows how these factors apply to facial recognition tracking.

284. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018) ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

285. *See supra* Part I.C.3.

286. *See* Lipman, *supra* note 40, at 456 ("[T]he Court should find that certain uses are Fourth Amendment searches in their own right that can be analyzed for reasonableness independently of their antecedent collection.").

287. *See Carpenter*, 138 S. Ct. at 2223.

The first *Carpenter* factor, "depth, breadth, and comprehensive reach," considers the size and scope of the data.[288] Data obtained via facial recognition systems possess each one of these qualities. These systems possess depth because of their precision—they are able to identify a particular individual at a particular location at a particular time.[289] They possess breadth because they are capable of constantly recording and identifying individuals, and storing that data indefinitely.[290] Finally, they are comprehensive because they are capable of tracking the whole of the population.[291] Thus, facial recognition data is precisely the type of information implicated by this factor.[292]

The "comprehensive reach" factor is also concerned with retroactive search capabilities, or the ability of law enforcement to trace one's movements from before they were suspected of any crime. In *Carpenter*, the Court notes that cell phone records allow police to compile records about a suspect retrospectively.[293] This effectively results

288. *See supra* notes 153–55.

289. *See* GROTHER ET AL., *supra* note 13 (describing the rapid improvements in the accuracy of facial recognition technology); *see also* Donohue, *supra* note 41, at 621 ("Images can be read using facial recognition technology, placing particular individuals in particular places at particular times."). It is true that facial recognition today remains imperfect. *See supra* note 22 and accompanying text. But it is rapidly improving. *See* Castelvecchi, *supra* note 28 (describing rapid improvement in accuracy). And the *Carpenter* majority acknowledged that it "must take account of more sophisticated systems that are already in use or in development." *Carpenter*, 138 S. Ct. at 2218 (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).

290. *See supra* Parts I.B (describing prevalence of cameras throughout American cities), II.B.1 (describing ease of storing data); *see also Hearing*, *supra* note 229 ("Locational tracking by facial recognition (both real time and using stored footage) is technically possible and raises hard Fourth Amendment questions.").

291. *See supra* Part I.B (describing vast networks of both cameras and databases); BAN FACIAL RECOGNITION, *supra* note 61 (interactive map showing facial recognition surveillance throughout the United States); *cf. Carpenter*, 138 S. Ct. at 2218 ("Critically, because location information is continually logged for all of the 400 million devices in the United States . . . this newfound tracking capacity runs against everyone.").

292. It is important to address the Court's statement in *Carpenter* that "[w]e do not . . . call into question conventional surveillance techniques and tools, such as security cameras." *Carpenter*, 138 S. Ct. at 2220. This statement does not apply to facial recognition tracking for two reasons. First, facial recognition tracking is not a "conventional surveillance technique[]"—it is a paradigm shift in surveillance, for the reasons described in Part I.A of this Note. Second, facial recognition tracking implicates each of the factors described in the majority's opinion. A finding that the case does not apply to facial recognition tracking would undermine the majority's reasoning and the broader principles it invokes.

293. *Carpenter*, 138 S. Ct. at 2218 ("Unlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when."); *see also* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J.,

in everyone becoming subject to "tireless and absolute surveillance," and the "police may . . . call upon the results of that surveillance without regard to the constraints of the Fourth Amendment."[294] The Court rightfully rejected this dystopian vision in *Carpenter*, and the principles under which they did so are applicable to facial recognition tracking as well.[295]

The second *Carpenter* factor is "the inescapable and automatic nature" of the collected data.[296] Again, this squarely applies to data collected via facial recognition systems, which can identify a person merely by their appearing in public.[297] As Chief Justice Roberts noted in *Carpenter*, "A person does not surrender all Fourth Amendment protection by venturing into the public sphere."[298] A facial recognition system with cameras on every corner or on every patrolling police officer does not give a person meaningful choice about whether or not to be recorded. Facial recognition tracking works by aggregating this data to provide information about a person's movements. Because the location data is collected in an "inescapable and automatic nature," the second *Carpenter* factor is met.

