Notes

THE FOURTH AMENDMENT LIMITS OF FACIAL RECOGNITION AT THE BORDER

EMMANUEL ABRAHAM PEREA JIMENEZ†

ABSTRACT

On any given day, hundreds of thousands of people enter the United States through ports of entry along the Mexican and Canadian borders. At the same time, the Department of Homeland Security ("DHS") seizes millions of dollars' worth of contraband entering the United States annually. Under the border-search exception, border officials can perform routine, warrantless searches for this contraband, based on no suspicion of a crime, without violating the Fourth Amendment. But as DHS integrates modern technology into its enforcement efforts, the question becomes how these tools fit into the border-search doctrine. Facial recognition technology ("FRT") is a prime example. To date, no court—and few legal scholars—have addressed how the Fourth Amendment would regulate the use of FRT at the border. This Note begins to fill that gap.

This Note contends that, after Carpenter v. United States*, the Fourth Amendment places at least some limits on the use of FRT at the border. Given the absence of caselaw, this Note uses a hypothetical border search to make three core claims. First—distinguishing between face verification and face identification—this Note argues that face identification constitutes a Fourth Amendment "search" only when the images displayed to a border official reveal "the privacies of life." Second, because of its invasive nature, this form of face identification is a nonroutine border search and is unconstitutional when conducted without reasonable suspicion. Lastly, this Note concludes that a border*

† Duke University School of Law, J.D. expected 2021; University of California at Davis, B.A. 2017. I would like to thank Professor Shane Stansbury for inspiring this Note topic, and Professor Lisa Kern Griffin for her invaluable guidance. Thank you as well to the editors of the *Duke Law Journal* for their incredible diligence in preparing this Note for publication. This Note is dedicated to my parents, Paulino and Juanita, who left their homes in Guanajuato, Mexico, so many years ago to come to this country.

official's reasonable suspicion must be linked to a crime that bears some nexus to the purposes underlying the border-search exception.

INTRODUCTION

At the San Ysidro Port of Entry, nearly one hundred thousand people cross the border into San Diego, California, on any given day.[1] Most will pass through primary inspection quickly and enter the United States without incident.[2] Some are referred to secondary inspection and remain at the border until a U.S. Customs and Border Protection ("CBP")[3] officer allows them to enter the country.[4] Regardless of how long they remain at the border, those travelers are being monitored. CBP's many surveillance towers, drones, and motion sensors are likely tracking their movements.[5] Devices known as "IMSI catchers" may be actively gathering their cell-site location information ("CSLI") and may even be collecting their text and voice messages too.[6]

In addition to these surveillance methods, facial recognition technology[7] ("FRT") is an emerging technology that will, once fully implemented, allow CBP to identify each traveler passing through San

1. *San Ysidro Land Port of Entry Fact Sheet*, GEN. SERVS. ADMIN., https://www.gsa.gov/cdnstatic/Overarching%20San%20Ysidro%20Fact%20Sheet%20-%20Dec%2011%202019.pdf [https://perma.cc/L2N9-7UGA] (last updated Dec. 11, 2019).

2. *See* RUTH ELLEN WASEM, JENNIFER LAKE, LISA SEGHETTI, JAMES MONKE & STEPHEN VIÑA, CONG. RSCH. SERV., RL32399, BORDER SECURITY: INSPECTIONS PRACTICES, POLICIES, AND ISSUES 10–11 (2005). All travelers entering the United States must present themselves to a Customs and Border Patrol ("CBP") officer for an initial, or "primary," inspection. *Id.* These inspections "usually last[] no longer than a minute." *Id.* at 10.

3. Not to be confused with the U.S. Border Patrol, which is a component agency of CBP, *see CBP Organization Chart*, U.S. CUSTOMS & BORDER PROT., https://www.cbp.gov/document/publications/cbp-organization-chart [https://perma.cc/M7CF-K95E], or U.S. Immigration and Customs Enforcement ("ICE"), which is a partner agency of CBP under the umbrella of the Department of Homeland Security ("DHS"), *see Operational and Support Component*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/operational-and-support-components [https://perma.cc/H6RH-HWKH].

4. If an officer suspects a traveler is inadmissible or otherwise violating the law, she may refer the traveler to a more extensive "secondary" inspection. WASEM ET AL., *supra* note 2, at 11. However, most travelers are not referred to secondary inspection. *Id.*

5. *See* Shirin Ghaffary, *The "Smarter" Wall: How Drones, Sensors, and AI Are Patrolling the Border*, VOX (Feb. 7, 2020, 8:01 PM), https://www.vox.com/recode/2019/5/16/18511583/smart-border-wall-drones-sensors-ai [https://perma.cc/V9UR-NRB2] ("Thousands of ground sensors are currently in use between ports of entry at the US border," along with drones, "a favored tool," and surveillance towers).

6. *Id*.

7. This Note uses variations of "facial recognition," such as "facial recognition technology" or "facial recognition systems," interchangeably.

Ysidro—and every other port of entry.[8] Facial recognition will also give CBP officers a window into the most private aspects of travelers' lives.[9] FRT identifies people through the automated analysis of a person's facial features.[10] And in recent years, it has become an increasingly common feature of modern life—from facilitating day-to-day tasks like unlocking cell phones[11] to making consequential decisions about who can enter the country.[12] The law enforcement benefits are clear.[13] But as with any new and powerful technology, so are its flaws and potential for abuse. FRT is often of questionable accuracy,[14] and in the wrong hands, it can be a potent tool for social repression.[15]

FRT also promises to stretch current constitutional doctrines as courts grapple with this rapidly evolving technology. In fact, courts are already confronting FRT-related issues in the context of the Fifth Amendment privilege against self-incrimination.[16] But so far, courts

---

8. *See infra* Part I.B.

9. *See infra* Part I.B.

10. *See infra* Part I.A.

11. *See* Jason Cipriani, *iPhone Face ID Is Pretty Cool. Here's How It Works and How To Use It*, CNET (Feb. 5, 2020, 3:00 AM), https://www.cnet.com/how-to/the-iphone-and-ipads-face-id-tech-is-pretty-darn-cool-heres-how-it-works-and-how-to-use-it [https://perma.cc/CB64-DNK9] ("When it launched Face ID in September 2017, Apple turned your close-up into the key that unlocks your iPhone. Since then, Apple has continued to expand the number and type of devices with Face ID . . . .").

12. *See infra* Part I.B.1.

13. *See, e.g.*, Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://nyti.ms/2NEbiJZ [https://perma.cc/S9LB-5G89] ("Federal and state law enforcement officers . . . had used [a facial recognition] app to help solve shoplifting, identity theft, credit card fraud, murder and child sexual exploitation cases."). Police departments across the country are using FRT systems, like Clearview AI, to identify suspects and solve crime. *See, e.g.*, *id.*

14. *See* CLARE GARVIE, ALVARO BEDOYA & JONATHAN FRANKLE, GEORGETOWN L. CTR. ON PRIV. & TECH., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 46–47 (2016) [hereinafter THE PERPETUAL LINE-UP], https://www.perpetuallineup.org [https://perma.cc/7BPC-PUBB] ("Compared to fingerprinting, state-of-the-art face recognition is far less reliable . . . ."). This is especially true when applied to people of color. Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://nyti.ms/3dAQA89 [https://perma.cc/N5X8-2ZXJ]. Issues related to the accuracy of FRT are beyond the scope of this Note.

15. *See* Chris Buckley & Paul Mozur, *How China Uses High-Tech Surveillance To Subdue Minorities*, N.Y. TIMES (May 22, 2019), https://nyti.ms/2HwEiRc [https://perma.cc/BMW6-55M3] (explaining the use of FRT to monitor and subdue minority populations in China).

16. *E.g.*, United States v. Wright, 431 F. Supp. 3d 1175, 1179 (D. Nev. 2020). These cases have typically involved the compelled unlocking of a smart phone using FRT. *See, e.g.*, *id.* (holding law enforcement violated the defendant's Fifth Amendment privilege against self-incrimination "when they forcibly unlocked his smartphone . . . by holding it up to his face").

have avoided directly addressing the Fourth Amendment search and seizure issues associated with FRT.[17] Yet, as the technology becomes a staple in law enforcement investigations, it is only a matter of time before courts address these issues head on. In anticipation of these challenges, scholars have devoted significant attention to FRT.[18] They largely focus on how the Fourth Amendment might regulate facial recognition in domestic law enforcement settings.[19] Very few scholars,[20] however, have addressed how the Fourth Amendment applies to FRT used at international borders,[21] where Fourth Amendment protections are often already diminished.[22]

---

17. *E.g.*, *id.* at 1186 n.6 ("[T]he Court need not, and does not, reach Defendant's Fourth Amendment argument as to the same issue."); United States v. Jackson, 19-CR-6026CJS, 2020 WL 810747, at *11 (W.D.N.Y. Feb. 19, 2020) (declining to reach the question of whether the Fourth Amendment permits compelled unlocking of a phone using FRT on the grounds that the evidence would have been inevitably discovered).

18. A Westlaw search of law reviews and journals for articles using the terms "facial recognition," "Fourth Amendment," and "search" recovered 242 pieces. Term Search in Secondary Sources, WESTLAW, https://1.next.westlaw.com (last visited Feb. 23, 2021) (in the search bar, type "'facial recognition,' and 'Fourth Amendment' and 'search'" and limit the Publication Type to "Law Reviews and Journals").

19. *See, e.g.*, Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 505–39 (2012) (exploring the Fourth Amendment considerations of FRT); Sabrina A. Lochner, Note, *Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans*, 55 ARIZ. L. REV. 201, 214–17 (2013) (arguing police use of FRT is not a search); Elizabeth Snyder, Note, *"Faceprints" and the Fourth Amendment: How the FBI Uses Facial Recognition To Conduct Unlawful Searches*, 68 SYRACUSE L. REV. 255, 260–70 (2018) (arguing the Federal Bureau of Investigation's ("FBI's") use of FRT is a search).

20. To date, the only scholar to have addressed this particular issue with any depth has been Professor Andrew Ferguson. In the context of a larger piece on the Fourth Amendment implications of FRT, Professor Ferguson briefly notes that the use of face verification at the border is most likely constitutional. *See* Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1205–07 (2021) (arguing that its use may be allowed given precise legislation). Similarly, Brandon Thompson, in a piece exploring the Fourth Amendment issues with DHS's biometric data collection system, briefly suggests the Fourth Amendment may limit the use of FRT at the border and proposes a legislative solution. Brandon R. Thompson, Note, *Homeland Advanced Recognition Technology (HART) Data Collection: Fourth Amendment Considerations & Suggested Statutory Alternatives*, 29 S. CAL. INTERDISC. L.J. 155, 170–71 (2019).

21. For purposes of this Note, the "border" means the physical border with either Mexico or Canada. How FRT might be regulated in near-the-border contexts, like roving stops, *see, e.g.*, United States v. Brignoni-Ponce, 422 U.S. 873, 884–85 (1975) (articulating circumstances under which U.S. Border Patrol officers may stop vehicles while on roving patrol), is beyond the scope of this Note.

22. United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985) (noting that the "expectation of privacy [is] less at the border than in the interior"). For example, searches that would be clearly unconstitutional if conducted without a warrant in the "interior" would pass

This Note is the first to comprehensively address how the Fourth Amendment might regulate facial recognition at the border. It argues that after the Supreme Court's decision in *Carpenter v. United States*,[23] the Fourth Amendment must offer some protection against the suspicionless use of FRT at the border. Drawing a distinction between two uses of FRT—face verification and face identification—this Note argues that the use of face identification at the border is a "search" implicating the Fourth Amendment only when the images displayed to an officer reveal "the privacies of life."[24] Because of the lack of caselaw applying the Fourth Amendment to FRT at the border,[25] this Note applies the existing border-search doctrine and argues that this form of face identification is particularly invasive and constitutes a nonroutine border search. As a nonroutine search, face identification—unlike mere verification—is unconstitutional without individualized, reasonable suspicion.[26] Further, reasonable suspicion must be tied to a crime that relates to the purposes underlying the border-search doctrine.[27]

This Note proceeds in five parts. Part I explains how FRT operates and how it is currently deployed at the border, and Part II outlines the Fourth Amendment doctrine defining "searches" after *Carpenter*. Part III then describes the border-search doctrine and the scope of Fourth

---

Fourth Amendment muster at the border. *Compare* United States v. Jones, 565 U.S. 400, 404 (2012) (holding the physical placement of a GPS tracker on a car is a search requiring a warrant), *with* United States v. Flores-Montano, 541 U.S. 149, 155–56 (2004) (permitting the removal of a gas tank without a warrant or individualized suspicion).

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

24. *See id.* at 2214 ("[T]he [Fourth] Amendment seeks to secure 'the privacies of life' against 'arbitrary power.'" (quoting Boyd v. United States, 116 U.S. 616, 630 (1886))).

25. A Westlaw search for cases using the terms "facial recognition," "Fourth Amendment," and "border" recovered only eight cases. Term Search in Secondary Sources, WESTLAW, https://1.next.westlaw.com (last visited Feb. 23, 2021) (in the search bar, search for All Federal Cases, type "'facial recognition,' and 'Fourth Amendment' and 'border'" and limit the results to those containing these precise terms). None of these cases explored whether the use of FRT at the border constitutes a search.

