University of Cincinnati Law Review

Volume 89 | Issue 2 Article 10

February 2021

Facial Recognition and the Fourth Amendment in the Wake of Carpenter v. United States

Matthew Doktor
doktormw@mail.uc.edu

Follow this and additional works at: https://scholarship.law.uc.edu/uclr

 Part of the Criminal Procedure Commons, Fourteenth Amendment Commons, and the Fourth Amendment Commons

Recommended Citation

Matthew Doktor, *Facial Recognition and the Fourth Amendment in the Wake of Carpenter v. United States*, 89 U. Cin. L. Rev. 552 (2021)
Available at: https://scholarship.law.uc.edu/uclr/vol89/iss2/10

This Student Notes and Comments is brought to you for free and open access by University of Cincinnati College of Law Scholarship and Publications. It has been accepted for inclusion in University of Cincinnati Law Review by an authorized editor of University of Cincinnati College of Law Scholarship and Publications. For more information, please contact ronald.jones@uc.edu.

FACIAL RECOGNITION AND THE FOURTH AMENDMENT IN THE WAKE OF *CARPENTER V. UNITED STATES*

Matthew Doktor

I. INTRODUCTION

By the time you are finished reading this sentence over 20,000 images were uploaded to social media—perhaps even an image of you.[1] And by the end of this sentence, algorithms can produce an index with images of you and corresponding links.[2] Private for-profit technology companies leverage those images and social media posts, scraped from public and private pages, to create databases searchable with facial recognition software.[3] While police have used facial recognition for roughly twenty years, practical limitations restrained that technology.[4] But with billions of images from Facebook, YouTube, LinkedIn, Twitter, and Instagram, this technology can now reveal historic records of a person's movement and associations.[5] Despite the practical necessity of internet and social media participation in modern society, research shows that Americans are uncertain how to control that participation.[6]

For the past century, rapidly developing technology has challenged the judiciary and legal scholars to adapt Fourth Amendment protections to the modern world. Early Fourth Amendment jurisprudence categorized police use of technology as non-searches.[7] But recently the United States Supreme Court questioned that precedent in the face of novel surveillance

1. Rose Eveleth, *How Many Photographs of You Are Out There in the World?* ATLANTIC (Nov. 2, 2015), https://www.theatlantic.com/technology/archive/2015/11/how-many-photographs-of-you-are-out-there-in-the-world/413389 [https://perma.cc/V89M-W7JF].

2. Anna Merlan, *Here's the File Clearview AI Has Keeping on Me, and Probably on You Too*, VICE (Feb. 28, 2020, 7:58 PM), https://www.vice.com/en_au/article/5dmkyq/heres-the-file-clearview-ai-has-been-keeping-on-me-and-probably-on-you-too [https://perma.cc/8XXA-XV9M].

3. Clearview AI founder describes itself as a new research tool for law enforcement. Kashmir Hill**,** *The Secretive Company that Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020, 6:17 PM), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/7VSE-N26K].

4. Robinson Meyer, *Who Owns Your Face?*, ATLANTIC (July 2, 2015), https://www.theatlantic.com/technology/archive/2015/07/how-good-facial-recognition-technology-government-regulation/397289 [https://perma.cc/J6YK-8NYW].

5. Kate Allen, *Face Recognition App Used by Police, Until the Chief Found Out; Civil Liberty Association Slams Use of Controversial Clearview AI Technology*, TORONTO STAR, Feb. 14, 2020., at A1.

6. Emily A. Vogels & Monica Anderson, *Americans and Digital Knowledge*, PEW RSCH. CTR.: INTERNET, SCI. & TECH (Oct. 9, 2019), https://www.pewresearch.org/internet/2019/10/09/americans-and-digital-knowledge/ (last visited Feb 22, 2020) [https://perma.cc/VEY9-34X2].

7. *See generally* Olmstead v. United States, 277 U.S. 438 (1928) (finding no search in a wiretap of a telephone line absent physical trespass); On Lee v. United States, 343 U.S. 747 (1952) (finding no search of a wired informant who transmitted a conversation to a nearby agent because of the permission granted to the informant to enter the premises).

Published by University of Cincinnati College of Law Scholarship and Publications, 2021

technologies.[8] Scholars also warn that this technology threatens privacy rights.[9]

At its core, Fourth Amendment jurisprudence reveals a reluctance to develop bright-line rules for police technology, at the expense of coherence and consistency. Instead the Court conceptualizes the Fourth Amendment and police technology primarily through an amorphous "reasonableness" standard.[10] While the Court describes warrantless searches as *per se* unreasonable and "subject to only a few specifically established and well-delineated exceptions," rapidly developing surveillance technology often blurs these exceptions and forces the Court into doctrinal contortions.[11] In turn, the lower courts are left to wade through inapposite doctrine to reconcile the factual contexts of each individual case.[12] Because of that precedent, some commentators argue for First Amendment protections from facial recognition technology.[13]

Recently, in *Carpenter v. United States*, the Court extended Fourth Amendment protections to third-party cell phone location data.[14] The Court grappled with the imprecise fit of Fourth Amendment jurisprudence and technology described as a "new phenomenon."[15] This Comment asks whether *Carpenter* extends Fourth Amendment protections to facial recognition searches of images mined from social media.

Part I of this Comment examines the development of modern law enforcement technology in the age of social media and algorithms. Part II traces the history of Fourth Amendment privacy rights and digital surveillance leading to *Carpenter*. Finally, Part III argues for the expansion of the decision's underlying principles to emerging facial recognition technology that leverages data derived from social media and internet usage.[16]

8. *See generally* Kyllo v. United States, 533 U.S. 27 (2001).

9. *See* Steven Breyer, *Our Democratic Constitution*, 77 N.Y.U. L. REV. 245, 262 (2002) ("These circumstances mean that efforts to revise privacy law to take account of the new technology will involve, in different areas of human activity, the balancing of values in light of predictions about the technological future."); *see also* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 631 (2017) ("As new technologies develop in the Internet of Things and beyond, the hope is that these informational security principles can be applied to keep the Fourth Amendment smart enough to adapt to these challenges.").

10. *Cf.* Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

11. Arizona v. Gant, 556 U.S. 332, 338 (2009).

12. *See* Sibron v. New York, 392 U.S. 40, 59 (1968).

13. Alexander T. Nguyen, *Here's Looking At You, Kid*: *Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?*, 7 VA. J.L. & TECH. 2, at nn. 45-48 (2002).

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

15. *Id.* at 2216.

16. Hill, *supra* note 3.

II. SURVEILLANCE IN THE DIGITAL AGE

On social media and the internet, privacy concerns quickly temper the allure of connectivity and immediacy. Facial recognition technology programmed on biometric data from images scraped from social media images poses a significant privacy challenge when private companies offer that technology to state actors. Ninety years after the Supreme Court first addressed wiretapping in *Olmstead v. United States*, electronic surveillance is a well-established fact of life.[17] Because of this prevalence, Congress passed legislation to regulate electronic surveillance in 1968.[18] As society entered the digital and information ages, legislatures and judiciaries attempted to delineate the legality of electronic surveillance.[19] Early decisions rested on the foundation that the defendant "assumed the risk" with the use of the technology, determining that a person voluntarily conveying their information through internet-based platforms had no expectation of privacy.[20]

In particular, federal courts have wrestled with government surveillance and data collection issues from social media accounts as early as 2011.[21] While the courts are familiar with the Fourth Amendment implications of electronic surveillance, facial recognition technology is a novel issue with little authority addressing the constitutional issues with its use.[22] Like facial recognition, data scraping and social media surveillance are comparatively recent developments that also threaten privacy rights. Together, these technologies compound privacy concerns.