It's worth noting that the concerns posed by the involuntary nature of cell phones are arguably even more true for facial recognition tracking. In both *Riley* and *Carpenter*, Chief Justice Roberts marvels at the degree to which cell phones have become a part of daily life, calling them "almost a 'feature of human anatomy.'"[299] The Chief Justice cites this pseudo-anatomical quality as part of the reason that cell phone tracking "achieves near perfect surveillance" and thus qualifies as an inescapable and automatic collection.[300] A person's face, of course, *is* a feature of human anatomy, inescapably accompanying a person wherever they go. It is difficult to conceive how one could logically have a reasonable expectation of privacy in the whole of their physical movements as chronicled in their cell phone (which, despite their popularity, remain an optional accessory) but not have that same expectation based on an actual feature of their anatomy.

concurring) ("The government can store such records and efficiently mine them for information years into the future.").

294. *Carpenter*, 138 S. Ct. at 2218.

295. *See Hearing*, *supra* note 229, at 10 ("Such a digitally aware Fourth Amendment [as in *Jones*, *Carpenter*, and *Riley*] would, of course, apply to the problem of facial recognition surveillance and any constitutional challenges to proposed legislation.").

296. *Carpenter*, 138 S. Ct. at 2223.

297. *See* Garvie & Moy, *supra* note 43.

298. *Carpenter*, 138 S. Ct. at 2217.

299. *Id.* at 2218 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

300. *Id.* at 2218, 2223.

The third prong of the *Carpenter* test asks whether a set of data is of a "deeply revealing nature."[301] Echoing the concerns described in Justice Sotomayor's *Jones* concurrence, this prong seeks to protect the "privacies of life" by limiting how much the police can learn about a person.[302] The use of facial recognition data to track a person's movements implicates this factor for the same reasons that using CSLI did in *Carpenter*: the use of aggregated data can potentially reveal the whole of a person's movements rather than their location at a particular point in time.[303] An individual's Fourth Amendment interest in avoiding government scrutiny into "an intimate window into [their] life, revealing . . . the 'privacies of life'" is not dependent on whether the data is obtained via cell phone or face.[304]

Determining whether information is "deeply revealing" on a case-by-case basis is likely unworkable.[305] Moreover, just as the "government's purpose in collecting information does not control whether the method of collection constitutes a search,"[306] the government's *purpose* in a given use cannot control whether that use is a search—such an approach would lead to endless questions about whether a stated use was pretextual. In *Carpenter*, the Court held that that accessing more than seven days of an individual's movements via CSLI is a search but declined to decide whether a shorter interval would also qualify as a search.[307] The Court's decision to cite a particular amount of time passing in finding that a search occurred without indicating the specific point at which it became a search leads to questions—at what point does the aggregation of information become "deeply revealing"? Is it time-based, or could other forms of aggregation constitute a search as well? These remain open questions for CSLI, facial recognition data, and other types of data that may be implicated by

301. *Id.* at 2223.

302. *See id.* at 2217.

303. *See id.*; *see also* United States v. Jones, 565 U.S. 400, 428 (2012) (Alito, J., concurring in the judgment).

304. *Carpenter*, 138 S. Ct. at 2217.

305. The "deeply revealing nature" factor shares this problem with the mosaic theory, because both approaches seek to address the problem that aggregation of information about a person can reveal much more about them than any one piece of that data. The mosaic theory is much maligned in part because it is so difficult to administer: how is an officer supposed to know the point at which she has compiled a "mosaic"? *See* Kerr, *supra* note 108, at 329–33 (describing problems with the mosaic theory including, "What test determines when a mosaic has been created?").

306. Grady v. North Carolina, 575 U.S. 306, 309 (2015) (per curiam).

307. *See Carpenter*, 138 S. Ct. at 2217 n.3 ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

the *Carpenter* factors. The next Subsection attempts to analyze these questions in the case of facial recognition tracking.