26. Individual suspicion is reasonable when there are "specific and articulable facts which, taken together with rational inferences from those facts," justify a search. Terry v. Ohio, 392 U.S. 1, 21 (1968). Probable cause is a higher standard. *See* Brinegar v. United States, 338 U.S. 160, 175–76 (1949) ("Probable cause exists where 'the facts and circumstances within [the officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that' an offense has been or is being committed." (alterations in original) (quoting Carroll v. United States, 267 U.S. 132, 162 (1925))).

27. *See infra* Part III.A.

Amendment protections available at the border. Next, Part IV poses a hypothetical border-search situation involving the use of FRT to frame the discussion of when, if at all, the use of FRT at the border constitutes a search. Finally, Part V argues that in certain circumstances, the suspicionless use of facial recognition at the border is an unreasonable search absent an officer having individualized, reasonable suspicion to justify it.

I. FACIAL RECOGNITION AT THE BORDER

The Fourth Amendment exists, in part, to "place obstacles in the way of a too permeating police surveillance."[28] Yet new technologies threaten to impose that very surveillance. To avoid leaving Fourth Amendment protections "at the mercy of advancing technology,"[29] as the Supreme Court has cautioned against, any application of the Fourth Amendment to new surveillance tools must begin with an understanding of that technology's capabilities. This Part describes how FRT operates. It then distinguishes between FRT's use for face verification and identification, and it concludes by discussing the technology's deployment at the border.

A. Introduction to Facial Recognition Technology

1. *How the Technology Works*. At its core, facial recognition is an automated form of biometrics that identifies a person based on his or her unique facial features.[30] The facial recognition process has three basic stages. First, during the collection and extraction stage, a computer algorithm scans an image to detect any human faces present in the frame.[31] Scans can occur in real time using an FRT-equipped camera or after the fact by scanning video footage and photographs captured in the past.[32] If the camera detects a face, the algorithm then

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

29. Kyllo v. United States, 533 U.S. 27, 35 (2001).

30. *Facial Recognition*, ELEC. FRONTIER FOUND. (last updated Oct. 24, 2017) [hereinafter EFF, *Facial Recognition*], https://www.eff.org/pages/face-recognition [https://perma.cc/2GL6-ZSXP]. Although each facial recognition system is different, FRT systems will typically plot virtual points on a person's face and measure the distance between features such as a person's eyes or the shape of a person's chin. *Id.*

31. THE PERPETUAL LINE-UP, *supra* note 14, at 9.

32. *See id.* at 10–12, 22 (noting that police can perform face identification "in real-time," when "[a] face recognition program extracts faces from live video feeds of one or more security

aligns the image, measures the distance between key facial features, and extracts those measurements to create a unique, numerical code known as a face template.[33]

Second, during the comparison and matching stage, facial-recognition software compares the extracted face template against other templates generated from known faces stored in a comparison database.[34] These databases are built by both governmental and private entities and are populated with images from governmental and commercial sources.[35] Third, after completing the comparison, the software returns a probabilistic "match" indicating who the software concludes is the person in the original image.[36] Depending on how a user adjusts the software's settings, the system will return the most likely matches—it will usually be just a few—or all matches that meet a predetermined confidence threshold.[37] Because the user can customize the search, what the matching process looks like in practice depends on how law enforcement is using FRT.

2. *How the Technology Is Used*. FRT has a variety of uses.[38] In general, these uses can be split into two groups: face verification and face identification.[39] Beginning with the former, the use of face verification is widespread and varies from unlocking smart phones to confirming someone's identity at the border.[40] Its purpose is to "confirm[] that a particular human face . . . matches a preset digital

---

cameras and continuously compares them," or after a stop or an arrest, when a "mug shot may be searched against the existing entries" in a database).

33. EFF, *Facial Recognition*, *supra* note 30.

34. *Id.*

35. *See* Hill, *supra* note 13. Governmental sources may, for example, include images from driver's license photos or criminal mugshot databases. *See* EFF, *Facial Recognition*, *supra* note 30 (describing the images contained in the FBI's image database). Private companies like Clearview AI may, on the other hand, collect images from social media sites through a process known as "scraping." Hill, *supra* note 13.

36. *See* EFF, *Facial Recognition*, *supra* note 30 ("Some face recognition systems, instead of positively identifying an unknown person, are designed to calculate a probability match score between the unknown person and specific face templates stored in the database. These systems will offer up several potential matches, ranked in order of likelihood . . . .").

37. For more information on the confidence thresholds used to generate matches, see *infra* notes 47–48 and accompanying text.

38. Ferguson, *supra* note 20, at 1112–13.

39. *See, e.g.*, THE PERPETUAL LINE-UP, *supra* note 14, at 10.

40. Ferguson, *supra* note 20, at 1113 & n.41.

image of that face."[41] Face verification can operate in a couple ways. For one, it can collect a person's face template *in real time* and compare it to a single image of that person.[42] It then produces a binary, yes-or-no response (a "one-to-one match") as to whether both images are the same person.[43] Alternatively, a user can submit a photo to the face-verification system to have it compared against a broader set of constrained pictures from sources like travel documents.[44]

Second, FRT can go beyond mere verification to be used for face *identification*. Such systems identify an unknown person by collecting his or her picture and "querying an entire gallery of images in a database to find an image similar to a submitted image."[45] Rather than return a simple one-to-one match, face-identification systems display a "candidate list" comprising all the images a system believes resemble the submitted image.[46] How many images the software returns depends on the confidence threshold set by the user.[47] For example, if a user sets a similarity score of seventy-five, then the system will return all images that have a 75 percent or greater likelihood of matching the person in the submitted image. Setting the score to ninety-nine will, of course, return fewer images.[48] Law enforcement officers typically use face-

41. *Id.* at 1113.

42. For example, a CBP official may verify a traveler's identity by comparing a single, real-time photo with the image on the travel document presented by the traveler. U.S. DEP'T OF HOMELAND SEC., DHS/CBP/PIA-056, PRIVACY IMPACT ASSESSMENT FOR THE TRAVELER VERIFICATION SERVICE 2, 33 (2018) [hereinafter TVS PRIVACY IMPACT], https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-january2020_0.pdf [https://perma.cc/CW7J-JE3Z] (describing how CBP compares "real-time photographs" against other face templates).

43. Ferguson, *supra* note 20, at 1114; U.S. DEP'T OF HOMELAND SEC., DHS/ICE/PIA-054, PRIVACY IMPACT ASSESSMENT FOR THE ICE USE OF FACIAL RECOGNITION SERVICES 3 (2020) [hereinafter ICE PRIVACY IMPACT], https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf [https://perma.cc/B5LA-GDWQ] (describing face verification as a one-to-one matching system).

44. *See* TVS PRIVACY IMPACT, *supra* note 42, at 4 (describing how TVS face verification compares the submitted photo against "photographs captured by CBP during previous entry inspection, photographs from U.S. passports and U.S. visas, and photographs from other DHS encounters"). Constrained images are pictures that have minimized the variables impacting accuracy such as "poses, expressions, lighting, and distances." ICE PRIVACY IMPACT, *supra* note 43, at 3. Unconstrained images are pictures that have not eliminated variables impacting image quality. *Id.* An example of an unconstrained image is the prototypical social media profile picture, which may be taken at an angle or include other people.

45. ICE PRIVACY IMPACT, *supra* note 43, at 3.

46. *Id.* at 4–5.

47. *Id.* at 4.

48. *See id.* (noting that a lower similarity score results in a larger number of images). This system is also found in the commercial context. Amazon's facial recognition system, known as

identification systems to identify suspects during criminal investigations.[49] Although face verification and identification operate similarly during collection and extraction, each raises distinct constitutional concerns during the comparison and matching process, as Parts IV and V discuss.

B. Facial Recognition at the Border

The deployment of FRT at the nation's borders comes primarily in two forms and largely maps onto the verification–identification distinction explained above. On one hand, CBP uses face verification to confirm the identities of people entering the United States through ports of entry. On the other hand, U.S. Immigration and Customs Enforcement ("ICE") uses face identification during criminal investigations both at and away from the border.

1. *Face Verification at Ports of Entry*. The Department of Homeland Security's ("DHS") Biometric Entry/Exit Program, known as the Traveler Verification Service ("TVS"), is the predominant use of FRT at the border.[50] First piloted in 2016, the TVS verifies the identities of travelers entering or exiting the United States.[51] And ultimately, the DHS aims to deploy face verification at all ports of entry—including air, sea, and land—under the auspices of agencies like CBP and the Transportation Security Administration ("TSA").[52]

The TVS collection and comparison process differs depending on the system's operational environment. These differences ultimately impact the kinds of images available to a border official evaluating a traveler's admissibility into the United States. For example, a person arriving by air will have her photograph taken at customs and compared against a "gallery of known identities, based on the

Rekognition, allows users to set the confidence threshold themselves. *See* AMAZON WEB SERVS., AMAZON REKOGNITION: DEVELOPER GUIDE 130 (2020), https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf#face-feature-differences [https://perma.cc/9BAS-9GV4].

49. EFF, *Facial Recognition*, *supra* note 30. One well-known example is that of Clearview AI. Hill, *supra* note 13.

50. *See* TVS PRIVACY IMPACT, *supra* note 42, at 4 ("CBP will use the TVS as its backend matching service for all biometric entry and exit operations that use facial recognition . . . .").

51. *Id.* at 1–2.

52. *See id.* at 45 ("CBP has been working with the Transportation Security Administration . . . to test the TVS process for verifying traveler identities using the TVS camera technology and matching services at the TSA security screening checkpoint." (footnote omitted)).

manifests for all incoming flights for that day."[53] If one is arriving by land in a personally owned vehicle, a photograph is taken of the driver as she approaches the border.[54] That image is compared against a gallery of recent travelers and images from travel documents.[55] Pedestrians, on the other hand, have their photograph taken as they approach the border and present their travel document to the CBP officer.[56] The officer then performs a one-to-one match to confirm the traveler's photograph matches what is on the travel document.[57]

If the TVS verifies the traveler's identity, then the traveler may enter or exit the United States, and the image is either immediately deleted or temporarily retained by DHS.[58] If the TVS fails to verify a traveler's identity, the individual may be subject to further inspection.[59] Current DHS policy gives *some* travelers the ability to opt out of TVS and choose a traditional, in-person inspection.[60]

2. *Face Identification During Criminal Investigations at the Border*. ICE currently uses face identification during criminal investigations conducted by its investigative arm, Homeland Security Investigations ("HSI").[61] Although it is authorized to operate away from the border,[62] HSI often conducts operations at the border in partnership with other agencies, like CBP.[63] ICE uses a variety of facial recognition services

53. *Id.* at 30.

54. *Id.* at 34 (describing how CBP "uses cameras at vehicle inbound lanes in order to take the facial images of vehicle occupants 'at speed' (under 20 mph) and biometrically match the new images against a TVS gallery of recent travelers").

55. *Id.*

56. *Id.* at 33.

57. *Id.*

58. *Id.* at 8–9.

59. *Id.* at 35.

60. *See id.* at 19–20. Currently, only U.S. citizens may opt out of a TVS scan. *See id.* at 20.

61. *See* ICE PRIVACY IMPACT, *supra* note 43, at 2, 5–6 ("HSI uses [facial recognition services'] many query functionalities to generate candidate lists to identify an unknown person or to locate a known person who may be using an alias or assumed identity. These requests are made in furtherance of ongoing investigations on a case-by-case basis." (footnote omitted)).

62. *See Domestic Operations*, U.S. IMMIGR. & CUSTOMS ENF'T, https://www.ice.gov/domestic-operations [https://perma.cc/B7AN-KKEH] (listing the cities where HSI operates domestically).

63. *See, e.g.*, United States v. Cano, 934 F.3d 1002, 1008 (9th Cir. 2019), *petition for cert. filed*, No. 20-1043 (U.S. Jan. 29, 2021) (describing how HSI agents supported a CBP investigation at the San Ysidro Port of Entry). HSI's authority to combat "cross-border criminal activity" empowers the agency to investigate crimes that are not necessarily restricted to the border. *See Homeland*

("FRS") from different vendors, like Clearview AI,[64] to identify unknown people.[65] The comparison databases underlying these FRSs pose significant privacy concerns because they give ICE agents access to a large number of images of people regardless of whether they have committed a crime or even crossed a border before.[66] Additionally, these images may reveal deeply personal information.

ICE's image-collection process is broader in some respects than that used by TVS. Rather than capturing photos in real time, ICE agents collect images from previously taken photographs or videos.[67] Sources include surveillance camera footage, social media websites, and images from seized digital devices.[68] Agents then submit these photos to an FRS for comparison against the particular FRS vendor's database in hopes of identifying the person in question.[69]

Which FRS vendor an ICE agent uses determines the number and kind of images the agent's search will return. If an agent submits an image to a federal-government FRS, the submitted image could be compared against millions of images drawn from government documents, such as passports and visas, images collected during FBI investigations, and national security watchlists.[70] ICE agents can also submit photos to FRSs operated by state and local law enforcement agencies to compare submitted photos against state DMV and criminal history records.[71] Finally, an agent can submit an image to commercial

---

Security Investigations, U.S. IMMIGR. & CUSTOMS ENF'T, https://www.ice.gov/hsi [https://perma.cc/M5FV-9SWG] (listing the crimes that HSI is authorized to investigate).