17. Olmstead v. United States, 277 U.S. 438, 466 (1928) (finding no Fourth Amendment search in the wiretapping of a suspects phone in an investigation without a physical search of a person, home, effects, or papers).

18. The Omnibus Crime Control and Safe Streets Act of 1968 regulated the circumstances and conditions in which oral and wire communications could be surveilled. *See* Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510-2519 (1968)).

19. *See* United States v. Warshak, 631 F.3d 266, 288 (2010) (finding a reasonable expectation of privacy in emails sent and stored on third-party services as analogous to a phone call or a letter, and that compelled disclosure of internet service providers to surrender the contents of a subscriber's email address under the Stored Communications Act is a Fourth Amendment search requiring compliance with the warrant requirement).

20. *See* United States v. Bynum, 604 F.2d 161, 164 (4th Cir. 2010) (quoting Smith v. Maryland, 442 U.S. 735, 744 (1979)).

21. *See In re* Application of The United States of America For An Order Pursuant to 18 U.S.C. § 2703(d)., 830 F. Supp. 2d 114, 131 (E.D. Va. 2011) (finding no reasonable expectation of privacy in the I.P. address information conveyed by users to Twitter when they "chose to use the internet to communicate with the Twitter Service").

22. *See* United States v. Jackson, No. 19-CR-60262CJS, 2020 U.S. Dist. LEXIS 28200, at *32 (W.D.N.Y. Feb. 19, 2020).

A. Web Scraping Social Media

Web scraping, as a general practice, refers to the extraction and collection of internet content for archival, data analysis, information aggregation, and network mapping purposes.[23] As social media users and user data grew, scraping that data from those users became increasingly profitable due to the impressive volume of user data uploaded to those platforms.[24] Even more concerning, scraping can harvest data and images from search results.[25] Those search engine results are indexed through express permissions granted to search engines by social media sites to access user information.[26] And data analytics firms are able to access private Facebook user data through third-party applications contracts with the site.[27]

Data analytics companies like HiQ represent an industry premised on access to data from social media member profiles.[28] While that data can remain anonymous in the aggregate, some private entities harvest user images for the sole purpose of identifying the people in social media images.[29] LinkedIn reported 90 million attempts to scrape data every day from its 50 million users.[30] According to Facebook, third parties have scraped user data from most of its 2.2 billion profiles.[31]

As those industries demonstrate, social media is a cultural mainstay in American society. In the context of the First Amendment, the Supreme Court explained that social media and the "modern internet" are the most powerful mechanisms for modern discourse, information, and connection.[32] Approximately seventy percent of all U.S. adults use Facebook, while photo sharing platforms like Instagram and Snapchat are

23. Andrew Sellars, *Twenty Years of Web Scraping And The Computer Fraud And Abuse Act*, 24 B.U. J. SCI & TECH. L. 372, 374 (2018) (explaining that web scraping has proliferated under the federal Computer Fraud and Abuse Act, which was designed as an anti-hacking measure).

24. Thomas Lee, *LinkedIn-HiQ Spat Raises Big Questions*, S.F. CHRON., Jul. 9, 2017, at D1.

25. Jack Nicas, *Facebook Says Russian Firms 'Scraped' Data, Some For Facial Reco*gnition, N.Y. TIMES (Oct. 12, 2018), https://www.nytimes.com/2018/10/12/technology/facebook-russian-scraping-data.html [https://perma.cc/6CDC-SE3F].

26. HiQ Labs, Inc. v. LinkedIn Corp., 938 F.2d 985, 990 (9th Cir. 2019).

27. Craig Timberg & Elizabeth Dwoskin, *Social Media Sites Helped Police Track Minorities, ACLU Says*, CHI. DAILY HERALD, Oct. 12, 2016, at 16.

28. Louise Matsakis, *Scraping The Web Is A Powerful Tool. Clearview AI Abused It.*, WIRED (Jan. 25, 2020), https://www.wired.com/story/clearview-ai-scraping-web/ [https://perma.cc/HT6Q-T6T9].

29. Matt O'Brien, *Facebook, YouTube: Firm Must Stop Scraping Faces From Sites*, NBC BAY AREA (Feb. 6, 2020), https://www.nbcbayarea.com/news/local/facebook-youtube-firm-must-stop-scraping-faces-from-sites/2228373/ [https://perma.cc/59WN-DUFR].

30. HiQ Labs, Inc., 938 F.3d at 991.

31. Barbara Ortutay, *Facebook: Most Users May Have Had Public Data 'Scraped'*, AP NEWS (Apr. 5, 2018), https://apnews.com/4c5ee5ee573846b68e13e6c3a77b01bf/Facebook:-Most-users-may-have-had-public-data-'scraped' [https://perma.cc/23VC-VHSF].

32. Packingham v. North Carolina, 137 S. Ct. 1730, 1738 (2017).

increasingly popular with teens and young adults.[33] Research shows that Americans know their online activity is tracked, and sixty percent of Americans consider it impossible to go through daily life without having the government collect data about them.[34]

B. Facial Recognition of Biometric Features

While facial recognition technology dates back to the 1960s, modern artificial neural networks coupled with social media images accelerated the development of the algorithms that comprise facial recognition technology.[35] At its core, a facial recognition tool determines whether an image contains a face, individual attributes, or a specific individual by comparing the biometric data in the image to existing photographs stored in a database.[36]

Biometric data is the foundation of facial recognition technology. In its most basic form, biometrics refers to automated recognition of individuals based on biological characteristics—a face, iris, fingerprint, or voice.[37] Due to the permanence and personal nature of facial characteristics as a biometric identifier, biometric data reveals historic and biographical information depending on the application.[38] Facial recognition algorithms train on biometric data and identify unique facial patterns, akin to a facial fingerprint, to create a "faceprint."[39]

As facial recognition remains unregulated technology, corporations, startups, and the government have developed facial recognition algorithms trained on private and public images.[40] Federal investigators increasingly rely on facial recognition as a routine investigative tool, and state law enforcement deploys the tool on low-level crimes like check-

33. Andrew Perrinn & Monica Anderson, *Share of U.S. Adults Using Social Media, Including Facebook, Is Mostly Unchanged Since 2018*, PEW RSCH. CTR. (Apr. 10, 2019), https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/ [https://perma.cc/A65N-6PXR].

34. PEW RSCH. CTR., AMERICANS AND PRIVACY: CONCERNED, CONFUSED, AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION 3 (2019).

35. Lane Brown, *There Will Be No Turning Back on Facial Recognition*, N.Y. MAG. (Nov. 12, 2019),https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html [https://perma.cc/ND5K-AETH].