2. Aggregation of Location Data Should Be Considered "Deeply Revealing"

It is unlikely that there is a perfect answer for the point at which location aggregation becomes deeply revealing, but the practical demands of policing require that courts attempt to provide clear guidance. There are two approaches that courts could take here. First, they could hold that the aggregation of data spanning some predetermined amount of time constitutes a search. In *Carpenter*, the Court indicated its willingness to use this type of metric to determine whether a search occurred.[308] A second approach is to go further and hold that any aggregation of facial recognition-based location data constitutes a search.

In determining that a search had occurred in *Carpenter*, the Court indicated that seven days of CSLI was sufficient but not necessary.[309] The main difficulty with a time-based approach is determining the amount of time that *is* necessary. Setting a bright-line rule (e.g., seven days or twenty-four hours) may be helpful but is somewhat arbitrary, and the constitutional basis for doing so is not clear. Moreover, many of the concerns raised by *Carpenter* are implicated by aggregating even short periods of a person's travels.

Time-based approaches attempt to delineate the point at which the state interest in effective policing gives way to an individual's constitutional right to be free from unreasonable searches. As discussed in Part II, it is unlikely that using facial recognition technology to identify a person at a single point would be considered a search,[310] and the regulation of facial identification is a matter for legislatures rather than the courts. A proponent for a time-based standard would argue that the aggregation of a single person's movements over a short period of time (say, while fleeing the scene of a crime) is analogous enough to existing methods of policing to avoid being a constitutional violation.[311]

Should courts choose to use a time-based rule, twenty-four hours would be superior to seven days. While both are arbitrary, twenty-

308. *See id.* at 2217; *see also Jones*, 565 U.S. at 430 (Alito, J., concurring) (failing to articulate an exact point at which GPS monitoring became a search but noting "the line was surely crossed before the 4-week mark").

309. *See Carpenter*, 138 S. Ct. at 2217 n.3.

310. *See supra* notes 217–24 and accompanying text.

311. *See supra* notes 225–26 and accompanying text.

four hours is a better point at which to set the cutoff because it would do a better job of protecting "deeply revealing information" while still allowing police to use such data in more typical or emergent instances. It is significantly more difficult to learn about a person's life based on their travels over the course of a single day than over the course of a week.

A second route is holding that any aggregation of location data constitutes a search. Under this theory, using any sort of facial recognition tracking would require a warrant, whether it was over five minutes or five weeks. The reasoning behind this approach is that location information is inherently deeply revealing, even over very short periods. Some courts have endorsed the principle of this approach in holding that the procurement of any CSLI by the state requires a warrant.[312]

The disadvantage of holding any aggregation of location data to be a search is that it may be overinclusive—requiring a warrant for short bursts of location monitoring is more restrictive than analogous methods in the pre-digital age. However, because many of those analogues are themselves suspect under a power-based/original understanding of the Fourth Amendment, this Note argues that the second route is the better of the two options. Therefore, courts should hold that any aggregation of facial recognition data to track a person's movements is a Fourth Amendment search.

Regardless of the viability of either of these approaches, the use of facial recognition records to track an individual for more than seven days should be considered a search under *Carpenter*, where the Court held that accessing seven days of CSLI records constituted a search.[313] For the reasons described above, the factors that the Court used to determine that CSLI was protected apply to facial recognition tracking as well.[314] So, because facial recognition tracking implicates the *Carpenter* factors in the same way as CSLI, the use of more than seven days of facial recognition tracking should constitute a search under current law.

312. *See, e.g.*, Zanders v. State, 118 N.E.3d 736, 739 (Ind. 2019) ("*Carpenter* made clear that seven days' or more worth of CSLI accessed constitutes a search—and also left open the possibility that accessing even fewer days of CSLI could constitute a search. This means that the State generally must obtain a warrant before procuring a person's CSLI."); United States v. Kealoha, No. 17-00582, 2019 WL 573409, at *2 (D. Haw. Feb. 12, 2019) ("Government will generally need a warrant to access CSLI." (quoting *Carpenter*, 138 S. Ct. at 2222)).

313. *See Carpenter*, 138 S. Ct. at 2217 n.3.

314. *See supra* Part III.A.