64. ICE PRIVACY IMPACT, *supra* note 43, at 17. In late 2020, Clearview AI signed a contract with ICE to provide "mission support" services to HSI's ongoing criminal investigations. Kim Lyons, *ICE Just Signed a Contract with Facial Recognition Company Clearview AI*, VERGE (Aug. 19, 2020, 3:19 PM), https://www.theverge.com/2020/8/14/21368930/clearview-ai-ice-contract-privacy-immigration [https://perma.cc/4BAM-VLAU].

65. ICE PRIVACY IMPACT, *supra* note 43, at 16–17. An ICE agent can use an FRS only when its use is "directly relevant to an investigation." *Id.* at 6.

66. For example, since 2018, ICE officials have run nearly one hundred face-identification searches of the Maryland driver's license database—which contains photos, addresses, and names of over seven million Maryland drivers—without state or court approval in an effort to identify undocumented immigrants. Drew Harwell & Erin Cox, *ICE Has Run Facial-Recognition Searches on Millions of Maryland Drivers*, WASH. POST (Feb. 26, 2020, 10:55 PM), https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers [https://perma.cc/CRP4-NY9T].

67. ICE PRIVACY IMPACT, *supra* note 43, at 6.

68. *Id.*

69. *See id.* at 9 (describing HSI's process for submitting photos to an FRS).

70. *Id.* at 13–16.

71. *Id.* at 12–13.

vendors—like Clearview AI—that "maintain their own repository of images collected from either their own processes or searches of open source systems."[72] These databases can contain countless unconstrained images pulled from an even wider range of sources like social media websites and CCTV camera footage.[73]

If the image submission returns a match, the FRS displays to the investigating agent a candidate list of all potentially similar images.[74] Again, because the agent can adjust the similarity score in the search's settings,[75] the number of images that populate the candidate list may be left to the agent's discretion.[76] If an image is collected from an open-source website, the FRS may display the source URL to the officer.[77] Taken together, an ICE agent can potentially access many images that both collectively and individually reveal private—possibly deeply personal—information unrelated to a criminal investigation.

Given the privacy concerns associated with face identification, ICE has implemented several safeguards designed to minimize its intrusive effects. ICE agents may submit photos only to FRS vendors that have been preapproved by HSI or the agent's supervisor, unless exigent circumstances warrant the service's immediate use.[78] Any approved FRS vendor that returns images containing multiple people must isolate and display only the matched individual's face.[79] Additionally, photos submitted to the FRS must be directly relevant to an ongoing HSI investigation,[80] but matches cannot be used to trigger law enforcement action on their own.[81] These agency safeguards are a step in the right direction because they limit unchecked intrusion into

72. *Id.* at 16–17.

73. *Id.* at 16; Madhumita Murgia, *Who's Using Your Face? The Ugly Truth About Facial Recognition*, FIN. TIMES (Sept. 18, 2019), https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e [https://perma.cc/8LCP-KRFR].

74. ICE PRIVACY IMPACT, *supra* note 43, at 9.

75. *See supra* notes 47–48 and accompanying text.

76. *Cf.* ICE PRIVACY IMPACT, *supra* note 43, at 4–5 (describing how the confidence levels set by the agent will influence the number of images returned).

77. *Id.* at 17.

78. *Id.* at 6–7. ICE protocols, however, do not specify what constitutes an "exigent circumstance."

79. *Id.* at 17.

80. *Id.* at 6.

81. *See id.* at 11 ("HSI agents are instructed that any vetted FRS candidate match must be further investigated by the HSI agent receiving the lead prior to ICE taking any enforcement action against an individual.").

personal privacy. But agency protocols, which are subject to change both over time and based on leadership, are no substitute for constitutional protections.[82] After all, "the Founders did not fight a revolution to gain the right to government agency protocols."[83] The Constitution must provide an independent limit on the conduct of government agents.[84] And one source for those potential constitutional limits is the Fourth Amendment.

II. FOURTH AMENDMENT SEARCH DOCTRINE

The Fourth Amendment protects people within the United States[85] against "unreasonable searches and seizures."[86] But if a government action is not a search (or seizure), then "the Fourth Amendment provides no protection *at all*."[87] So, the threshold inquiry is: Does the use of FRT at the border constitute a search?[88] If so, then as Part III details, a court must determine whether that search was reasonable.[89]

---

82. *See* Riley v. California, 573 U.S. 373, 398 (2014) (rejecting the government's assurances that it would develop internal protocols to address privacy concerns relating to cloud computing).

83. *Id.*

84. *See id.* at 398, 403 (holding that the Fourth Amendment required a warrant for a cell phone search, despite assurances from the government that agencies would "develop protocols to address" cloud computing issues).

85. The Court has typically applied the Fourth Amendment to searches of noncitizens at the border. *See, e.g.*, United States v. Montoya de Hernandez, 473 U.S. 531, 533, 539 (1985) ("Having presented herself at the border for admission, . . . respondent was entitled to be free from unreasonable search and seizure."). However, after *United States v. Verdugo-Urquidez*, the application of the Fourth Amendment to aliens who are in the United States, but who have not "developed substantial connections" to the United States, is an open question. 494 U.S. 259, 271–73 (1990); *see also* Karen Nelson Moore, *Aliens and the Constitution*, 88 N.Y.U. L. REV. 801, 840–42 (2013) ("Whether aliens located within U.S. territory must satisfy the substantial connections test, or whether something less is sufficient, remains unresolved.").

86. U.S. CONST. amend. IV.

87. BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 211 (2017); *see also* Smith v. Maryland, 442 U.S. 735, 740 (1979) (noting that "the application of the Fourth Amendment depends on whether the person invoking its protection can claim" a search occurred).

88. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213–14 (2018) (noting that Fourth Amendment protection rests upon the existence of a "search" and focusing the analysis on whether the use of a new technology constitutes an unreasonable search).

89. *See Montoya de Hernandez*, 473 U.S. at 537 ("The Fourth Amendment commands that searches and seizures be reasonable. What is reasonable depends upon all of the circumstances . . . .").

A search occurs, as the Court held in *Katz v. United States*,[90] when the government intrudes into an arena where a person has a reasonable expectation of privacy.[91] That test has both subjective and objective components.[92] Subjectively, a person must demonstrate an "actual expectation of privacy."[93] Objectively, that expectation must "be one that society is prepared to recognize as 'reasonable.'"[94] The "basic guideposts" of the Fourth Amendment—namely, shielding "the privacies of life [from] arbitrary power" and "plac[ing] obstacles in the way of a too permeating police surveillance"—enhance the scope of this right.[95] Common sense suggests that this framework would encompass a wide range of law enforcement activity.[96] But in practice, post-*Katz* caselaw has limited the scope of what constitutes a "search."[97] This Part begins by surveying the Fourth Amendment doctrines that, pre-*Carpenter*, restricted the scope of what constitutes a "search." It then discusses the Supreme Court's decision in *Carpenter*, how it has reshaped the "search" analysis, and how it impacts the constitutionality of FRT.

*A. Pre-*Carpenter *Limits on Reasonable Expectations of Privacy*

When there is no reasonable expectation of privacy, there is no Fourth Amendment "search." Prior to *Carpenter*, the Court's decisions established limiting principles constraining what could count as a reasonable expectation of privacy. Two in particular—activities and spaces visible to others and the third-party doctrine—posed challenges for classifying the use of FRT as a "search" for the purposes of the Fourth Amendment.

---

90. Katz v. United States, 389 U.S. 347 (1967).

91. *See id.* at 361 (Harlan, J., concurring) (reasoning that the scope of the Fourth Amendment is related to a place where one has a reasonable expectation of privacy).

92. *See id.* (stating a search occurs when the government intrudes on a subjective expectation of privacy "that society is prepared to recognize as 'reasonable'").

93. *Id.*

94. *Id.*

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

96. *See* FRIEDMAN, *supra* note 87, at 211 ("Common sense would seem to dictate that whenever the government comes snooping, that's a search.").

97. *See* CHRISTOPHER SLOBOGIN, GOVERNANCE STUD. AT BROOKINGS, IS THE FOURTH AMENDMENT RELEVANT IN A TECHNOLOGICAL AGE? 3–9 (2010), https://www.brookings.edu/wp-content/uploads/2016/06/1208_4th_amendment_slobogin.pdf [https://perma.cc/W7C2-9Y2U] (summarizing the three doctrines that, post-*Katz*, have limited the scope of what constitutes a Fourth Amendment search).

First, activities and spaces visible to others are not entitled to Fourth Amendment protection given that they are "knowingly expose[d] to the public."[98] Due to this principle, the Fourth Amendment typically does not protect from the mere observation of a person's physical characteristics, including one's facial features.[99] As a result, the Fourth Amendment offers fewer protections against law enforcement collection of biometrics by noninvasive means—like photography.[100] Like photographing a person, FRT might not amount to a search. The system takes a photo in real time or uses one submitted by a law enforcement officer for verification or identification. Yet to the contrary, some argue that FRT actually goes one step further. They argue that people have a reasonable expectation of privacy in identity while in public—that is, a privacy to remain relatively anonymous while in public spaces.[101] Because revealing a person's identity using FRT would violate that expectation, the argument goes, such use of FRT is arguably a search for the purposes of the Fourth Amendment.[102]

Relatedly, the Supreme Court has held that law enforcement's observation of one's public movements is not a search. For instance, in *United States v. Knotts*,[103] the Court held that the GPS tracking of a car was not a search because the vehicle's location on public roads was conveyed to the public.[104] Thus, to the extent FRT—like GPS—reveals one's location because the background of an unconstrained photo betrays where the photo was taken, the Fourth Amendment would have historically offered little protection. But even pre-*Carpenter*, this

98. *See Katz*, 389 U.S. at 351.

99. *See* 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.").

100. *See, e.g.*, *In re.* Search of [Redacted] Washington, D.C., 317 F. Supp. 3d 523, 531 (D.D.C. 2018) (collecting cases). Some commentators argue that facial recognition is simply another form of photography and, therefore, is not a search. *See, e.g.*, Lochner, *supra* note 19, at 214–17 ("[U]nder both the trespass test and *Katz* test, FRT is not likely to be a Fourth Amendment search.").

101. *See* Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1600–19 (2017) (arguing FRT infringes on one's reasonable expectation of privacy in identity while in public); *see also* Jeffrey M. Skopek, *Reasonable Expectations of Anonymity*, 101 VA. L. REV. 691, 725–61 (2015) (arguing for the Fourth Amendment significance of anonymity).

102. Hirose, *supra* note 101, at 1600.

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

104. *Id.* at 281–82.

conclusion was not inevitable. Indeed, in *United States v. Jones*,[105] Justice Sonia Sotomayor reasoned in a concurring opinion that with sufficient locational data, police might learn enough about a person's private life to make such surveillance a search.[106] Further, she suggested that due to technological advances, the Court would need to look more closely at what privacy means in the digital age.[107]

Second, under the third-party doctrine, information voluntarily conveyed to another is not entitled to an expectation of privacy.[108] The Court has explained that an individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the [g]overnment."[109] In practice, this doctrine empowered the government to freely access records held by third parties—such as banks and phone companies—without implicating the Fourth Amendment.[110] To the extent FRT relies on similar third-party information, the Fourth Amendment would have offered little protection. In short, pre-*Carpenter* caselaw limited the scope of what constituted a reasonable expectation of privacy so much that law enforcement use of FRT was arguably unregulated by the Fourth Amendment.

B. Carpenter *Searches*

Before 2018, the case for classifying the use of FRT as a search was difficult because of these limiting principles. However, the Court's landmark decision in *Carpenter* fundamentally altered this analysis.[111]

---

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

106. *See id.* at 415 (Sotomayor, J., concurring) (noting that GPS-monitoring can "generate[] 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" that should be relevant to the search analysis).

107. *See id.* at 417–18 (arguing that the third-party doctrine may be "ill suited to the digital age" where people disclose a "great deal" of personal information during even "mundane tasks").

108. *See* Smith v. Maryland, 442 U.S. 735, 744–45 (1979) (permitting the warrantless use of a pen register to record calling history); United States v. Miller, 425 U.S. 435, 443–45 (1976) (permitting the warrantless collection of bank records).

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

110. *See* SLOBOGIN, *supra* note 97, at 7–9 (detailing how the third-party doctrine permits the governmental collection of private, digital information "free and clear of Fourth Amendment constraints").