36. *Facial Recognition Technology: Ensuring Transparency in Government Use: Hearing Before the H. Comm. on Oversight and Reform*, 116th Cong. (Jun. 4, 2019) (statement of Dr. Charles H. Romine, Director of Information Laboratory, National Institute of Technology, Department of Commerce).

37. NAT'L RSCH. COUNCIL, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 18 (Joseph N. Palto & Lynette L. Millett eds., 2010).

38. *Id.* at 111.

39. Abigail Tracy, *Facebook Has Your Faceprint, Here's Why That Matters*, FORBES (June 24, 2015), https://www.forbes.com/sites/abigailtracy/2015/06/24/facebook-has-your-faceprint-heres-why-that-matters/#2294241d18eb [https://perma.cc/RBH7-8NKW].

40. Brown, *supra* note 35.

cashing fraud and petty theft.[41] The FBI and twenty-one state agency databases comprise a network of over 641 million photos from criminal justice databases, driver's license photos, and visa applications.[42] Yet, that massive image database and algorithms are limited due to the nature of the images of individuals directly facing the camera.[43] From 2013 to 2018, the capability of facial recognition algorithms increased exponentially according to the National Institute for Standards and Technology.[44]

But the reliability of facial recognition tools is questionable. Despite rapid technological improvements, vendors creating or executing this technology must navigate changes in facial appearance caused by aging and image quality.[45] In one ACLU study, Amazon's facial recognition tool "Rekognition" erroneously matched twenty-eight members of Congress to images from a 25,000 image mugshot database.[46] Moreover, studies reveal that racial and gender biases permeate facial recognition technology: some commercial algorithms misclassify white women as men at a nineteen percent error rate and women of color as men as often as thirty-five percent of the time.[47] Those error rates are especially concerning in light of government use of social media posts; for example, for surveillance of police brutality protests in Ferguson and Baltimore.[48]

C. Automated and Systemic Surveillance

Clearview AI, an artificial intelligence company, incorporated facial recognition, biometrics, and social media scraping to create a four billion image facial recognition database.[49] The company then commercialized

41. Drew Harwell, *FBI, ICE Find State Driver's License Photos Are A Goldmine For Facial Recognition Searches*, WASH. POST, Jul. 8, 2019, at A08.

42. *Facial Recognition Technology: Hearing Before the H. Comm. on Oversight and Reform*, 116th Cong. (2019) (Statement of Gretta Goodwin, Director of Homeland Security and Justice).

43. Kashmir Hill, *Face Scan App Inches Toward End of Privacy*, N.Y. TIMES, Jan. 19, 2020, at A1.

44. *Facial Recognition Technology: Ensuring Transparency in Government Use: Hearing Before the H. Comm. on Oversight and Reform*, 116th Cong. (Jun. 4, 2019) (statement of Dr. Charles H. Romine, Director of Information Laboratory, National Institute of Technology, Department of Commerce).

45. PATRICK GROTHER, ET. AL., DEPT. OF COMMERCE, NAT'L INST. OF STANDARDS AND TECH., ONGOING FACE RECOGNITION VENDOR TEST, NISTIR 8238 7 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.

46. Jason Murdock, *Amazon Face Recognition Tech Matches 28 Members of Congress with Mugshots*, NEWSWEEK (Jul. 27, 2018), https://www.newsweek.com/amazons-face-recognition-tool-matches-28-members-congress-criminal-mugshots-1044850 [https://perma.cc/29GE-EPRR].

47. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACHINE LEARNING RES. 1, 8 (2018).

48. Craig Timberg & Elizabeth Dwoskin, *Social Media Sites Helped Police Track Minorities, ACLU Says*, CHI. DAILY HERALD, Oct. 12, 2016, at 16.

49. Tim Cushing, *How Much Data Does Clearview Gather On People?*, TECHDIRT (Mar. 27, 2020), https://www.techdirt.com/articles/20200324/17015544165/how-much-data-does-clearview-

its database of images and the accompanying facial recognition algorithm through contracts with federal, state, and local agencies, and private citizens.[50] Using scraped images, the facial recognition technology develops a biometric template for each face based on the unique facial geometry of each person.[51] These user images were scraped in violation of the terms of service of the respective platforms. [52] Search results on the platform return all scraped photos connected to that biometric template with links to sites.[53] As such, the search results can reveal every piece of information about a person that a person knowingly publishes, or what others have published about them. As law enforcement officials deploy Clearview's algorithm in criminal investigations, the sensitive images are incorporated into the dataset.[54]

This technology plays a larger role in law enforcement investigatory practices. Until recently, major technology companies abstained from combining these technologies over concerns of privacy and abuse.[55] But in early 2019, Indiana State Police searched a smartphone video of a shooting in a public park against Clearview AI's database and instantly matched the shooter to social media images with links to Venmo, Facebook, Twitter, and LinkedIn profiles.[56] In 2020, thousands of law enforcement departments use that or similar technology.[57] In light of this widespread use and the racial biases inherent in this technology, it is no wonder that reports of wrongful arrests at the hands of facial recognition have begun to surface.[58]

---

gather-people-answer-sadly-will-not-surprise-you.shtml [https://perma.cc/VS6P-5ZB6].

50. Ryan Mac, Carolina Haskins, & Logan McDonald, *Clearview AI Once Told Cops to "Run Wild" With its Facial Recognition Tool*, BUZZFEED NEWS (Jan. 28, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-cops-run-wild-facial-recognition-lawsuits [https://perma.cc/C7WA-HJPP].

51. Jake Goldenfein, *Australian Police are Using the Clearview AI Facial Recognition System with No Accountability*, THE CONVERSATION (Mar. 3, 2020), http://theconversation.com/australian-police-are-using-the-clearview-ai-facial-recognition-system-with-no-accountability-132667 [https://perma.cc/BK7M-25ZT].

52. Aaron Mak, *Clearview's Terrifying Facial Recognition Can't Go Back in the Bottle*, SLATE (Feb. 6, 2020), https://slate.com/technology/2020/02/youtube-linkedin-and-others-serve-clearview-ai-with-cease-and-desist-letters.html [https://perma.cc/U85Y-YYMK].

53. Hill, *supra* note 43.

54. *Id.*

55. Kashmir Hill, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, N.Y. TIMES (Jan. 22, 2020), https://www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html [https://perma.cc/B5JM-ZK56].

56. Hill, *supra* note 43.

57. Ryan Mac, Carolina 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), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement [https://perma.cc/5R5Y-QF8C].