The main counterargument to this proposal is that the use of facial recognition data is not a search because it occurs after the data has already been collected. This issue goes to the heart of the discussion distinguishing between data collection and use. Under the old, pre-*Carpenter* rules, this argument may have been correct. The fact that the collection itself did not constitute a search would have absolved law enforcement from constitutional scrutiny. However, as discussed throughout this Note, facial recognition tracking is precisely the type of digital innovation addressed in *Carpenter*. The inclusion of the "deeply revealing nature" factor shows that the Court has recognized that data can be constitutionally protected based on what it may reveal as well as how it was collected.

The fulcrum on which this argument rests is the degree to which the aggregation of data can provide new and better information than the data can provide in isolation. Those that argue that there is no need to consider use restrictions are effectively arguing that there is no difference between a policeman on the beat jotting down notes about one's movements and an army of cameras creating an eternal record of movements for every person in the city. This Note asserts that there is a difference,[315] and a practical consideration of Fourth Amendment rights must account for it.

A second counterargument posits that police will only have access to data that was collected in public areas, and because a person does not have any sort of reasonable expectation of privacy in public, then anything captured in public is fair game for law enforcement. But each of these premises is flawed.

First, there could be cameras both inside buildings and out. Private businesses as well as public entities may choose to employ facial recognition identification, and businesses may voluntarily (or potentially be required to) hand such records over to police at their request.

Second, as the Court noted in *Carpenter*, a person does not forego Fourth Amendment protection simply by appearing in public. As discussed, comprehensive surveillance technologies like CSLI and facial recognition have the ability to capture vast amounts of information at low cost, creating the possibility of "tireless and absolute surveillance" for police.[316] Because "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere," it is no longer clear that the fact that information was collected in public renders it free from constitutional scrutiny.[317]

315. *See supra* Part II.B.

316. *See Carpenter*, 138 S. Ct. at 2218.

317. *Id.* at 2217.

B. THIS APPROACH BALANCES FOURTH AMENDMENT RIGHTS AND BROADER PUBLIC POLICY

Applying use restrictions to facial recognition tracking strikes the proper balance between the Fourth Amendment rights of the individual and the broader interests of society. As discussed in Part I, Fourth Amendment jurisprudence is currently in the process of reckoning with these changes.[318]

There are benefits to both security and liberty in permitting broad collection of data and scrutinizing its use. When bulk data is collected, any one data point is unlikely to reveal much information.[319] As discussed throughout this Note, it is the aggregation and use of that data by the police that can raise concerns related to both privacy and liberty.[320] As a result, it is possible to design a surveillance system that can reap the benefits of data aggregation while still protecting the individual liberties guaranteed by the Constitution by shifting the primary focus of the law from collection to use.[321]

This approach recognizes the constitutional rights of individuals by ensuring that the Fourth Amendment plays an oversight role for modern policing. The Fourth Amendment commands that searches be reasonable.[322] By recognizing the use of facial recognition data to track individuals as a search, this rule ensures that the Fourth Amendment will remain relevant to current and future policing. It recognizes that the unrestrained use of a massive surveillance apparatus based on the recording of Americans' faces can threaten every individual's Fourth Amendment rights. Thus, an analysis that accounts for use continues the Court's effort to ensure the "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[323]

Relatedly, a use-based approach provides constitutional oversight to the use of facial recognition data that the government collects from third parties. Many private entities also collect data through

318. *See supra* Part I.C.

319. Kerr, *supra* note 206, at 7–8 ("[C]omputer surveillance and modern camera surveillance tend to work by gathering more information that is less invasive per datum . . . .").

320. *See supra* Part II.B.

321. *See, e.g.*, Kerr, *supra* note 206, at 7 ("To reap those benefits [of surveillance systems], the best way to design surveillance systems is to allow the initial collection but then place sharp limits on the later stages such as disclosure.").

322. U.S. CONST. amend. IV.

323. Kyllo v. United States, 533 U.S. 27, 34 (2001); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting *Kyllo*).

facial recognition technology.[324] Though the future of the third-party doctrine is somewhat uncertain in light of *Carpenter*, it is difficult to imagine banning the police from accessing third-party records at all.[325] The Constitution does not regulate the ability of private entities to engage in such collection. This fact once again underscores the importance of focusing on how that information is *used* when considering questions of surveillance.