111. *See, e.g.*, ORIN S. KERR, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT (forthcoming in Oxford University Press) (manuscript at 1) [hereinafter KERR, *Implementing* Carpenter], https://papers.ssrn.com/abstract_id=3301257 [https://perma.cc/VG2S-PK7N] (discussing *Carpenter* as "embark[ing] on a new path" of Fourth Amendment

There, the Court examined whether government collection of CSLI held by a third party could, in some circumstances, constitute a search.[112]

Timothy Carpenter was suspected of being involved in a string of cell-phone-store robberies over a four-month period.[113] During the course of the investigation, the government sought a court order—based on less than probable cause—to compel the disclosure of more than five months of Carpenter's aggregated CSLI data.[114] After receiving 127 days of CSLI data, the government noticed, and ultimately argued at trial, "that Carpenter was right where the . . . robbery was at the exact time of the robbery."[115] He was convicted and sentenced to over one hundred years in prison.[116] On appeal, Carpenter argued that the government's warrantless collection of his CSLI violated the Fourth Amendment.[117]

The Court agreed that collecting aggregate data on Carpenter's location was a Fourth Amendment search.[118] Although *Carpenter*'s holding was narrow,[119] the decision's rationale marked an evolution in Fourth Amendment doctrine that—as courts are beginning to recognize—carries significant implications for the constitutionality of modern surveillance techniques.[120] A close reading of *Carpenter*

---

jurisprudence); Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J. F. 943, 943 (2019) (discussing how *Carpenter* limits the third-party doctrine); Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 358 (2019) (noting "*Carpenter* work[ed] a series of revolutions in Fourth Amendment law"); Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 206 (2018) (discussing *Carpenter*'s effect on the third-party doctrine).

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

113. *Id*. at 2212.

114. *Id.*

115. *Id.* at 2212–13 (quoting Joint Appendix at 131, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402), 2017 WL 3614549, at *131).

116. *Id.* at 2213.

117. *Id.*

118. *Id.* at 2219.

119. *Id.* at 2220.

120. For examples of the modern technologies being evaluated under the *Carpenter* framework, see generally United States v. Gratkowski, 964 F.3d 307, 311–13 (5th Cir. 2020) (considering *Carpenter*'s application to a collection of Bitcoin transactions but ultimately rejecting it); Leaders of a Beautiful Struggle v. Balt. Police Dep't, 456 F. Supp. 3d 699, 715–17 (D. Md.), *aff'd*, 979 F.3d 219, *reh'g en banc granted*, 831 Fed. App'x. 662 (4th Cir. 2020) (considering *Carpenter*'s application to advanced aerial surveillance); United States v. Carme, No. 19-10073-RGS, 2020 WL 3270877, at *4–5 (D. Mass. June 17, 2020) (considering *Carpenter*'s application to forensic deciphering of BitTorrent software but ultimately rejecting it); Commonwealth v.

highlights several key factors relevant to the Fourth Amendment analysis of governmental surveillance tools that access third-party records.[121] In particular, those factors include the sophistication of the technology in question and the absence of any meaningful disclosure to the third party collecting the data.

First, the impact of modern technology was central to *Carpenter*'s rationale and holding.[122] The CSLI data collected by the government was only available because of "seismic shifts in digital technology."[123] This technology, in turn, gave the government seamless—and nearly instantaneous—access to "an entirely different species" of information about individuals.[124] Before the digital age, the cost and logistical challenges associated with continuous physical surveillance made obtaining similar locational information nearly impossible.[125] But now, locational information like CSLI is captured continuously, is accurate, and does not require physical surveillance.[126] Importantly, because CSLI tracks a person's cell phone—which is frequently on one's person—CSLI gives law enforcement an even more comprehensive profile of a person's movements than tracking a vehicle would.[127] Given the novel concerns this raised, the Court could not easily extend prior precedents.[128] Thus, the use of digital surveillance technology that gives the government seamless access to a qualitatively and quantitatively different kind of record implicates *Carpenter*.[129]

McCarthy, 142 N.E.3d 1090, 1099–107 (Mass. 2020) (considering *Carpenter* in its analysis of automated license plate readers); State v. Muhammad, 451 P.3d 1060, 1071–74 (Wash. 2019) (applying *Carpenter* to real-time CSLI).

121. *See* KERR, *Implementing* Carpenter, *supra* note 111 (manuscript at 16–27) (discussing three components of a *Carpenter* search).

122. *Id.* at 16.

123. *Carpenter*, 138 S. Ct. at 2219.

124. *Id.* at 2222.

125. *Id.* at 2217.

126. *See id.* at 2217–19.

127. *See id.* at 2218–19 ("Only the few without cell phones could escape this tireless and absolute surveillance.").

128. *See id.* at 2222 ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents.").

129. *See id.* (noting that CSLI does not resemble traditional business records); *supra* note 120 (listing cases that adopt or distinguish the *Carpenter* analysis based on whether the technology was sufficiently modern or traditional); *see also* KERR, *Implementing* Carpenter, *supra* note 111 (manuscript at 16–19) (discussing *Carpenter* as limited to digital-age technology).

Second, the absence of any meaningful disclosure was another significant factor driving *Carpenter*'s holding.[130] The CSLI produced by Carpenter's phone was generated continuously, automatically, and without his knowledge.[131] Because there was no "*affirmative* act on the part of [Carpenter] beyond powering up" his phone, Carpenter did not voluntarily disclose his locational information in any "meaningful sense" that justified applying the third-party doctrine.[132] The Court also rejected the government's argument that Carpenter's decision to use a cell phone was equivalent to a voluntary disclosure of his CSLI data because, as the Court noted in its earlier decision in *Riley v. California*,[133] cell phones are "indispensable to participation in modern society."[134] Deciding to use a cell phone may have *technically* been a voluntary disclosure, but the lack of any meaningful choice meant that Carpenter was effectively compelled to disclose the CSLI.[135] Because the third-party doctrine does not apply to records created without a meaningfully voluntary choice,[136] the collection of those records by the government is likely a search.

Based on these factors, *Carpenter*'s central innovation was extending a reasonable expectation of privacy to third-party digital records that reveal the "privacies of life."[137] Writing for the majority, Chief Justice John Roberts noted that the government's collection of 127 days' worth of historical CSLI meant that Carpenter's movements had effectively been surveilled every moment of his life.[138] The Court cited concerns first expressed in Justice Sotomayor's concurrence in *United States v. Jones* and concluded that the aggregation of a person's

130. KERR, *Implementing* Carpenter, *supra* note 111 (manuscript at 20).

131. *See Carpenter*, 138 S. Ct. at 2220 ("Virtually any activity on the phone generates CSLI.").

132. *Id.* (emphasis added) (reasoning that Carpenter did not "voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements" (alteration in original) (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979))).

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

134. *Carpenter*, 138 S. Ct. at 2220 (citing *Riley*, 573 U.S. at 385).

135. *See id.* ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."); *see also* KERR, *Implementing* Carpenter, *supra* note 111 (manuscript at 21) ("*Carpenter* has a compulsion requirement.").

136. *See supra* notes 108–09 and accompanying text.

137. KERR, *Implementing* Carpenter, *supra* note 111 (manuscript at 21–22).

138. *See Carpenter*, 138 S. Ct. at 2218–19 ("Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years . . . .").

movements via CSLI is "deeply revealing."[139] Following Justice Sotomayor's earlier argument regarding GPS tracking, the Court concluded CSLI could also demonstrate one's "familial, political, professional, religious, and sexual associations."[140] Information *that* intimate, post-*Carpenter*, cannot be collected by the government without constitutional restrictions.

Thus, digital records that are similarly revealing when aggregated may be entitled to a reasonable expectation of privacy.[141] As a result, when police obtain those records in pursuit of a suspect, it constitutes a search under the Fourth Amendment. FRT and CSLI share similarities that, as Part IV discusses, likely implicate *Carpenter*'s analysis.[142] But as the Court acknowledged, this rule would not carry across all contexts.[143] The next Part explores *Carpenter*'s application to a new technology in a unique context: the border.

III. FOURTH AMENDMENT REASONABLENESS AT THE BORDER

Even if a search has occurred, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"[144] The baseline measure of reasonableness is the existence of a warrant, signed by a neutral magistrate, and supported by probable cause.[145] As a general rule, warrantless searches are "*per se* unreasonable . . . subject only to a few specifically established and well-delineated exceptions."[146] The "border-search exception" is one such case.[147] However, exceptions to the warrant requirement are subject to two key limitations: scope and intrusiveness.[148]

---

139. *Id.* at 2217, 2223 (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

140. *Id.* at 2217–18 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

141. KERR, *Implementing* Carpenter, *supra* note 111 (manuscript at 22).

142. *See infra* Part IV.

143. *Carpenter*, 138 S. Ct. at 2222–23. The Court recognized that the warrantless collection of CSLI might be reasonable if there are exigent circumstances that make obtaining a warrant unreasonable. *Id.* Furthermore, the Court declined to consider "collection techniques involving foreign affairs or national security." *Id.* at 2220.

144. Riley v. California, 573 U.S. 373, 381 (2014) (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)).

145. Coolidge v. New Hampshire, 403 U.S. 443, 454–55 (1971) (plurality opinion).

146. Katz v. United States, 389 U.S. 347, 357 (1967).

147. United States v. Ramsey, 431 U.S. 606, 620 (1977).

148. United States v. Cano, 934 F.3d 1002, 1011–12 (9th Cir. 2019), *petition for cert. filed*, No. 20-1043 (U.S. Jan. 29, 2021).

Given that exceptions to the warrant requirement are justified only for limited purposes, those purposes control the scope of the search.[149] Searches that do not further the purposes underlying an exception are outside the exception's scope and require a warrant—or a different exception—to be justified.[150] Additionally, the manner in which a search is conducted remains relevant to its constitutionality, even if that search is within the scope of an enumerated exception.[151] At a certain point, a search may be conducted in a manner *so* intrusive that it becomes unreasonable without added Fourth Amendment protections.[152] Courts evaluate the reasonableness of a search "by 'balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.'"[153]

To understand how the Fourth Amendment should regulate FRT at the border, this Part outlines the structure of the border-search exception and the underlying purposes that control its scope. It then describes the distinction between routine searches, which require no individual suspicion, and nonroutine searches, which are unreasonable without individualized suspicion. This Part concludes with a discussion of the debate over whether electronic-device searches are routine or nonroutine as a helpful frame for later applying the doctrine to FRT.

---

149. *See Riley*, 573 U.S. at 385–86 (declining to extend the search-incident-to-arrest exception to cell phones that posed no risk to officer safety or of evidence destruction); Arizona v. Gant, 556 U.S. 332, 339 (2009) (noting that officer safety and evidence preservation needs to "define the boundaries of the [search-incident-to-arrest] exception"); *see also* Mincey v. Arizona, 437 U.S. 385, 393–95 (1978) (holding unlawful a warrantless search based on the exigent circumstances exception when there was no exigency).

150. *Gant*, 556 U.S. at 351 (stating that when the justifications underlying one exception are absent, a search will be "unreasonable unless police obtain a warrant or show that another exception to the warrant requirement applies").

151. *See Cano*, 934 F.3d at 1012 ("[W]hile routine searches may be conducted at the border without any showing of suspicion, a more intrusive, nonroutine search must be supported by 'reasonable suspicion.'" (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 537–41 (1985))).

152. *See Montoya de Hernandez*, 473 U.S. at 533–35, 541 (suggesting a 16-hour border detention "beyond the scope" of a routine search would be unconstitutional without reasonable suspicion); *Cano*, 934 F.3d at 1011 ("[S]ome searches, even when conducted within the scope of the exception, are so *intrusive* that they require additional justification, up to and including probable cause and a warrant."). Notably, these protections extend equally to citizens and noncitizens at the border.

153. *Montoya de Hernandez*, 473 U.S. at 537–41 (quoting United States v. Villamonte-Marquez, 462 U.S. 579, 588 (1983)).

A. The Border-Search Doctrine

Under the border-search exception, border officials[154] may conduct warrantless, and often suspicionless, searches at the border.[155] The legal authority to conduct warrantless searches is "as old as the Fourth Amendment itself"[156] and based on the United States' "inherent authority to protect, and a paramount interest in protecting, its territorial integrity."[157] To that end, the Supreme Court has identified several justifications that animate the border-search doctrine. Warrantless border searches are permissible to the extent they are needed to protect national security, collect duties, intercept contraband, and enforce immigration laws.[158] Although the precise scope of the exception remains an open question,[159] a border search that is too attenuated from this rationale falls outside the scope of the exception.[160]

Even within the scope of the exception, border searches must still be reasonable.[161] At the border, the reasonableness balance is "qualitatively different" and weighs "much more favorably to the Government."[162] The government's paramount interest in border security is weighed against the individual's diminished—but not

154. Border searches may only be conducted by "customs and immigration officials, but not general law enforcement such as FBI agents." *Cano*, 934 F.3d at 1013; *see also* 19 C.F.R. § 162.6 (2020) (stating all people and objects entering the country are "liable to inspection and search by a Customs officer").

155. United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004).

156. United States v. Ramsey, 431 U.S. 606, 619 (1977).

157. *Flores-Montano*, 541 U.S. at 153.

158. *See id.* at 152–53 (acknowledging the border-search doctrine rests on the sovereign's right to protect itself, regulate the collection of duties, prevent the introduction of contraband, and prevent the entry of unwanted persons into the United States). For a comprehensive review of the United States' customs and immigration laws, see Laura K. Donohue, *Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches*, 128 YALE L.J. F. 961, 972–93 (2019) [hereinafter Donohue, *Customs, Immigration, and Rights*].