58. Kashmir Hill, *Facial Recognition Led to Black Man's Arrest. It was Wrong.*, N.Y. TIMES, June 25, 2020, at A1.

Illinois, Texas, and Washington regulated biometric data collection through legislation prior to the United States Supreme Court decision in *Carpenter* and reporting of Clearview AI's capabilities. Illinois passed the Biometric Information Privacy Act out of concern over the inherent permanence of biometric features.[59] The Illinois statute prohibits private companies from collecting biometric information without user consent.[60] Similarly, Washington requires notice and consent of the user before any biometric data is collected for a commercial purpose.[61] Texas requires the same.[62] Federal law relies on the 1986 Stored Communications Act to generally regulate electronic communication records.[63] Under that law, a federal court only needs to find facts showing a reasonable ground to believe that the content of digital communications is relevant to a criminal investigation.[64]

As facial recognition and biometric algorithms become more sophisticated, and social media further ingrains itself into societal fabric, Fourth Amendment jurisprudence has slowly recognized the privacy implications of digital surveillance. The important focus on the principles underlying Fourth Amendment protections implicates privacy concerns related to emerging digital surveillance technology. The willingness of the Supreme Court to incorporate modern technology into its Constitutional doctrine has led to incongruous and winding results. Part II explores those results.

II. FOURTH AMENDMENT JURISPRUDENCE

The Fourth Amendment prohibits "unreasonable searches and seizures" of "persons, houses, papers, and effects."[65] American jurisprudence delineates between searches and non-searches as a gatekeeping function for that Constitutional right. This Part examines the application of Fourth Amendment protections to surveillance technology by the United States Supreme Court. First, this Part outlines the limitations placed on Fourth Amendment protections when a person knowingly exposes information to a third-party. Next, this Part surveys

59. 740 ILL. COMP. STAT. 14 / 5 (2018).

60. Matthew Kulger, *Does It Hurt You if Your Face is Tracked by Technology?*, CHI. TRIB., Nov. 28, 2018, at C18.

61. WASH. REV. CODE § 19.375.020 (2019).

62. *See* TEX. BUS. & COM. CODE ANN. § 503 (West 2019).

63. *See* 18 U.S.C. § 2703.

64. 18 U.S.C. § 2703(d).

65. 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, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

the line of Supreme Court cases that limit Fourth Amendment protections when a person knowingly exposes a fact to the public. Finally, this Part examines the evolution of Fourth Amendment privacy interests in the digital age, culminating in a recent watershed opinion in *United States v. Carpenter*.

In *Katz v. United States*, the Court explained Fourth Amendment protections govern "people, not places."[66] Justice Harlan's concurrence to the majority opinion set forth two threshold requirements for Fourth Amendment searches: first, whether an individual had a subjective expectation of privacy; and second, whether there was a societal objective expectation of privacy.[67] In *Katz*, the Court concluded that stereophonic tape recorders attached to a phone booth to eavesdrop on Charlie Katz's phone calls constituted a search within the meaning of the Fourth Amendment.[68] That conclusion rested on the "vital role" of public telephones within society and acknowledged the shifting societal norms predicated on entrenched technology.[69] But Fourth Amendment protections were considered inapplicable to information that a person "knowingly exposes to the public."[70]

A. Knowing Exposure to Third Parties

The United States Supreme Court has adopted a categorical exception to Fourth Amendment protections when a person reveals information to the public under the "third-party doctrine." According to the third-party doctrine, American citizens have no legitimate expectation of privacy in information willingly exposed.[71] As a result, law enforcement agencies

66. Katz v. United States, 389 U.S. 347, 351 (1967). In a prior decision, the Supreme Court narrowed Fourth Amendment protections to "material things" based on the plain language of the amendment and held police wiretapping outside was not a search within the Court's understanding. Olmstead v. United States, 277 U.S. 438, 464 (1928) ("The Amendment itself shows that the search is to be of material things -- the person, the house, his papers or his effects.").

67. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("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.").

68. *Id*. at 353. One significant aspect of Katz is the Court's departure from its Fourth Amendment surveillance precedent. Katz departed from the "eroded underpinnings" of Olmstead v. United States and Goldman v. United States, Fourth Amendment cases controlled by the trespass doctrine.

69. *Id*.at 352.

70. *Id*. at 351. That same year, the Court struck down New York's permissive eaves dropping statute as a violation of the Fourth Amendment in Berger v. New York. Berger v. New York, 388 U.S. 41, 44 (1967). In Berger, the Court recognized the fervor of the law enforcement community, which considered telephone surveillance "the most important technique of law enforcement." *Id*. at 60.

71. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979) ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.").

acquiring information known to an informant or held by a business is considered "not a search" in the eyes of Fourth Amendment jurisprudence.[72] While this doctrine grew out of government use of confidential informants, police technology has created an amorphous doctrine with contradictory rulings.[73] According to Professor Richard Uviller, the Court's interpretation of privacy expectation hinges on the degrees of awareness on the part of the surveilled and that the invisible agent in *Katz* is wholly distinct from the "visible" undercover agent.[74]

Similarly, the Court in *Smith v. Maryland* found no Fourth Amendment search when police installed a pen register in a telephone company's central office to record the numbers dialed by defendant Michael Lee Smith.[75] Under the guise of the defendant "assuming the risk" of information voluntarily turned over to third-parties and the "limited capabilities" of the recording technology, the Court found no reasonable expectation of privacy in the telephone numbers that Americans dial.[76]

Dissenters and legal scholars have questioned the underlying premise and societal expectations promulgated under the third-party doctrine.[77] Professor Sherry Colb questioned the "knowingly exposed" element of the third-party doctrine when the government "deliberately manipulates

72. *See* United States v. Miller, 425 U.S. 435 (1976).

73. *See* United States v. White, 401 U.S. 745, 747 (1971) ("On four occasions the conversations took place in Jackson's home; each of these conversations was overheard by an agent concealed in a kitchen closet with Jackson's consent and by a second agent outside the house using a radio receiver. Four other conversations -- one in respondent's home, one in a restaurant, and two in Jackson's car -- were overheard by the use of radio equipment.").

74. H. Richard Uviller, *Evidence From The Mind of the Criminal Suspect: A Reconsideration of the Current Rules of Access and Restraint*, 87 COLUM. L. REV. 1137, 1151 (1987) ("The law treats secret surveillance of speech or other behavior largely according to whether the surveilling agent is visible or invisible to the subject. An agent, visibly present though masquerading, is thought to gather evidence in a fundamentally different manner than a concealed agent or a hidden electronic device. The theory is that the contents of the mind, deliberately revealed to another person, are willingly shared, while the secret eye or ear, possibly electronically enhanced, bypasses constitutional concern to spirit the evidence away.").

75. *Smith*, 442 U.S. at 745-46 (finding "no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not "legitimate." The installation and use of a pen register, consequently, was not a "search," and no warrant was required.").

76. *Id*. at 742 ("we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.").