This approach also is cognizant of the government interests at stake. First, applying *Carpenter* to the use of facial recognition data tracking rather than deeming all facial recognition collection a search properly reserves the question of how to comprehensively regulate facial recognition technology to the legislature.[326] There are a number of questions legislatures must consider regarding facial recognition technology, beginning with whether to allow it at all.[327] At the time of this writing, some cities[328] and states[329] have decided to ban the use

324. *See, e.g.*, SCHNEIER, *supra* note 183 ("In countries like the United States, [the surveillance apparatus] is being built by corporations in order to influence our buying behavior, and is incidentally used by the government."); *see also* Seabrook, *supra* note 254 ("Where the U.S. leads the world is in the commercial use of face recognition by private companies."). For an excellent discussion of the role of surveillance as a driver of the modern technology economy, see generally SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2019).

325. A full exploration of this concept would require an extensive discussion of the third-party doctrine, including its viability following *Carpenter*, both of which are outside the scope of this Note. It is sufficient for present purposes to assert that there is a reasonable chance the police will continue to be able to access records created in the private sector, including facial databases. *See supra* notes 143, 145.

326. *See supra* note 229.

327. Note that the legislative question of whether to allow police to use facial recognition technology is a distinct question from whether that use is prohibited by the Fourth Amendment.

328. San Francisco was the first major American city to ban government use of facial recognition. *See* Kate Conger, Richard Fausset & Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html [https://perma.cc/L29T-CQCR]. Somerville, Massachusetts, and Oakland, California, followed. *See* Caroline Haskins, *Oakland Becomes Third U.S. City To Ban Facial Recognition*, VICE (July 17, 2019, 6:41 AM), https://www.vice.com/en_us/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz [https://perma.cc/S72L-3UCQ]. For an updated map of cities that have banned the technology, see *supra* note 61.

329. In October 2019, California passed the Body Camera Accountability Act (AB 1215), banning the use of facial recognition technology in police-worn body cameras for three years. *See* Anderson, *supra* note 62; *The Body Camera Accountability Act (AB 1215)*, ACLU S. CAL., https://www.aclusocal.org/en/legislation/body-camera-accountability [https://perma.cc/J76V-Z6MF]. The Massachusetts legislature voted to ban police use of facial recognition, but Governor Charlie Baker refused to sign the legislation into law. Adi Robertson, *Massachusetts Governor Won't Sign Facial*

of facial recognition technology by law enforcement, while others have embraced it.[330]

Additionally, the approach described here is pragmatic. It balances the invasiveness of facial recognition technology with the public interest in allowing some uses of the technology. The use-based approach advocated here allows much of law enforcement's use of facial recognition to go forward as it would under the current model (e.g., identification on the street is not a search or is a reasonable search). But when the use becomes sufficiently invasive, as it does with tracking, the government must justify its actions.[331]

Finally, this approach is administrable. It provides clear notice to police departments that attempts to use facial recognition data to track individuals are subject to Fourth Amendment scrutiny.[332] Departments are already developing standard operating procedures for the use of facial recognition,[333] and the approach described here can easily be conveyed to rank-and-file officers through the use of SOPs and similar documents. Importantly, this rule does not attempt to deny police departments the benefits of facial recognition technology altogether by deeming the collection of facial data or identification using that data to be an unconstitutional search.

C. OF WARRANTS AND REASONABLENESS—TWO PATHS

Once it is determined that the information at issue meets the *Carpenter* test, the use of that information is a search. But what then? The Fourth Amendment prohibits *unreasonable* searches and seizures.[334] The Court's typical approach has been to deem searches in the criminal context per se unreasonable in the absence of a warrant, with

Recognition Ban, VERGE (Dec. 16, 2020), https://www.theverge.com/2020/12/16/22179245/facial-recognition-bill-ban-rejected-massachusetts-governor-charlie-baker-police-accountability [https://perma.cc/K6XN-TKBB]. Other states have introduced similar legislation; for an up-to-date overview of facial recognition policies at the state level, see *State Facial Recognition Policy*, EPIC, https://epic.org/state-policy/facialrecognition [https://perma.cc/J9U9-PRQ9].