159. *Compare Cano*, 934 F.3d at 1016–19 (holding the border-search exception only sanctions searches for contraband presently at the border, not "evidence of past or future border-related crimes"), *with* United States v. Kolsuz, 890 F.3d 133, 143–44 (4th Cir. 2018) (stating the border-search exception encompasses both the direct interception of contraband and evidence of "ongoing transnational crime"), *and* United States v. Aigbekaen, 943 F.3d 713, 720–21 (4th Cir. 2019) (holding the border-search exception does not encompass searches solely for evidence of *domestic* crimes).

160. *See, e.g.*, *Aigbekaen*, 943 F.3d at 721 (holding an electronic-device search, based solely on knowledge of domestic crimes, would go beyond the scope of the exception).

161. United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985).

162. *Id.* at 538–40.

absent—expectation of privacy.[163] In practice, several factors affect the reasonableness of a border search, including where the search takes place and how it is conducted.

1. *Where a Search Is Conducted.* Searches at the physical border or its "functional equivalent"—such as an international airport—are almost always per se reasonable and do not require any individualized suspicion.[164] Meanwhile, searches physically removed from the border often require some level of individualized suspicion.[165]

2. *How a Search Is Conducted: Routine and Nonroutine Border Searches*. Recognizing that some border searches are conducted in a more intrusive manner than others, courts distinguish between routine and nonroutine searches. As the term connotes, most common border searches are considered routine under existing law. This includes identification checks, vehicle and luggage inspections, canine sniffs, and removal of the outer garments.[166] The Court has treated routine searches as essential to furthering the government's mission to determine a person's admissibility, collect customs duties, and intercept contraband.[167] More importantly, the privacy intrusion caused by these searches—at least in the context of the government's

163. *See id.* at 539 (noting a traveler's expectation of privacy is only "*less* at the border than in the interior" (emphasis added)).

164. *See* United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004) ("Time and time again, we have stated that 'searches made at the border . . . are reasonable simply by virtue of the fact that they occur at the border.'" (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977))); *see also id.* at 150 (holding that a search at the Otay Mesa Port of Entry did not require reasonable suspicion). The exception applies equally at the Canadian border and any interior airport where an international flight can land. *See* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 10.5(a) nn.14 & 16 (6th ed. 2020) (collecting cases applying the exception at the Canadian border and international airports).

165. Known as "extended border searches," the Court has, in some contexts, been willing to require probable cause for these searches. *See, e.g.*, United States v. Brignoni-Ponce, 422 U.S. 873, 881–82 (1975) (holding Border Patrol officers may, on a "roving-patrol," stop a vehicle near the border to inquire about "citizenship and immigration status . . . but any further detention or search must be based on consent or probable cause"). For further background on the contours of "extended border searches," see generally LAFAVE, *supra* note 164, §§ 10.5(g), (h), (i), (j).

166. *See generally* LAFAVE, *supra* note 164, § 10.5(a) (describing routine searches at the border and existing caselaw).

167. *See Flores-Montano*, 541 U.S. at 154–55 (highlighting drug-seizure statistics prior to holding that the removal of a gas tank is a routine search that does not violate the Fourth Amendment); United States v. Aigbekaen, 943 F.3d 713, 720 (4th Cir. 2019) (noting that routine, suspicionless searches at the border are permissible because of the government's interests at the border).

security needs—is relatively minimal.[168] Routine searches "are reasonable simply by virtue of the fact that they occur at the border" and require no individualized suspicion.[169]

This presumption of reasonableness can be rebutted, however, by demonstrating that a particular search is so intrusive as to render it *non*routine. Nonroutine searches go "beyond the scope of a routine customs search"[170] and are unreasonable unless supported by individualized suspicion.[171] Though there is no established test for distinguishing between routine and nonroutine searches,[172] courts have found nonroutine searches in different factual contexts. Some courts have found highly intrusive searches of a person's body to be nonroutine,[173] because unlike a routine search, these "cause any person significant embarrassment."[174] As a result, an officer must have reasonable suspicion before she can conduct them.[175] Courts typically place body-cavity searches, for example, in this category, thus making them nonroutine.[176]

The Supreme Court has also suggested that in some instances, physically destructive searches of personal property can be nonroutine

168. *See Flores-Montano*, 541 U.S. at 154 ("[O]n many occasions, we have noted that the expectation of privacy is less at the border than it is in the interior. We have long recognized that automobiles seeking entry into this country may be searched." (citation omitted)).

169. *Id.* at 152–53 (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977)).

170. United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985).

171. *See id.* (holding an extended detention of a traveler to be reasonable if agents "reasonably suspect that the traveler is smuggling contraband in her alimentary canal").

172. *See* YULE KIM, CONG. RSCH. SERV., RL31826, PROTECTING THE U.S. PERIMETER: "BORDER SEARCHES" UNDER THE FOURTH AMENDMENT 10–14 (2009) (noting there is "no established test that determines whether a particular search procedure is routine" and describing different types of routine and nonroutine search criteria).

173. *See, e.g.*, United States v. Kelly, 302 F.3d 291, 294 (5th Cir. 2002) ("Non-routine searches include body cavity searches, strip searches, and x-rays . . . . These types of objectively intrusive searches would likely cause any person significant embarrassment and invade 'the privacy and dignity of the individual.'" (quoting United States v. Sandler, 644 F.2d 1163, 1167 (5th Cir. 1981))).

174. *Id.*

175. *Id.* ("'Non-routine' border searches . . . are more intrusive and require a particularized reasonable suspicion before a search can be conducted.").

176. *See, e.g.*, Bustillos v. El Paso Cnty. Hosp. Dist., 891 F.3d 214, 220 (5th Cir. 2018) ("Cavity searches, strip searches, and x-ray examinations are all 'non-routine.'" (citation omitted)). For example, the forced inspection of a suspect's rectum in search of narcotics is nonroutine. *See id.* For more examples of nonroutine body searches, see generally LAFAVE, *supra* note 164, § 10.5(e).

and require reasonable suspicion.[177] These cases, although rare, typically involve the permanent, physical destruction of property—such as drilling into a car.[178] Additionally, some courts have held that border searches significantly intruding on personal privacy, even though they do not involve the physical search of the body or destruction of personal property, are nonroutine.[179] This issue has most commonly arisen in the context of searches of electronic devices, as the next Section details.

B. Border Searches of Electronic Devices

Border officials have been searching electronic devices, such as cell phones and laptops, as long as they have been in common use.[180] Beginning with *Riley v. California* in 2014, however, the Supreme Court has recognized the unique privacy interests associated with these devices.[181] Following this decision, lower courts split on whether searches of electronic devices at the border can continue to be treated as routine.[182]

In *Riley*, the Court rejected the warrantless search of an arrestee's cell phone pursuant to the search-incident-to-arrest exception.[183] Under that exception, officers searching an arrestee's person, and any containers within reaching distance, do not need a warrant if the search is conducted to ensure the officers' safety or prevent the destruction of evidence.[184] The *Riley* Court, however, refused to extend this exception to cell phones.[185] It reasoned that such searches exceed the scope of the

177. *Cf.* United States v. Flores-Montano, 541 U.S. 149, 154 n.2 (2004) (noting "the obvious factual difference[s]" between removing and reassembling a fuel tank and "potentially destructive drilling" into a vehicle).

178. *See id.* (collecting drilling cases).

179. *See, e.g.*, United States v. Mejia, 720 F.2d 1378, 1381–82 (5th Cir. 1983) (stating reasonable suspicion justifies an abdominal x-ray scan).

180. U.S. DEP'T OF HOMELAND SEC., DHS/CBP/PIA-008(A) PRIVACY IMPACT ASSESSMENT UPDATE FOR CBP BORDER SEARCHES OF ELECTRONIC DEVICES 1–2 (2018), https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf [https://perma.cc/3MKN-NYJJ] (noting CBP first issued a policy regarding electronic-device searches in 2009).

181. *See* Riley v. California, 573 U.S. 373, 393–97 (2014) (describing how "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person").

182. *See infra* notes 196–212 and accompanying text.

183. *Riley*, 573 U.S. at 401–03.

184. Arizona v. Gant, 556 U.S. 332, 343 (2009).

185. *Riley*, 573 U.S. at 384–86.

exception given that, in the vast majority of situations, an arrestee's cell phone poses no risk to officers and cannot be used to destroy evidence.[186] Furthermore, cell phone searches present special privacy concerns—unlike traditional containers such as boxes or car trunks—given the sheer amount of deeply personal information contained in cell phones.[187] Because the warrantless search of an arrestee's cell phone would "untether the rule from the justifications underlying the . . . exception,"[188] the Court held that officers searching a cell phone must first obtain a warrant.[189] *Riley*'s logic quickly raised questions about the status of electronic-device searches at the border.[190]

Unlike the *Riley* Court,[191] lower courts calibrate the level of suspicion required for an electronic-device search at the border to the specific kind of search that was conducted. Although there are no established categories, courts tend to distinguish between brief, manual inspections and more thorough, "forensic" searches of electronic devices.[192] Manual inspections are generally treated as routine searches that do not require individualized suspicion.[193] Forensic searches, on the other hand, involve the use of specialized software to "gain

186. *Id.* at 386–91.

187. *See id.* at 393 (noting how "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse," especially because of cell phones' "immense storage capacity").

188. *Id.* at 386 (quoting *Gant*, 556 U.S. at 343).

189. *See id.* at 403 ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

190. In the aftermath of *Riley*, some scholars argue that electronic-device searches must be considered nonroutine. *See, e.g.*, Eunice Park, *The Elephant in the Room: What Is a "Nonroutine" Border Search, Anyway? Digital Device Searches Post-*Riley, 44 HASTINGS CONST. L.Q. 277, 298–303 (2017); Thomas Mann Miller, Comment, *Digital Border Searches After* Riley v. California, 90 WASH. L. REV. 1943, 1987–96 (2015).

191. The cell phone in *Riley* was inspected hours after the initial arrest back at the police station. *Riley*, 573 U.S. at 379. However, the Court fashioned a categorical rule for all cell phone searches rather than distinguishing between where or how a search was conducted. *See id.* at 398, 403 (establishing a categorical rule on how cell-phone searches are conducted and emphasizing the need for the rule to be categorical to provide law enforcement with clear standards).

192. *See, e.g.*, United States v. Kolsuz, 185 F. Supp. 3d 843, 858 (E.D. Va. 2016) (holding that the manual search of defendant's iPhone at the airport was a routine border search, but the subsequent forensic search of the defendant's iPhone conducted at the HSI office in Sterling, Virginia was a "nonroutine border search requiring some level of individualized suspicion").

193. *See, e.g.*, Alasaad v. Mayorkas, 988 F.3d 8, 18–19 (1st Cir. 2021) (distinguishing between basic and advanced searches, and holding the former requires no individual suspicion); Park, *supra* note 190, at 288–92 (outlining how courts have "attempted to distinguish between routine and nonroutine [electronic-device] searches" by construing manual inspections as routine searches and forensic searches as nonroutine searches).

access . . . review, copy, and/or analyze [a device's] contents."[194] These searches may be considered nonroutine and thus may require some level of individualized suspicion to be constitutional.[195]

Since *Riley*, a circuit split has emerged regarding the appropriate level of Fourth Amendment protection applicable to searches of electronic devices.[196] Some courts take the position that all searches of electronic devices are routine and do not require *any* level of individualized suspicion.[197] In *United States v. Touset*,[198] for example, the Eleventh Circuit expressly rejected the argument that the privacy interests associated with digital technology changed the border-search analysis:

> [I]t does not make sense to say that electronic devices should receive special treatment because so many people now own them or because they can store vast quantities of records or effects. The same could be said for a recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents. Border agents bear the same responsibility for preventing the importation of contraband in a traveler's possession regardless of advances in technology.[199]

Additionally, in the eyes of the *Touset* court, *Riley*'s reasoning simply did not apply because only intrusive searches of a person's *body*

194. Donohue, *Customs, Immigration, and Rights*, *supra* note 158, at 970 (quoting U.S. CUSTOMS & BORDER PROT., CPD DIRECTIVE NO. 3340-049A, BORDER SEARCH OF ELECTRONIC DEVICES 5 para. 5.1.4 (2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf [https://perma.cc/H8SU-UKRS]).

195. *See, e.g.*, *Kolsuz*, 185 F. Supp. 3d at 858 (holding that the forensic search of the defendant's iPhone was a nonroutine border search requiring "some level of individualized suspicion").

196. *Compare* United States v. Cano, 934 F.3d 1002, 1015–18 (9th Cir. 2019), *petition for cert. filed*, No. 20-1043 (U.S. Jan. 29, 2021) (reasonable suspicion required), *and* United States v. Kolsuz, 890 F.3d 133, 146–48 (4th Cir. 2018) (individualized suspicion required but declining to decide the standard), *with* United States v. Touset, 890 F.3d 1227, 1233 (11th Cir. 2018) (no reasonable suspicion required).

197. *See, e.g.*, *Touset*, 890 F.3d at 1233 ("We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property."); United States v. Feiten, No. 15-20631, 2016 WL 894452, at *6 (E.D. Mich. Mar. 9, 2016) ("Allowing customs officials without a warrant to forensically search an electronic device presented at an international border or its equivalent is utterly consistent with its historical mooring of protecting the country by preventing unwanted goods from crossing the border into the country.").