77. *Id*. at 750 (Marshall, J., dissenting). In *Smith v. Maryland*, Justice Marshall disagreed on two principles. First, inherent in participation in modern society is the practical necessity of modern communication, that necessity forces members of society into the risk of disclosure. Second, Justice Marshall framed the assumption of risk on what privacy expectation should be held in light of a "free and open society" and cautioned that "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance." *Id.*

reality to create relationships for the sole purpose of betrayal."[78] Some scholars see the Court's third-party doctrine as permitting government intrusion into homes and lives through "a legion of spies," while, at the same time, decrying state agents who walk into our homes and rifle through our drawers.[79]

B. Knowing Exposure to the Public

What a government agent observes in public is presumptively not a search and is not protected by the Fourth Amendment.[80] The Court is reluctant to force "law enforcement officers to shield their eyes" in public.[81] Because a person exposes information, that person has no reasonable expectation of privacy. Yet again, technology forces the Court to contort the boundaries of what is and is not a search of a person's public activities. Two cases illustrate the slight distinctions that lead to incongruous Fourth Amendment protections: *United States v. Knotts* and *United States v. Karo.*

In *Knotts*, police officers installed a beeper in a drum of chloroform that they believed Leroy Knotts and Darryl Petschen would use to manufacture amphetamines.[82] Officers then tracked the beeper's signal by car and helicopter as Petschun drove the chloroform drum and beeper to a cabin where, after obtaining a search warrant, police discovered an amphetamine laboratory.[83] The Court analyzed the surveillance by removing the technology from the equation. First, the Court equated the use of the beeper to police following a car on public streets and highways.[84] As a result, the Court found no reasonable expectation of privacy in a person's movements because that information is voluntarily conveyed to "anyone who wanted to look."[85] Then, the Court acknowledged the beeper but disregarded its role, reasoning that the Fourth Amendment does not prohibit police from using sensory augmented technology, finding support in a 1927 decision involving a flashlight.[86]

One year later, in *United States v. Karo*, the Court ruled that police use

78. Sherry F. Colb, *What is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN L. REV 119, 141 (2003).

79. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 365 (1974).

80. *See generally* United States v. Dunn, 480 U.S. 294 (1987).

81. California v. Ciraolo, 476 U.S. 207, 213 (1986).

82. United States v. Knotts, 662 F.2d 515, 516 (8th Cir.1981).

83. United States v. Knotts, 460 U.S. 276, 279 (1983).

84. *Id*. at 281.

85. *Id*.

86. *Id*. at 282 (quoting United States v. Lee, 274 U.S. 559 (1927)).

of a beeper to monitor a suspect's movements through a home was unconstitutional.[87] In contrast to *Knotts*, the Court held the surveillance violated the reasonable expectation of privacy and infringed on the defendant's Fourth Amendment rights.[88] The Court distinguished its decision on grounds that the beeper was monitored within the house and revealed "a critical fact about the interior of the premises."[89] The Court honed in on the fact that the record in *Knotts* was unclear about whether the beeper was monitored inside the cabin, whereas in *Karo* the police conceded that they monitored the beeper in the interior of the home.[90]

C. Adjudicating Privacy in the Digital Age: Kyllo, Jones, then Carpenter

In a series of police-technology search cases, the Court acknowledged the awkward fit between Fourth Amendment precedent and technology. First, in *Kyllo v. United States* the Court considered the constitutionality of government agents conducting warrantless thermal scans of homes with a thermal imager.[91] Thermal scans of the exterior of a suspect's apartment detected heat emanating from halide lights to grow marijuana.[92] The Court of Appeals for the Ninth Circuit concluded there was no Fourth Amendment violation for two reasons: there was no subjective expectation of privacy in the heat emanating from a home and there was no objective expectation of privacy in the hot spots on the roof and wall of the home.[93]

The Supreme Court disagreed that the thermal imaging was a non-invasive scan of the exterior of the house.[94] Instead, the Court's holding was premised on the "sophisticated systems that are already in use or in development" that, if left unregulated, would hold citizens at the mercy of advancing technology.[95] Next, the Court refused to hinge a rule on whether or not the surveillance would access "intimate" details due the evolving nature of technology.[96] But that same technology employed within a suspect's home mandated a bright and firm line, that technology not in the public use implemented to reveal information about the home

87. United States v. Karo, 468 U.S. 709 (1984).
88. See *id.* at 716.
89. *Id*. at 715.
90. *Id*. at 714.
91. Kyllo v. United States, 553 U.S. 27, 29 (2001).
92. *Id*. at 30.
93. United States v. Kyllo, 190 F.3d 1041, 1047 (9th Cir.1999).
94. *Kyllo*, 553 U.S. at 35.
95. *Id*. at 36.
96. *Id*. at 39.

is a search that requires warrant.[97]

Then, in *United States v. Jones* the Court revisited the privacy implications of Global Positioning System (GPS) tracking devices on a suspect's car. In *Jones,* police installed a device on the undercarriage of Antoine Jones' jeep, which resulted in 2,000 pages of data from four weeks of surveillance.[98] The *Jones* majority opinion returned to a historical trespass analysis and held the physical installation of the device was a trespass, and therefore, a Fourth Amendment violation.[99]

In the concurrences, a new understanding for Fourth Amendment rights in the digital era emerged. In his concurring opinion, Justice Alito noted the impossibility of an eighteenth century analogue to the installation of the GPS tracker and rebuked the reliance on eighteenth century tort law to analyze twenty-first century Fourth Amendment issues.[100] Instead, his concurrence focused on long-term surveillance and the current landscape of technologies that facilitate long-term surveillance.[101] Furthermore, technology has erased most, if not all, practical limitations on long-term surveillance.[102] While claiming the legislature as the proper body to ensure the protections of privacy rights, he found a reasonable expectation of privacy under *Katz* in long-term monitoring and cataloguing of public movements.[103]

Justice Sotomayor also signaled the need for a new Fourth Amendment doctrine in light of the emerging technological capabilities of the government. In her concurring opinion, she noted that the questions surrounding reasonable expectations of privacy hinge on whether citizens reasonably expect the government to collect and store data that implicates the private details of their lives.[104] While GPS data was the central theme of her concurrence, focusing on the collection of "aggregate data" implicates the multitude of devices and technologies referenced in Justice

97. *Id.* at 40.

98. United States v. Jones, 565 U.S. 400, 403 (2012).

99. *Id.* at 405.

100. *Id.* at 418 (Alito, J., concurring) ("is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner?").

101. *Id.* at 428 (Alito, J., concurring) ("In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen. Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users--and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States.").

102. *Id.* at 430 (Alito, J., concurring).

103. *Id.* at 431 (Alito, J., concurring).

104. *Id.* at 416 (Sotomayor, J., concurring).

Alito's concurrence.[105] Finally, Justice Sotomayor questioned the propriety of the third-party doctrine in the digital age as "people reveal a great deal of information about themselves to third parties" while carrying out unremarkable tasks.[106] While she concurred in the judgement, she urged the Court to decouple privacy from secrecy, and cautioned that all public actions should not forfeit an underlying privacy right.[107]

1. Carpenter v. United States: Privacy and Digital Monitoring of the Whole of our Movements

The Court grappled with the very issues raised by the *Jones* concurrences in *Carpenter v. United States*—specifically, long-term data collection tracking a person's every movement.[108] In *Carpenter*, police accessed over 130 days' worth of cell-site location information (CSLI) data[109] from Timothy Carpenter's cell phone provider, equaling roughly 13,000 location points to track him.[110] Writing for the Majority, Justice Roberts attempted to redefine the "reasonable expectation of privacy" in the digital age without complete abandonment of Fourth Amendment precedent. Adopting Justice Alito's language of surreptitious monitoring and Justice Sotomayor's long-term data collection concerns in their respective *Jones* concurrences, Justice Roberts concluded that the use of historic CSLI data to track Carpenter violated the "reasonable expectation [of privacy] in the whole of his physical movements."[111]

Despite framing *Carpenter* as a narrow holding, the decision may have broad implications. While the Court refused to explicitly overrule the third-party doctrine of *Smith v. Maryland* and *United States v. Miller*, the *Carpenter* opinion disqualified that doctrine from the "novel circumstances" of CSLI data, concluding that third-party disclosure does not preclude Fourth Amendment protections.[112] Given the widespread use of cell phones in the United States and the "seismic shifts in digital technology" that make detailed chronicles of a person's physical presence

105. *Id*. (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.").