330. *See supra* Part I.B (describing cities that have embraced facial recognition technology).

331. Importantly, as the Court recognized in *Riley*, there is a distinction between preventing such searches altogether and the warrant requirement. *See* Riley v. California, 573 U.S. 373, 401 (2014) ("Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search . . . .").

332. *Id.* at 398 ("[O]ur general preference [is] to provide clear guidance to law enforcement through categorical rules.").

333. *See, e.g.*, CRIME INTEL. UNIT, *supra* note 256.

334. U.S. CONST. amend. IV.

some exceptions.[335] As many commentators have observed, this approach has likely made the Court reluctant to label a given practice a search, because the warrant requirement is severe.[336]

In *Carpenter*, after determining that a search had occurred, the Court held that a warrant was required without much discussion.[337] The warrant requirement for anything deemed a search in the criminal context is an even poorer fit in the post-*Carpenter* world, where the Fourth Amendment applies to searches of information.[338] This is apparent in how the lower courts have applied *Carpenter*, generally seeking to limit it to the facts of that case.[339] The tension between the lofty principles articulated throughout *Carpenter* and the reality of modern policing suggests that the Court will eventually need to reconsider the warrant requirement in the context of digital searches.

The Court has two paths to choose from. On the one hand, it could continue on course and deem *Carpenter* searches of facial recognition databases per se unreasonable without a warrant. If that's the case, the analysis ends here—the officer must obtain a warrant supported

335. *See Riley*, 573 U.S. at 382 ("Our cases have determined that '[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant.' . . . In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." (first and second alterations in original) (citation omitted)).

336. *See, e.g.*, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 388 (1974) ("[The] all-or-nothing approach to the amendment puts extraordinary strains upon the process of drawing its outer boundary lines."); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 769 (1994) ("Because it creates an unreasonable mandate for all searches, the warrant requirement leads judges to artificially constrain the scope of the Amendment itself by narrowly defining 'search' and 'seizure.'"). Justice Scalia, writing for the majority in *Kyllo v. United States*, noted this tendency himself. 533 U.S. 27, 32 (2001) ("But in fact we have held that visual observation is no 'search' at all—perhaps in order to preserve somewhat more intact our doctrine that warrantless searches are presumptively unconstitutional.").

337. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) ("Having found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records.").

338. *See* Alan Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J.F. 943, 944 (2019) (arguing that "*Carpenter*'s embrace of a categorical warrant requirement was a mistake"). Professor Rozenshtein also points out the difficulty of applying the warrant requirement to emerging police techniques where the identity of a given individual may not be known at the outset of the investigation. *See id.* at 951.

339. *Id.* at 950–51 nn.33–40 (summarizing how courts are narrowly applying *Carpenter*).

by probable cause to conduct the search or it is inadmissible under the exclusionary rule.[340] Alternatively, the Court could continue the restoration of Fourth Amendment principles embodied in the *Carpenter* shift by returning to the language of the Fourth Amendment and asking whether the search was *reasonable*.

There is strong support for an approach based on reasonableness. First, the text of the Fourth Amendment itself prevents *unreasonable* searches.[341] Second, the Court has acknowledged it in its jurisprudence, noting that the "touchstone of the Fourth Amendment is reasonableness."[342] Finally, an approach that centers on reasonableness would enable the application of the Fourth Amendment to the array of searches that current jurisprudence does not consider as such, including the identification of an individual using facial recognition technology.[343]

Professor Alan Rozenshtein provides a helpful framework for contrasting these two approaches. In his article *Fourth Amendment Reasonableness After* Carpenter, Professor Rozenshtein contrasts *selective* and *regulatory* approaches to the Fourth Amendment.[344] The selective approach is "a narrow-scope, high-requirements position that captures much of contemporary Fourth Amendment doctrine."[345] The regulatory approach, in contrast, embraces the view that "[t]he touchstone of the Fourth Amendment is reasonableness."[346] This approach would apply the Fourth Amendment to a much broader range of activity, but would weigh the interests of the government against the rights of the individual in determining whether a given search was reasonable.[347] Professor Slobogin describes this concept as the

340. *See* Bernard A. Berkman & Gerald S. Gold, *Excluding Illegally Obtained Evidence*, 5 AM. JUR. TRIALS 331 (2020).