198. United States v. Touset, 890 F.3d 1227 (11th Cir. 2018).

199. *Id.* at 1233.

could be considered nonroutine.[200] Other courts have simply avoided the constitutional question altogether by relying on the fact that reasonable suspicion existed at the time of the search or by applying the good-faith exception to the exclusionary rule.[201]

On the other side of the split, several courts have held that forensic searches of electronic devices, which typically involve the use of specialized software, are too intrusive to be routine.[202] On this line of reasoning, such searches are unconstitutional unless predicated on individualized suspicion.[203] In reaching that conclusion, lower courts have raised important questions about the scope of the border exception in the digital age.

In *United States v. Cano*,[204] the Ninth Circuit construed the border-search exception to only permit searches aimed at intercepting contraband *present* at the border, rather than "evidence of past or future border-related crimes."[205] Thus, forensic searches of electronic devices are constitutional only if the officer reasonably suspects it presently contains digital contraband.[206] The Fourth Circuit has also found electronic-device searches nonroutine, but arrived at that conclusion via a different route. In *United States v. Aigbekaen*,[207] it held that "the Government must have individualized suspicion of an offense that bears *some nexus* to the border search exception's purposes of protecting national security, collecting duties, blocking the entry of

200. *Id.* at 1234.

201. *See, e.g.*, United States v. Wanjiku, 919 F.3d 472, 479 (7th Cir. 2019) (finding both that reasonable suspicion existed and that the agents acted in good faith when they searched the devices); United States v. Molina-Isidoro, 884 F.3d 287, 290 (5th Cir. 2018) (applying the good-faith exception); United States v. Ramirez, EP-18-CR-3530-PRM, 2019 WL 3502913, at *14–15 (W.D. Tex. Aug. 1, 2019) (applying both).

202. *See, e.g.*, United States v. Cano, 934 F.3d 1002, 1015–16 (9th Cir. 2019), *petition for cert. filed*, No. 20-1043 (U.S. Jan. 29, 2021) ("Accordingly, we hold that manual searches of cell phones at the border are reasonable without individualized suspicion, whereas the forensic examination of a cell phone requires a showing of reasonable suspicion."); United States v. Kolsuz, 890 F.3d 133, 145–56 (4th Cir. 2018) ("[I]t is clear that a forensic search of a digital phone must be treated as a nonroutine border search, requiring some form of individualized suspicion.").

203. *Cano*, 934 F.3d at 1015–18; *Kolsuz*, 890 F.3d at 146–48.

204. United States v. Cano, 934 F.3d 1002 (9th Cir. 2019).

205. *Id.* at 1018.

206. *Id.* at 1019–20 (concluding that "border officials may conduct a forensic cell phone search only when they reasonably suspect that the cell phone to be searched itself contains contraband").

207. United States v. Aigbekaen, 943 F.3d 713 (4th Cir. 2019).

unwanted persons, or disrupting efforts to export or import contraband."[208]

The government's general interest in enforcing domestic criminal law is, according to the Fourth Circuit, unrelated to the sovereign's interest in controlling who and what enters the country.[209] Thus, a forensic search of an electronic device exceeds the scope of the border-search exception when it is based entirely on knowledge of domestic crimes, rather than cross-border crimes.[210] Similarly, in *Alasaad v. Mayorkas*,[211] the First Circuit took a broad view of the scope of the border exception. The *Alasaad* court held that the border-search exception encompasses "search[es] for contraband, evidence of contraband, or for evidence of activity in violation of the laws enforced or administered by CBP or ICE."[212]

Further, the courts that say electronic-device searches are nonroutine have recognized that after *Riley* and *Carpenter*, the privacy interests implicated by digital devices are simply too significant to jeopardize by withholding Fourth Amendment protection.[213] Courts that have decided what level of suspicion is necessary for these searches have settled on reasonable suspicion given its "modest, workable," and familiar nature.[214] Given that the Fourth Amendment question associated with FRT's use at the border has not yet been squarely presented to a court, there is no caselaw on how border-search law might apply.[215] The privacy issues associated with electronic-device searches, however, offer a useful framework for evaluating a future

208. *Id.* at 721 (emphasis added).

209. *See id.* (noting the border-search exception to the warrant requirement cannot be invoked based on a generalized interest in law enforcement).

210. *Id.* In *Aigbekaen*, the CBP officers searched the defendant's computer because they suspected it contained evidence of his involvement in purely domestic sex trafficking. *Id.* at 717–18. The Fourth Circuit held this search "lacked sufficient . . . nexus to the sovereign interests underlying the border search exception." *Id.* at 724.

211. Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir. 2021).

212. *See id.* at 20–21 (noting that "the border search exception's purpose is not limited to interdicting contraband; it serves to bar entry to those 'who may bring anything harmful into this country'" (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 544 (1985))).

213. *See, e.g.*, United States v. Cano, 934 F.3d 1002, 1014–16 (9th Cir. 2019), *petition for cert. filed*, No. 20-1043 (U.S. Jan. 29, 2021) (noting that the volume and sensitive nature of personal information stored on an electronic device requires a showing of reasonable suspicion before a forensic search); United States v. Kolsuz, 890 F.3d 133, 144–47 (4th Cir. 2018) (same).

214. *Cano*, 934 F.3d at 1015 (quoting United States v. Cotterman, 709 F.3d 952, 966 (9th Cir. 2013)).

215. *See supra* note 25.

case involving FRT's use at the border. To understand how those limitations might take shape, consider the following hypothetical border search.

IV. WHEN IS THE USE OF FACIAL RECOGNITION AT THE BORDER A SEARCH?

Imagine you are a Border Patrol officer stationed at one of the many secondary inspection stations at the Laredo Juarez-Lincoln Port of Entry. It is early January, so northbound traffic into Texas is an absolute nightmare.[216] The agent in the booth notifies you that another car is coming to your station. A surveillance camera captured an image of the driver as he approached the border in his car, but the TVS failed to return a positive match. Therefore, he was automatically directed to secondary inspection. You turn on your chest-mounted body camera to record the interaction. You meet with the driver and check his identification. He is a Nuevo Laredo resident studying in Laredo on a student visa. When you ask why he is crossing on a Saturday, he informs you that he is going to visit some friends before the semester starts on Monday. He mentions that he crosses on an almost daily basis for class.[217] Another agent walks a drug-sniffing dog around the car, but the dog does not alert. You have a hunch something is not right, but it is also one of the busiest days of the year and more cars are coming. So, you let him go.

Your shift ends, and, as DHS policy requires, you review your body camera footage from the day.[218] When you come back to the footage from your encounter with the student, you remember your hunch. You isolate a still photograph of his face and, against DHS

---

216. Every year, thousands of Mexican-American families—including this Author's own—return to Mexico to celebrate Christmas in their hometowns. Daniel Becerril, *This Caravan of Migrants Headed South to Mexico—for Christmas*, REUTERS (Dec. 26, 2019, 3:09 AM), https://www.reuters.com/article/us-usa-immigration-mexico/this-caravan-of-migrants-headed-south-to-mexico-for-christmas-idUSKBN1YU0LN [https://perma.cc/6VXM-BR6M]. However, the traffic congestion in early January—when everyone returns from the holidays—makes entry into the United States painfully slow.

217. Charlotte West, *Thousands of Students Cross the U.S.-Mexico Border Every Day To Go to College*, HECHINGER REP. (June 19, 2019), https://hechingerreport.org/thousands-of-students-cross-the-southern-border-every-day-to-go-to-college [https://perma.cc/Q9NY-VUKZ].

218. *See* U.S. CUSTOMS & BORDER PROT., U.S. DEP'T OF HOMELAND SEC., DHS/CBP/PIA-052, PRIVACY IMPACT ASSESSMENT FOR THE INCIDENT-DRIVEN VIDEO RECORDING SYSTEMS (IDVRS) EVALUATION 5 (2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp052-idvrs-april2018.pdf [https://perma.cc/8SFR-YGN8].

policy, send it directly to the resident HSI agent so she can run it through an FRS.[219] First, she submits the image to the standard, approved government FRS which displays his visa photograph, driver's license, and images from his border crossings. Unsatisfied, you ask her if there is any other FRS she can use. She recalls learning about a new commercial FRS the agency had preliminarily contracted with and, although the FRS was still in the DHS approval process, she submits the photo. Within seconds, the FRS returns dozens of images. One group of images appears to be from surveillance camera footage because, in the background, you notice different landmarks like the local mall, a church, and a school campus.

One image appears to be his Facebook profile picture, based on the link underneath the image. But the largest set of images shows him with several groups of people. In some of these images, he is facing the camera and wearing a necklace bearing an image of Jesus Malverde—a religious symbol your training and experience has taught you is associated with drug traffickers.[220] In another, he appears to be in the background and looking slightly away from the camera. In the foreground of this image, you notice one man carrying a pistol and another man you recognize as a wanted cartel member. You start accessing the source links. The first image is from his Facebook profile, which is set to private. The other photos all appear on other people's profiles, although he is not tagged in any of them. Based on this information, his crossing history, and your training, you suspect he might be a drug courier.[221] So, you tag the footage as having potential evidentiary value and advise co-agents to send the driver to secondary the next time he crosses. The whole process takes less than five minutes.

---

219. ICE agents "must use reasonable efforts to identify the individual" through traditional investigation techniques before submitting the image to an FRS. ICE PRIVACY IMPACT, *supra* note 43, at 6–7.

220. *See* Nathaniel Janowitz, *A Narco-Saint, a Death Cult, and a Lost-Cause Apostle Await the Pope in Mexico*, VICE NEWS (Feb. 11, 2016, 9:45 AM), https://www.vice.com/en_us/article/wja4nb/a-narco-saint-a-death-cult-and-a-lost-cause-apostle-await-the-pope-in-mexico [https://perma.cc/DZ42-5972]. Of course, this is not always the case as many law-abiding Catholics treat Jesus Malverde as a saint. *Id.* However, border officials have treated the observation of Malverde as a fact justifying further investigation. *E.g.*, United States v. Valera-Delgado, 547 F. Supp. 2d. 704, 707–08 (W.D. Tex. 2008).

221. Alex Riggins, *Former Student Who Recruited Classmates as Cross-Border Drug Mules Sent to Prison*, L.A. TIMES (Aug. 20, 2019, 1:19 PM), https://www.latimes.com/california/story/2019-08-20/chula-vista-high-schooler-who-recruited-teen-drug-mules-sent-to-prison [https://perma.cc/LNH9-JPYH].

On Monday, he crosses again and is immediately directed to your secondary inspection station. You run a drug canine around the car, and this time the dog alerts by sitting down. A search reveals a secret compartment containing two kilos of heroin. The driver is charged with importing narcotics.[222] In your report, you note that your suspicion arose only *after* viewing the candidate list returned by the commercial FRS.[223] The driver moves to suppress the seized drugs on two grounds. First, the driver challenges the initial TVS scan that misidentified him and sent him to secondary. Second, he challenges your viewing of the candidate list returned by the commercial FRS. Both, he alleges, constitute illegal searches. Answering either question requires applying "the blunt instrument of the Fourth Amendment" to technology far beyond anything envisioned by its authors.[224]

This Part builds on the hypothetical in two ways, loosely corresponding to the two grounds on which the suspect in the hypothetical challenged the introduction of drugs as evidence against him. It distinguishes between face verification and face identification, introduced above,[225] to analyze the use of FRT at the border. First, Section A argues that the use of TVS for face verification is likely permissible under the Fourth Amendment. Second, Section B argues that the use of commercial FRS databases for face identification likely violates a reasonable expectation of privacy, thus requiring some level of suspicion before such a search is permissible under the Fourth Amendment.

A. Face Verification and Reasonable Expectations of Privacy

The use of facial recognition at the border presents two questions relevant to the Fourth Amendment search inquiry. Given facial recognition's primary purpose is to identify people, the first question is whether people have a reasonable expectation of privacy in their identity, even when subject to the diminished protections at the border. Additionally, because FRT can only identify people after analyzing the images contained in a comparison database, the second question is whether, post-*Carpenter*, there is a reasonable expectation of privacy in the images contained within those databases. How these questions

222. 21 U.S.C. § 952(a) (2018).

223. A "hunch" is not reasonable suspicion. Terry v. Ohio, 392 U.S. 1, 27 (1967).

224. *See* Riley v. California, 573 U.S. 373, 408 (2014) (Alito, J., concurring in part) (criticizing the efficacy of applying the Fourth Amendment to modern technology).

225. *See supra* Parts I.A–I.B.

are answered depends on whether the FRT is being used for face verification or identification. As to the former, the use of FRT for face verification is likely not a search under the Fourth Amendment because there is no reasonable expectation of privacy in identity at the border.

As noted above,[226] there is a plausible argument that individuals maintain a reasonable expectation of privacy in their identity as a general matter. Social norms reflect a subjective expectation of privacy in one's identity when in public. As Professor Mariko Hirose notes: "[W]e invite 'the intruding eye' of strangers to glance at or even examine our faces as we pass by, but we do not invite them to also identify us by our names and addresses, much less occupation, immigration status, criminal history, and other personal information."[227] Given this social practice—and the fact that law enforcement cannot compel someone to identify themselves without reasonable suspicion of wrongdoing[228]—this expectation of privacy is likely reasonable.