106. *Id*. at 418 (Sotomayor, J., concurring).

107. *Id*. at 417 (Sotomayor, J., concurring).

108. *See* Carpenter v. United States, 138 S. Ct. 2206, 2211 (2019).

109. *See id.* ("Most modern devices, such as smart phones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI).").

110. *Id*. at 2212.

111. *Id*. at 2219.

112. *Id*. at 2217.

over the course of years, the Court reasoned that there was a "world of difference" between CSLI data and the seemingly primitive technology in *Smith.*[113]

2. *Carpenter*'s Aftermath

In the wake of *Carpenter*, several lower federal courts have extended Fourth Amendment protections beyond historic CSLI data.[114] One district court within the Tenth Circuit relied on *Carpenter* to find a reasonable expectation of privacy in a generally public Facebook account.[115] The court considered a warrant granting access to the entire Facebook profile overbroad due to the pervasive nature of the data the account would reveal. Finally, the court compared a search of the entire Facebook account to a general warrant for rummaging through the entirety of a person's electronic belongings.[116]

Likewise, a Fourth Circuit district court extended the reasoning in *Carpenter* to find a reasonable expectation of privacy in non-public Facebook content.[117] The court likened social media posts to sealed packages and private calls entrusted to an intermediary to deliver the information and found the third-party doctrine inapplicable.[118] According to the court, recognizing the manner in which technology enables the government's ability to encroach on private areas in our lives requires protection of social media accounts due to the intimate, momentous, and weighty information conveyed through those sites.[119] However, even in the aftermath of *Carpenter*, some lower courts dismiss the notion of any reasonable expectation of privacy in social media posts.[120]

In 2019, the Ninth Circuit relied on *Carpenter* to determine whether biometric data collection for facial recognition technology harmed social media users' privacy rights.[121] Facebook's facial recognition software employs biometric face templates to identify users from the millions of photos uploaded to Facebook for photo and location tagging.[122] The court

113. *Id*. at 2219-20.

114. *See generally* United States v. Diggs, 385 F. Supp. 3d 648 (N.D. Ill. 2019) (extending *Carpenter* to GPS data that tracked the defendant's movements over the course of a month).

115. United States v. Irving, 347 F. Supp. 3d 615, 621 (D. Kan. 2018).

116. *Id*. at 624.

117. United States v. Chavez, 423 F. Supp. 3d 194, 202 (W.D. N.C. 2019).

118. *Id*. at 203.

119. *Id.*

120. Ward v. City of Hobbs, 398 F. Supp. 3d 991, 1073 (N.M. 2019) ("regardless of what the Supreme Court decides to do with social media on the internet, only the most ignorant or gullible think that what they post on the internet is or remains private.").

121. Patel v. Facebook, Inc., 932 F.3d 1264, 1273 (9th Cir. 2019).

122. *Id.*

concluded that biometric privacy rights are akin to the rights protected in *Carpenter* due to the "detailed, encyclopedic, and effortlessly compiled" nature of the information revealed by facial recognition technology.[123] The court considered future development and application of the technology, cautioning against facial recognition scans of real-time surveillance data and biometric templates being used to unlock password protected phones through the facial recognition lock.[124]

Similarly, a district court within the Ninth Circuit relied on *Carpenter* to find that the use of biometric face scans of a suspect to access his smart phone violated the Fifth Amendment.[125] The court differentiated biometric data from fingerprinting and DNA swabs because of the manner of identification and access to a database of a person's most intimate information.[126]

Focusing on the nature of the data, some federal courts have shown a willingness to extend Fourth Amendment protections to information that is encyclopedic and intimate. Furthermore, these cases demonstrate the looming issues in the aftermath of *Carpenter*. These cases also demonstrate the degree to which courts are confronting policing technology and the privacy implications implicit in Clearview AI's platform. With *Carpenter* as a guidepost courts will need to address the tension between Fourth Amendment privacy expectations and access to databases like Clearview AI's.

III. EXTENDING THE FOURTH AMENDMENT

The preceding Parts of this Comment highlighted the questions and challenges that courts will face regarding biometric privacy rights and the Fourth Amendment in the wake of *Carpenter*. On one hand, *Carpenter* cabined its holding as a narrow decision.[127] On the other hand, the lower courts are already extending *Carpenter* to novel circumstances. In the meantime, national attention has focused on the digital privacy rights implicated by a multi-billion image database harvested from social media sites that are practically inseparable from modern life.

Answering those questions requires an application of the guideposts set forth in *Carpenter*. First, this Part applies state use of facial recognition scans of biometric databases to the third-party doctrine as understood in *Carpenter*. It then turns on the subjective expectation of privacy in a person's biometric data. Finally, this Part identifies an objective

123. *Id*.

124. *Id*.

125. *See In re* The Search of a Residence in Oakland, 354 F. Supp. 3d 1010 (N.D. Cal. 2019).

126. *Id*. at 1016.

127. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

expectation of privacy in a person's biometric data as currently used in Clearview AI's database.

The Article concludes by arguing that Fourth Amendment prohibition on unreasonable searches should extend protection to an individual's biometric data as a natural extension of Supreme Court jurisprudence and as a matter of policy. Facial recognition scans of biometric data harvested by third-parties, as a modern surveillance technology, renders the third-party doctrine anachronistic. Like CSLI data, facial recognition scans of biometric data intrude into a sphere of privacy that merits protection through the Fourth Amendment's warrant requirement.[128]

A. Unreasonable: The Third-Party Doctrine

As a threshold matter, the third-party doctrine is particularly inappropriate in the context of facial recognition searches of biometric data due to the nature of an individual's biometric data. Fourth Amendment jurisprudence historically prohibits intrusions into the human body.[129] While the technology is predicated on the user images uploaded to social media platforms and internet sites, the scan and map of facial geometry is distinguishable from the user image itself.[130] The user image itself becomes ancillary as the technology extracts the facial features and formats them into a face print.[131] Just as the thermal scan of the house in *Kyllo* was not the same as officers on a public street observing a home with the naked eye, facial recognition searches of biometric databases are not naked-eye reviews of user photographs.[132]

Social media platforms predicated on user interactions and connectivity developed the capacity to map the biometric data of user images to enable user tags, suggest content, and target advertisements, among other functions.[133] Few could have imagined a society in which a person's daily life and intimate relationships are indexed and searchable in the matter of seconds in 2009, let alone in 1979 when *Smith* and *Miller* articulated the third-party doctrine.[134] But the unimaginable became

128. *Id.* at 2213.