341. 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 . . . .").

342. Riley v. California, 573 U.S. 373, 381 (2014) ("As the text makes clear, 'the ultimate touchstone of the Fourth Amendment is "reasonableness."'" (citations omitted)); Grady v. North Carolina, 575 U.S. 306, 310 (2015) ("The reasonableness of a search depends on the totality of the circumstances, including the nature and purpose of the search and the extent to which the search intrudes upon reasonable privacy expectations.").

343. *See supra* Part II.B.2.a.

344. Rozenshtein, *supra* note 338, at 949–52.

345. *Id.* at 949.

346. *Id.* at 952.

347. *Id.*

"proportionality principle."[348] At its core, this approach embraces an idea that is both intuitive and fundamentally reasonable: some searches are more justified than others.

A Fourth Amendment analysis based on reasonableness, rather than on the present search/non-search binary, would have implications for the assertions made throughout this Note. Most significantly, a number of "identification" scenarios, which would not be searches under current doctrine, would likely be considered searches.[349]

Should the Court travel down this road, it would be a sea-change for Fourth Amendment jurisprudence. That probably makes it unlikely in the near term. However, it is nevertheless worth mentioning here because the realities of the digital age will continue to exert pressure on the Court to consider aspects of Fourth Amendment jurisprudence it has long taken for granted.

Note too that this approach is by no means fantasy, nor is it unworkable. *Naperville Smart Meter Awareness v. City of Naperville* showed what a judicial application of this model might look like.[350] Additionally, courts could look to legislative guidance to determine whether a given practice is generally held to be reasonable.[351] Professors Maria Ponomarenko and Barry Friedman convincingly argue that the public can and should set rules for how the police operate.[352] As the public decides, through the legislative process, how it wants the police to use facial recognition technology, the contours of what constitutes a reasonable search will become clearer.

A full exploration of the warrant requirement and its downstream effects is well beyond the scope of this Note. And to be sure, a model where the Court determines that law enforcement must obtain a warrant to conduct a search using certain kinds of facial recognition data would be an improvement over the pre-*Carpenter* state of affairs, where the Fourth Amendment played no role in such an analysis. However, an embrace of reasonableness as the touchstone of the

348. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 17 (2007) ("[W]hen contemplating surveillance (or any other investigative technique), government should be required to provide justification proportionate to the intrusiveness of the surveillance . . . .").

349. But importantly, many such scenarios would likely be considered reasonable searches and thus not Fourth Amendment violations.

350. 900 F.3d 521, 527, 529 (7th Cir. 2018) (finding that a *Carpenter* search had occurred in collection of smart meter data, but applying a reasonableness balancing test to determine that search was reasonable).

351. *See supra* note 229.

352. *See* Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827 (2015).

Fourth Amendment would enable the Court to continue to extend the principles it invoked in *Carpenter* and provide constitutional oversight to the myriad surveillance methods, including facial recognition technology, that are available to modern law enforcement.

CONCLUSION

Facial recognition tracking has the potential to change the nature of public spaces. In the not-so-distant future, a rapidly developing system of cameras and databases will make it possible for data showing all public movements to be recorded and stored. Facial recognition tracking is the aggregation of that data to reveal the whole of an individual's movements, and thus provide the government with a portrait of their life. This Note shows that courts can and should analyze law enforcement's use of facial recognition technology to track individuals as a search under the Fourth Amendment. In *Carpenter*, the Supreme Court signaled that it is changing its approach to applying the Fourth Amendment to police investigations conducted with sophisticated modern technologies. Facial recognition systems are one such technology. Courts should hold that the use of facial recognition data to track individuals is a search under *Carpenter* because such data are comprehensive, collected involuntarily, and when aggregated, reveal the privacies of life. This approach ensures that the Fourth Amendment to the Constitution remains a relevant protection for the American people in the digital age.