However, these arguments carry less weight at the border. There, anyone seeking to enter the United States must identify themselves and demonstrate they are lawfully entitled to enter.[229] Those whose identities cannot be verified may be denied entry into the country.[230] Normally, this poses no problem under the Fourth Amendment because determining a traveler's admissibility is one of the core purposes underlying the border-search exception.[231] Travelers seeking entry into the United States, therefore, waive any expectation of privacy in their identity at the border. However, the emerging use of FRT to verify a traveler's identity may change the constitutional calculus. This is because the databases on which FRT relies to be effective can reveal personal information unrelated to determining

226. *See supra* notes 101–02 and accompanying text.

227. Hirose, *supra* note 101, at 1601. This expectation is arguably diminished in the age of social media, on which users regularly disclose private information. *See* Brian Mund, Note, *Social Media Searches and the Reasonable Expectation of Privacy*, 19 YALE J.L. & TECH. 238, 247–48 (2017) (describing current caselaw finding no reasonable expectation of privacy for information disclosed on social media networks).

228. Hiibel v. Sixth Jud. Dist. Ct. of Nev., 542 U.S. 177, 188 (2004).

229. *See generally* DHS Inspection of Persons Applying for Admission, 8 C.F.R. § 235.1 (2020) (outlining the identification requirements "to lawfully enter the United States").

230. *See* § 235.1(f)(1).

231. *See* Carroll v. United States, 267 U.S. 132, 154 (1925) (noting that requirements for international travelers to identify themselves are permissible for national self-protection).

someone's admissibility. That is, because the FRT search goes beyond the scope of law enforcement's needs to determine a person's admissibility, and because it may reveal deeply personal information, it risks running afoul of the Fourth Amendment.

CBP's face verification system, the TVS, likely does not violate a reasonable expectation of privacy in third-party data in its current form. Similar to the CSLI in *Carpenter*, the face verification performed by the TVS is possible only due to "seismic shifts in digital technology."[232] Facial recognition systems analyze a traveler's facial features, create a numerical face template, and compare it against other face templates to produce a nearly instantaneous match. But there are key differences between the TVS and the technology at issue in *Carpenter*.

If the TVS is used to perform a one-to-one match, the software compares only a travel document and a traveler's face. Third-party records are, by definition, not being accessed, and *Carpenter* is not implicated.[233] Even when the TVS accesses third-party records to verify a traveler's identity, those records were likely voluntarily disclosed "in [a] meaningful sense."[234] This is so because the TVS accesses images from governmental sources like passports, visas, and photos from previous border crossings.[235] These images are taken only after a person takes an affirmative step to disclose their face and identity to the government. For example, the student in the above hypothetical would have had to apply for a student visa and voluntarily submit his photograph to the Department of State.[236] There is nothing surreptitious about this process. The third-party doctrine likely applies to these kinds of images and forecloses any reasonable expectation of privacy.

---

232. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

233. *Cf. id.* at 2223 (finding the warrantless collection of CSLI to be a search, despite the fact that the information came from a third party, "[i]n light of [its] deeply revealing nature[,] . . . depth, breadth, and comprehensive reach").

234. *Id.* at 2220 (noting the inescapable nature of CSLI).

235. *See supra* Part I.B.1.

236. *See Student Visa*, U.S. DEP'T OF STATE, https://travel.state.gov/content/travel/en/us-visas/study/student-visa.html [https://perma.cc/QNV9-7FJT] (listing a photo as one of the identification requirements for a student visa). The same argument applies to images from recent border crossings. Cameras are ubiquitous and readily visible at the border. In fact, the City of Laredo uploads live video feeds of each border crossing. *Laredo, Texas*, CITY OF LAREDO, https://www.cityoflaredo.com/bridgesys/Cameras/bridge4cam.html [https://perma.cc/Q5XP-HG9Y]. Therefore, the decision to cross the border forecloses any expectation of privacy in one's images from those crossings.

Finally, these records do not reveal "the privacies of life."[237] If the TVS is used to produce a one-to-one match, then the only information disclosed to the border officials is that the person presenting herself is the same person pictured on her travel document. The personal information disclosed to border officials is similarly limited when TVS queries a third-party database. Travel document photographs are usually taken in a controlled setting and only display the individual's face.[238] They typically reveal nothing about a person's associations, political activities, or religious beliefs[239]—three areas the Court was particularly concerned with preserving the privacy of in *Carpenter*.[240]

Although images from border crossings can reveal locational information, the inferences that can be drawn from such images are limited. A border official viewing these photos would know only when and how often a person crosses the border, not where a traveler was before reaching the border or where she went after.[241] The collection of even a large number of images from previous border crossings likely does not raise constitutionally significant privacy concerns.[242] Applied to the hypothetical, such images would only provide a snapshot of the student's movements—far from divulging "the privacies of life." Given the limited scope of the information accessed by the TVS, the use of face verification at the border is likely not a search implicating the Fourth Amendment.

---

237. *Carpenter*, 138 S. Ct. at 2217 (quoting Riley v. California, 573 U.S. 373, 403 (2014)).

238. *E.g.*, *Passport Photos*, U.S. DEP'T OF STATE, https://travel.state.gov/content/travel/en/passports/how-apply/photos.html [https://perma.cc/VYR2-NEYK].

239. Of course, there are instances where a travel document may reveal information about one's religious beliefs—such as wearing a necklace or head covering. *See id.* ("You may not wear . . . head coverings, except for religious . . . purposes and with a signed statement."). That information is affirmatively disclosed to the government in those cases.

240. *See Carpenter*, 138 S. Ct. at 2217.

241. On this issue, *Commonwealth v. McCarthy*, 142 N.E.3d 1090 (Mass. 2020), provides a useful analogy. In *McCarthy*, police collected automated-license-plate-reader data from cameras stationed at two Cape Cod bridges. *Id.* at 1095. The court recognized that, while police certainly collected a large amount of data, the scope of the information disclosed was fairly limited. *See id.* at 1105–06. Therefore, the images did not reveal "the privacies of life," and there was no search. *Id.* at 1106.

242. *Cf. Carpenter*, 138 S. Ct. at 2223 (granting Fourth Amendment protection to CSLI, in part, because of "its depth, breadth, and comprehensive reach").

B. Face Identification and Reasonable Expectations of Privacy

Unlike face verification, face identification probably amounts to a search because it intrudes on the reasonable expectation of privacy in third-party digital records. Like face verification, face identification is possible only because of advances in digital technology. But there is a constitutionally significant difference between the kinds of records accessed during face identification. As currently used by ICE, the specific FRS an agent uses will determine the kinds of images she can see. Submitting an image to a governmental FRS may access millions of face templates generated from passports, driver's licenses, and criminal mugshots.[243] There likely is no expectation of privacy in this class of images. However, the use of a commercial FRS raises more serious Fourth Amendment concerns.

The implication of a commercial vendor using "internal processes" to collect images is that the images used for face identification from that vendor will sometimes lack the constitutionally required level of voluntariness.[244] Consider the issue of surveillance camera footage. Commercial vendors can populate their databases with images collected from surveillance cameras through contracts with private companies and government agencies or through collecting the footage themselves.[245] These images are often captured surreptitiously and without a person's knowledge.[246] Traveling in public, of course, exposes one to the risk that she will be seen by others. That decision, however, does not equate to an assumption of the risk that a private company will compile a "comprehensive dossier of [one's] physical movements."[247] Moreover, how could one even avoid that risk? With nearly 70 million active surveillance cameras—roughly

243. ICE PRIVACY IMPACT, *supra* note 43, at 12–16.

244. *Cf. Carpenter*, 138 S. Ct. at 2220 (finding that the collection of CSLI data did not trigger the third-party doctrine because Carpenter did not in any meaningful sense voluntarily "assume[] the risk" that his locational information would be aggregated (alteration in original) (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979))).

245. *See, e.g.*, Murgia, *supra* note 73 (describing the creation of an image database by government researchers); Jake Satisky, *A Duke Study Recorded Thousands of Students' Faces. Now They're Being Used All over the World*, DUKE CHRON. (June 11, 2019, 9:24 PM), https://www.dukechronicle.com/article/2019/06/duke-university-facial-recognition-data-set-study-surveillance-video-students-china-uyghur [https://perma.cc/ZHT7-JSFS] (describing how researchers collected images from surveillance footage on a university campus).

246. *See* Satisky, *supra* note 245 ("What they might not have known is that . . . Duke researchers were recording them and putting their likenesses into a data set.").

247. *Carpenter*, 138 S. Ct. at 2220.

one for every four people[248]—the only real options are to stay home or take affirmative steps to defeat facial recognition systems.[249]

The practice of collecting images via "searches of open source systems" poses similar risks.[250] Clearview AI, for example, "scrapes" the internet for supposedly "publicly available" images from websites like Facebook, LinkedIn, and YouTube, and it compiles them into a single database for law enforcement use.[251] But just because an image is "publicly available" does not mean it was affirmatively disclosed to the public. For example, in the above hypothetical, the driver's Facebook profile picture likely was "meaningfully disclosed" since he affirmatively uploaded the picture to Facebook.[252] But what about the images where the driver is with his friends and facing the camera? The awareness that his picture was being taken does not *necessarily* equate to consent for his photo to be uploaded to the internet.

And the picture where he was in the background facing away from the camera? Surely, he could not affirmatively disclose a picture he did not know was being taken. Even if one lacks an expectation of privacy over any single picture, the act of being in public, associating with others, and potentially having your picture taken does not necessarily equal an assumption of the risk that *all* of these pictures will be secretly collected and aggregated in a database. Regardless, a commercial vendor like Clearview AI collects each of these images, without

248. Liza Lin & Newley Purnell, *A World with a Billion Cameras Watching You Is Just Around the Corner*, WALL ST. J. (Dec. 6, 2019, 1:00 AM), https://www.wsj.com/articles/a-billion-surveillance-cameras-forecast-to-be-watching-within-two-years-11575565402 [https://perma.cc/9B82-XAL6].

249. "Defeating" facial recognition refers to measures taken to prevent an FRS from identifying someone. This often entails obstructing a clear view of one's face or interfering with an FRT-enabled camera. *See* COUNTERTERRORISM MISSION CTR., U.S. DEP'T OF HOMELAND SEC., VIOLENT ADVERSARIES LIKELY TO USE PROTECTIVE MASKS TO EVADE FACIAL RECOGNITION SYSTEMS 1–2 (2020), https://www.documentcloud.org/documents/6989376-U-FOUO-in-Violent-Adversaries-Likely-to-Use.html [https://perma.cc/QM52-4E5A] (describing methods used to defeat facial recognition).

250. *See* ICE PRIVACY IMPACT, *supra* note 43, at 16 (describing how these systems may violate the privacy standards of social media platforms).

251. Hill, *supra* note 13.

252. This hypothetical of course assumes the suspect had a certain level of consent to his images being online. A much more troubling case would exist in the case of someone who chooses not to have an online presence but whose image was captured incidentally in another person's photo and uploaded to the internet.

distinction, and displays them to law enforcement.[253] This directly implicates *Carpenter*.

The images displayed by a commercial FRS can collectively reveal the "privacies of life" in at least two ways. Commercial FRSs that display surveillance camera footage can disclose a person's locational information, depending on the camera's location.[254] With enough surveillance footage, a border official could access "a comprehensive chronicle of [a person's] past movements."[255] This, the Court said in *Carpenter*, gives the government "an intimate window into a person's life," because locational information "reveal[s] . . . 'familial, political, professional, religious, and sexual associations.'"[256] If both sets reveal the same substantive information, it makes little sense to privilege locational information revealed directly by CSLI over locational information revealed incidentally by FRT.[257]

Most importantly—and unlike the CSLI in *Carpenter*—face identification directly reveals the personal information protected under *Carpenter*. For example, ICE acknowledges that it uses commercial FRSs that "scrape" social media websites.[258] When these images are unconstrained, they can display everyone and everything contained in the picture. A border official can, as the hypothetical illustrates, learn who one's friends are or simply who is nearby. A border official can determine religious or political affiliations based on where someone is or what they are wearing. Depending on the number of pictures available online, the entirety of a person's private life could be displayed to any border official who decides to use a commercial FRS. If individuals have a reasonable expectation of privacy in locational records because they reveal "the privacies of life" *by inference*, as in *Carpenter*,[259] then images that reveal that same

253. Hill, *supra* note 13.

254. For example, if you live in Los Angeles, a company could hypothetically contract with Caltrans to access its network of CCTV cameras and capture your movements on most freeways. *Caltrans CCTV Map*, CALTRANS, http://cwwp2.dot.ca.gov/vm/iframemap.htm [https://perma.cc/3JMX-8L9W].

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

256. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).

257. Moreover, *Carpenter* did not foreclose the possibility that its reasoning could apply to data that reveals location incidentally. *See id.* at 2220 ("Nor do we address other business records that might incidentally reveal location information.").