129. *See* Schmerber v. California, 384 U.S. 757, 769-70 (1966) ("[With respect to searches involving intrusions beyond the body's surface[, t]he interests in human dignity and privacy which the Fourth Amendment protects forbid any intrusions on the mere chance that desired evidence might be obtained.").

130. *See infra* pp. 5-6.

131. U.S. GOV'T ACCOUNTABILITY OFFICE, FBI FACIAL RECOGNITION TECHNOLOGY, GAO-16-267 6 n.14 (2016).

132. Kyllo v. United States, 533 U.S. 27, 33 (2001).

133. Joaquin Quinero Candela, *Managing Your Identity on Facebook With Face Recognition Technology*, FACEBOOK (Dec. 19, 2017), https://about.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology [https://perma.cc/7G6M-R2FU].

134. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("After all, when Smith was

reality due to the rise of social media and rapid developments in facial recognition technology.[135]

What's more, voluntary exposure is inapplicable to biometric face prints because, like the CSLI in *Carpenter*, that data is not truly "shared" as the term is normally understood.[136] The biometric data used by Clearview AI was never "voluntarily conveyed" to them in any sense—it was web-scraped.[137] Clearview AI's situation is wholly distinct from *Miller*, where a company voluntarily conveyed information to the government.[138] Rather, social media platforms and other websites scraped by Clearview AI have actively sought to halt that practice.[139]

As an increasingly indispensable aspect of participation in society, social media and the internet are "pervasive and insistent part[s] of daily life."[140] While most Americans understand the pervasive nature of data collection and commodification online, most feel they have little to no control over their personal data.[141] *Carpenter* recognized that user data increasingly stems from passive collection through the cell phone applications.[142] Moreover, individual users lack control over data stored on other user accounts.[143] Combined with web scraping, the permanence of data creates a digital paper trail left behind for algorithms to follow.

As such, the same principles underlying the *Carpenter* decision preclude application of the third-party doctrine to the biometric data upon which facial recognition algorithms rely.

---

decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements.").

135. *See infra* pp. 4-6.

136. *Carpenter*, 138 S.Ct. at 2210.

137. *See infra* pp 3 –5.

138. United States v. Miller, 425 U.S. 435, 443 (1976).

139. Mak, *supra* note 52.

140. *Carpenter*, 138 S.Ct. at 2219 (quoting Riley v. California, 573 U.S. 373, 283 (2014).

141. Brook Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kamar, & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information [https://perma.cc/72RW-97VQ].

142. Kim Komando, *You're Not Paranoid: Your Phone Really is Listening In*, USA TODAY (Dec. 19, 2019), https://www.usatoday.com/story/tech/columnist/2019/12/19/your-smartphone-mobile-device-may-recording-everything-you-say/4403829002/ [https://perma.cc/8936-TCMK]; *Carpenter*, 138 S. Ct. at 2220 ("Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates.").

143. Nicole Karlis, *You Just Deleted Facebook. Can You Trust Facebook to Delete Your Data?*, SALON (Feb. 11, 2019), https://www.salon.com/2019/02/10/you-just-deleted-facebook-can-you-trust-facebook-to-delete-your-data/ [https://perma.cc/P46K-TGLR].

B. Reasonable: Expectations of Biometric Privacy

The Fourth Amendment secures the right of the people to be "secure in their persons." This constrains unjustified bodily intrusions on the mere chance evidence might be obtained.[144] And courts have long recognized that the collection and analysis of biological samples is a search under the Fourth Amendment.[145] State use of biometric databases like Clearview AI's intrude beyond the skin to measure and map the human body based on biological characteristics.[146] Fingerprinting and buccal swabs of suspects have been upheld in the context of custodial booking procedures, but in the context of a for-profit biometric database of web-scraped images, the inherent government interest in booking procedures is inapplicable.[147]

Nor does this technology fall within the category of searches that are reasonable due to the "minimal intrusion." Admittedly, biometric mapping of a photograph is far less physically invasive than, for example, compelled surgery; but a person's individual dignitary interests in personal privacy are nonetheless implicated.[148] Yet, the ease at which the Clearview AI database was created implicates fundamental privacy and security concerns, particularly because of the surreptitious nature of the image collection and the absence of any mechanism to give or withdraw consent.

Unlike fingerprinting, facial recognition searches of biometric databases probe into the individual's private life and thoughts.[149] Within seconds of uploading an image, the technology can identify a person, reveal which social media accounts that person is on, and provide access to a catalogue of images of that person along with links to web addresses where they appeared.[150] Given the intimate nature of social media use and the ubiquity of social media in society, that catalogue can potentially provide a pictorial timeline for the user. One Facebook user's data alone

144. Schmerber v. California, 384 U.S. 757, 767–68 (1966).

145. *See* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 618 (1989).

146. U.S. GOV'T ACCOUNTABILITY OFFICE, FBI FACIAL RECOGNITION TECHNOLOGY, GAO-16-267 5 (2016).

147. *See generally* Maryland v. King, 569 U.S. 435 (2013).

148. Winston v. Lee, 470 U.S. 753, 761 (1985).

149. United States v. Davis, 394 U.S. 721, 727 (1969) ("[F]ingerprinting may constitute a much less serious intrusion upon personal security than other types of police searches and detentions. Fingerprinting involves none of the probing into an individuals private life and thoughts that marks an interrogation or search."); *See also* Missouri v. McNeely, 569 U.S. 141, 148 (2013) citing Winston v. Lee, 470 U.S. 753, 760 (1985) ("[A]n invasion of bodily integrity implicates an individual's 'most personal and deep-rooted expectations of privacy.'").

150. Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, (Mar. 5, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html [https://perma.cc/2J4M-8JFD].

is the equivalent of 400,000 pages of Microsoft Word documents.[151] That data can include a person's historic location, social, political, and biographical information. Even before *Carpenter*, the Sixth Circuit found a reasonable expectation that emails would be shielded from outside scrutiny because of the "sensitive and sometimes damning substance" of emails, which implies an expectation that emails are private and not public.[152]

This technology necessarily implicates broad privacy interests that society has deemed reasonable. As the courts in the Ninth Circuit have explained, a person's biometric data is detailed, encyclopedic, and effortlessly compiled.[153] The capability of Clearview AI's facial recognition scans of a person's biometric data implicates a person's history through the results of biometric queries. While the Supreme Court's caution surrounded the privacy implications of CSLI data chronicling an individual's physical movements, biometric data implicates intimate details of a person's life beyond their physical location or the heat radiating from their home.[154] As a whole, government access to a database of harvested images for the purposes of scanning the biometric faceprints defies society's expectation that law enforcement will not secretly monitor and catalog an individual's life.[155]

According to the Supreme Court, "the degree of community resentment aroused by particular practices is clearly relevant to an assessment of the quality of intrusion upon reasonable expectations of personal security."[156] In the very active and fervent debate surrounding Clearview AI's platform, multiple cities have banned the use of facial recognition and state legislative initiatives regulate this type of technology. New Jersey prohibited police use of the Clearview AI through the Attorney General's office.[157] In response to public awareness and opposition to the technology, some law enforcement agencies have banned its use altogether.[158] Cities like San Francisco, Oakland, and Somerville passed

151. Karlis, *supra* note 143.

152. *See* United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) (holding that a subscriber enjoys a reasonable expectation in the contents of emails stored, sent, or received through a commercial internet service provider).

153. *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1273 (9th Cir. 2019).

154. *See* Kyllo v. United States, 533 U.S. 27, 38 (2001); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

155. *Carpenter*,138 S.Ct. at 2217 (citing United States v. Jones, 565 U.S. 400, 430 (Alito, J. concurring in judgment)).

156. Terry v. Ohio, 392 U.S. 1, 14 n.11 (1968).

157. Samantha Malamed, *Police Tested Facial Recognition Program*, PHILA. INQUIRER, Mar. 6, 2020, at B1.

158. David Hernandez, *San Diego Police, DA Ban Use of Facial Recognition App—But Not Before it was Tested*, SAN DIEGO UNION-TRIBUNE (Mar. 16, 2020), https://www.sandiegouniontribune.com/news/public-safety/story/2020-03-16/san-diego-police-das-

ordinances in 2019 prohibiting the use of facial recognition and other surveillance technologies.[159] While those cities restrict the use of that technology, other cities like Chicago use it without any oversight, approval, or public input.[160] Furthermore, New York City police have defended the use of the technology as merely an investigative lead, but less than probable cause.[161] Other law enforcement officials acknowledge the need to regulate the practice, but reject outright prohibition due to public safety needs.[162]

On the federal side, two U.S. Senators probed Clearview AI over its practices while the House of Representatives held hearings on the impact of facial recognition technology on civil rights and liberties.[163] Those hearings demonstrated strong bipartisan support for transparency and accountability for the use of facial recognition technology in the U.S.[164]

Proponents of facial recognition technology defend its use as a research tool to identify perpetrators and victims of crimes, and argue that police should be able to use "every tool available" to find suspects and bring them to justice.[165] Yet even the most efficacious law enforcement practices are subject to constitutional scrutiny—"the enshrinement of constitutional rights necessarily takes certain policy choices off the table."[166] While the United States Supreme Court has disfavored bright-line rules, it has refused to leave reasonable expectations of privacy at the

office-tried-out-a-facial-recognition-app [https://perma.cc/E76K-8WDS].

159. *See* S.F., CAL., CODE § 19.B.2(d) (2019) (making it unlawful for any department to obtain, access, or use any facial recognition technology); OAKLAND, CAL., CODE § 964.045 (2019) (prohibiting Oakland employees to obtain, retain, request, access, or use facial recognition technology or information obtained from facial recognition technology); SOMERVILLE, MASS., ORDINANCE § 2019-16 (June 27, 2019) (prohibiting any Somerville official from obtaining, retaining, accessing, or using any facial recognition system or any information obtained from a facial recognition surveillance system).

160. Tom Schuba, *CPD Using Controversial Facial Recognition Program that Scans Billions of Photos from Facebook, Other Sites*, CHI. SUN-TIMES (Jan. 29, 2020), https://chicago.suntimes.com/crime/2020/1/29/21080729/clearview-ai-facial-recognition-chicago-police-cpd [https://perma.cc/E76K-8WDS].

161. Craig McCarthy, *NYPD Issues Policy on Facial Recognition Software After Nearly a Decade of Use*, N.Y. POST (Mar. 12, 2020), https://nypost.com/2020/03/12/nypd-issues-policy-on-facial-recognition-software-after-nearly-a-decade-of-use [https://perma.cc/55VX-NZQP].

162. DJ Pangburn, *San Diego's Massive 7-Year Experiment with Facial Recognition Technology Appears to be a Flop*, FAST COMPANY (Jan. 9, 2020), https://www.fastcompany.com/90440198/san-diegos-massive-7-year-experiment-with-facial-recognition-technology-appears-to-be-a-flop [https://perma.cc/T3SA-BLQY].

163. Ryan Mac, Caroline Haskins, & Logan McDonald, *Senators are Probing Clearview AI on the Use of Facial Recognition by Gulf States and International Markets*, BUZZFEED (Mar. 4, 2020), https://www.buzzfeednews.com/article/ryanmac/senators-markey-wyden-clearview-ai-facial-recognition [https://perma.cc/G3Q3-6LTY]; *See also Facial Recognition Technology: Ensuring Transparency in Government Use Before the H. Comm. On Oversight and Reform*, 116 Cong. (2019).

164. *Id*.

165. Schuba, *supra* note 160.

166. District of Columbia v. Heller, 554 U.S. 570, 636 (2008).

mercy of advancing police technology that would allow police to discern all human activity.[167] In those cases, it has drawn firm and bright lines that require a warrant for the use of particular surveillance methods.

Electronic privacy rights advocates urge a complete prohibition on the technology.[168] As it stands, there is not a single viable basis for monitoring unconstitutional biometric searches of individuals through facial recognition technology. As a matter of policy, concrete mechanisms protecting the constitutional right to privacy must deter abuse of this technology. At a minimum, before running a facial recognition search against a biometric database like Clearview AI's, law enforcement should follow the basic the Fourth Amendment directive: get a warrant.

IV. CONCLUSION

This account of Fourth Amendment jurisprudence shines a light on the constitutional tensions surrounding police use of facial recognition technology. The history illuminates the United States Supreme Court's tumultuous relationship with privacy rights in the surveillance age. The sophistication of policing technology has far outpaced the reasoning of the courts. As modern Fourth Amendment decisions illustrate, the Court has recently shown a willingness to reconsider ill-fitting precedent in light of modern surveillance technology. In the age of *Carpenter*, Fourth Amendment protections should extend to an individual's biometric data.

But perhaps the clearest lesson is how unclear Fourth Amendment protections are. The technology at the fingertips of Americans today, like the constitutional amendments that the technology implicates, is vexatious and intractable. There is no question that courts have tried to balance legitimate policing needs with constitutional protections. While the United States Supreme Court's decisions attempt to reflect the privacy expectations of the nation, in an important sense, its decisions have molded the expectations of law enforcement and civilians. The Court in *Carpenter* may have conditioned its holding as a "narrow one" to avoid disturbing both the past and the future.[169] But that decision did not make the question of Fourth Amendment protections in the digital surveillance era disappear. In fact, that question is now more urgent than ever. The digital age, the universality of social media, the more than three billion social media images scraped, the acceleration of facial recognition

167. Kyllo v. United States, 533 U.S. 27, 36 (2001).

168. *See* Jennifer Lynch, *Clearview AI-Yet Another Example of Why We Need a Ban on Law Enforcement Use of Face Recognition Now*, ELECTRONIC FRONTIER FOUNDATION (January 31, 2020), https://www.eff.org/deeplinks/2020/01/clearview-ai-yet-another-example-why-we-need-ban-law-enforcement-use-face [https://perma.cc/9EZP-G7TR].

169. Carpenter v. United States 138 S.Ct. 2206, 2220 (2018).

technology, and the onset of digital surveillance companies have only escalated the tensions of Fourth Amendment privacy expectations. If the courts hesitate, the damage may be irreparable.