258. ICE PRIVACY IMPACT, *supra* note 43, at 16.

259. *See Carpenter*, 138 S. Ct. at 2217 (protecting location records because they "hold for many Americans the 'privacies of life'").

information *directly* must be entitled to an expectation of privacy. Consequently, the use of face identification at the border is a search and thus implicates the reasonableness requirement of the Fourth Amendment. That conclusion, however, does not determine what level of protection the Fourth Amendment offers.

V. WHEN IS THE BORDER USE OF FACIAL RECOGNITION UNREASONABLE?

Any use of FRT that constitutes a search must ultimately be reasonable to pass Fourth Amendment scrutiny.[260] In the border context, this inquiry begins with a presumption in favor of the government's authority to use FRT without any individualized suspicion.[261] However, if its use becomes too intrusive on personal privacy—determined relative to the sovereign's security needs—then it is a nonroutine search warranting additional Fourth Amendment protection.[262]

A. Face Verification and Fourth Amendment Reasonableness

The use of TVS for face verification, as explained above, is most likely not a Fourth Amendment search. Therefore, TVS can be used without implicating the Fourth Amendment at all.[263] Further, even if it were a search, it would most likely be a routine search that could be conducted without any individualized suspicion.

Face verification falls within the scope of the border-search exception since it substantially furthers the government's interest in determining a traveler's admissibility. One of the core interests underpinning the border-search doctrine is the need to prevent the entry of "unwanted persons and effects."[264] An essential corollary to that interest is "requiring one entering the country to identify himself as entitled to come in."[265] This has traditionally been accomplished by

260. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) ("The Fourth Amendment commands that searches and seizures be reasonable.").

261. *Id.* at 538.

262. *See id.* at 538, 541 (holding that the "detention of a traveler at the border, beyond the scope of a routine customs search and inspection" requires reasonable suspicion).

263. *See* FRIEDMAN, *supra* note 87, at 211 ("[I]f something is not a 'search' . . . the Fourth Amendment provides no protection *at all*.").

264. United States v. Flores-Montano, 541 U.S. 149, 152 (2004).

265. United States v. Ramsey, 431 U.S. 606, 618 (1977) (emphasis omitted) (quoting Carroll v. United States, 267 U.S. 132, 154 (1925)).

a border official physically inspecting a traveler's documentation and visually confirming they are the same person. The TVS can identify a traveler more quickly and more accurately than a border official can.[266]

Additionally, face verification's intrusion on individual privacy is minimal. If the TVS is used for a one-to-one match, the information used for verification is restricted to what is contained on a person's travel document. Even when the TVS accesses images in a comparison database, the comparison is limited to images where the expectation of privacy is minimal—such as other government-issued travel documents. CBP's image-retention policy also places strict time limits on the retention of photos collected via the TVS.[267] And again, even if the use of face verification at the border was a search, it would be more akin to a routine border search that could be performed without any individualized suspicion.

B. Face Identification and Fourth Amendment Reasonableness

The Fourth Amendment analysis for face identification—as opposed to face verification—leads to a different conclusion. This Section first analyzes the reasonableness of face identification, concluding it is unreasonable outside of some individualized suspicion. It then discusses what level of individualized suspicion is appropriate to satisfy the Fourth Amendment.

1. *Reasonableness Balancing for Face Identification*. Suspicionless face identification is unreasonable at the border when it reveals "the privacies of life." The issues associated with face identification parallel those associated with electronic-device searches in at least two ways. First, this use of FRT does not fit neatly within the scope of the border-search doctrine. Like the information gleaned from an electronic-device search, the information revealed by a commercial FRS search, such as travel habits, associations, or beliefs, may not directly

266. *See* TVS PRIVACY IMPACT, *supra* note 42, at 3 ("[F]acial recognition has presented CBP with the best biometric approach because it can be performed relatively quickly, with a high degree of accuracy . . . ."); *see also* U.S. Customs & Border Prot., Changing the Face of Travel 9–10 (July 2018) (published online by the Electronic Privacy Information Center), https://epic.org/foia/dhs/cbp/biometric-entry-exit-alt-screening-procedures/Changing-the-Face-of-Travel-Preso-July2018.pdf [https://perma.cc/3RR7-LWXZ] (highlighting, *inter alia*, the faster boarding times and up to 98.2 percent match rate associated with FRT).

267. *See* TVS PRIVACY IMPACT, *supra* note 42, at 8–9.

determine a person's admissibility.[268] But the information displayed by a commercial FRS can certainly be relevant in other ways to furthering the government's interests at the border.[269] For example, if the student in the hypothetical is admissible on a student visa, but surveillance camera footage returned by an FRS suggests he never travels to the school, that may be grounds for further questioning.[270] Information about one's associations can, as demonstrated in the hypothetical, be relevant to determining whether someone might be importing contraband or whether they pose a national security threat.

Second, the intrusion on a traveler's dignity and privacy interests occasioned by face identification is, after *Carpenter* and *Riley*, too great to be without some level of Fourth Amendment protection. Like electronic devices, face identification can reveal information that details the full scope of an individual's private life. An investigating border officer can submit someone's image to a commercial FRS and—long after a traveler has left the border—examine every aspect of that person's private life. Routine compliance with immigration and customs law does not require that level of disclosure.[271] This type of face recognition thus resembles a nonroutine electronic-device search, and its use should be considered unreasonable without some level of individualized suspicion.

2. *A Reasonable Suspicion Standard*. Border officials should be required to have reasonable suspicion to justify using face identification, as opposed to face verification. Following the Fourth Circuit's approach, the standard for reasonable suspicion should be that it must pertain to a crime that "bears some nexus to the border search exception's purposes of protecting national security, collecting

268. Admissibility is conditioned on having legal status to enter the country. Images from CCTV and social media will not typically indicate whether someone is legally authorized to enter the country.

269. *See* United States v. Aigbekaen, 943 F.3d 713, 721 (4th Cir. 2019) (suggesting that what constitutes an evidentiary basis for a specific crime is relevant to individualized suspicion).

270. If someone is issued a student visa, one's ability to work is often restricted, see generally *Students and Employment*, U.S. CITIZENSHIP & IMMIGR. SERVS., https://www.uscis.gov/working-united-states/students-and-exchange-visitors/students-and-employment [https://perma.cc/YZ4C-T8W4]. Violation of those rules can impact a student's future ability to enter the United States. *See* 8 U.S.C. § 1182(a)(6)(G) (2018) (stating that a student visa holder who "violates a term or condition of such status" is inadmissible "until the alien has been outside the United States for a continuous period of 5 years after the date of the violation").

271. *Cf. Aigbekaen*, 943 F.3d at 720–21 (treating a forensic device search as nonroutine based, in part, on the privacy interests implicated by such devices).

duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband."[272] This limitation would keep the rule tethered to the purposes underlying the border-search exception.

Requiring officers to establish reasonable suspicion of wrongdoing before they use FRT to conduct face identification should be the constitutional floor at the border for several reasons. For one, it is the only standard the Supreme Court and courts of appeals have suggested would apply at the border for nonroutine searches.[273] Plus, no lower court that has decided this issue in the electronic-device-search context has required more than reasonable suspicion.[274]

Most importantly, it is arguably the standard that strikes the appropriate balance between the government's security prerogatives and individual privacy interests at the border.[275] Given the amount of contraband entering the United States, and the creative tactics employed by smugglers, a higher standard simply might not be practical.[276] In many cases, there may be enough facts for a border official to have reasonable suspicion but not enough to establish probable cause.[277] And even if probable cause could accommodate the needs of border officials, *Riley* and *Carpenter* both contemplate that

272. *Id.* at 721.

273. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 540–41 (1985); *cf.* United States v. Molina-Isidoro, 884 F.3d 287, 291 (5th Cir. 2018) ("For border searches both routine and not, no case has required a warrant."). The Supreme Court expressly rejected other amorphous standards such as "clear indication" or "plain suggestion." *See Montoya de Hernandez*, 473 U.S. at 536, 540–41 ("We do not think that the Fourth Amendment's emphasis upon reasonableness is consistent with the creation of a third verbal standard in addition to 'reasonable suspicion' and 'probable cause'; we are dealing with a constitutional requirement of reasonableness, not *mens rea* . . . .").

274. *See, e.g.*, United States v. Cano, 934 F.3d 1002, 1007 (9th Cir. 2019), *petition for cert. filed*, No. 20-1043 (U.S. Jan. 29, 2021) (reasonable suspicion applies); *see also* United States v. Wanjiku, 919 F.3d 472, 485 (7th Cir. 2019) ("[N]o circuit court, before or after *Riley*, has required more than reasonable suspicion for a border search of cell phones or electronically-stored data.").

275. *See Montoya de Hernandez*, 473 U.S. at 541 ("The 'reasonable suspicion' standard . . . effects a needed balance between private and public interests when law enforcement officials must make a limited intrusion on less than probable cause.").

276. *See, e.g.*, *id.* at 541–43 (noting "alimentary canal smuggling at the border . . . gives no external signs and inspectors will rarely possess probable cause to arrest or search"). For an insight into the contraband seized at the border to date, see *CBP Enforcement Statistics Fiscal Year 2021*, U.S. CUSTOMS & BORDER PROT. [hereinafter *CBP 2021 Statistics*], https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics [https://perma.cc/C7YB-Q65M].

277. *See Montoya de Hernandez*, 473 U.S. at 541–43.

different contexts might require different standards.[278] Given that probable cause has never been applied to searches at the border,[279] it is difficult to imagine a standard higher than reasonable suspicion without direction from the Supreme Court.

To be sure, the reasonable suspicion standard is not without flaws. Reasonable suspicion, some argue, does little to prevent "arbitrary, discriminatory, and harassing searches,"[280]—especially considering the judicial deference afforded to the training and experience of border officials.[281] Because the reasonable suspicion standard offers little substantive protection, they argue only probable cause is appropriate after *Riley* and *Carpenter*.[282] However, courts routinely employ the reasonable suspicion standard to suppress evidence and check government overreach.[283] This standard, while not perfect, offers a baseline level of protection against completely suspicionless searches.[284] That is the "very evil the Fourth Amendment was intended to stamp out."[285]

---

278. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018); Riley v. California, 573 U.S. 373, 401–02 (2014) ("[O]ther case-specific exceptions may still justify a warrantless search of a particular phone.").

279. Probable cause has been applied to searches and seizures *near* the border. *See, e.g.*, United States v. Brignoni-Ponce, 422 U.S. 873, 881–82 (1975) (holding that an officer on roving patrol may question suspects about their citizenship status or any suspicious circumstance, "but any further detention or search must be based on consent or probable cause"). What standard might apply in those contexts is beyond the scope of this Note.

280. *E.g.*, Christopher I. Pryby, Note, *Forensic Border Searches After* Carpenter *Require Probable Cause and a Warrant*, 118 MICH. L. REV. 507, 527 (2019).

281. *See, e.g.*, Abidor v. Napolitano, 990 F. Supp. 2d 260, 282 (E.D.N.Y. 2013) ("Reasonable suspicion is a relatively low standard and border officials are afforded deference due to their training and experience." (citing *Montoya de Hernandez*, 473 U.S. at 542)).

282. *E.g.*, Pryby, *supra* note 280, at 520–30 ("[T]he government must develop probable cause and obtain a warrant before performing a forensic search of an electronic device at the border."); Donohue, *Customs, Immigration, and Rights*, *supra* note 158, at 1014. One recent article questions the historical assumptions underlying suspicionless searches of electronic devices, see generally Note, *The Border Search Muddle*, 132 HARV. L. REV. 2278 (2019).

283. In the border context, courts have suppressed evidence discovered when officers had little more than vague suspicions of wrongdoing. *See, e.g.*, United States v. Aigbekaen, 943 F.3d 713, 723–24 (4th Cir. 2019) (finding reasonable suspicion did not exist simply because the agent "had a concern" that an electronic device "might" contain child pornography); United States v. Puga, No. 5:19-CR-1346-1, 2019 WL 7170623, at *6 (S.D. Tex. Dec. 24, 2019) (holding a 911 call "that vaguely reported 'suspicious' behavior" does not amount to reasonable suspicion).

284. *See, e.g.*, *Aigbekaen*, 943 F.3d at 723–24 (4th Cir. 2019) (finding reasonable suspicion did not exist simply because the agent "had a concern" that an electronic device "might" contain child pornography).

285. Samson v. California, 547 U.S. 843, 858 (2006) (Stevens, J., dissenting).

3. *A Source Rule for Face Identification at the Border*. The *Riley* Court recognized the importance of fashioning legal doctrine that "provide[s] clear guidance to law enforcement through categorical rules."[286] The need for a categorical rule is especially important for the use of face identification at the border. For some of the databases used by border officials employing FRT, there might not be a reasonable expectation of privacy at all. As the hypothetical demonstrates, there may be a reasonable expectation of privacy over some sets of images but not others. A subjective standard is superficially appealing: when the government "learns something invasive, a search has occurred."[287] But an officer might not know whether a set of images is "invasive" before conducting the search or until additional facts are known.[288]

Similarly, drawing a mosaic-theory line based on when the amount of information collected becomes too intrusive is also unclear.[289] The number of photos displayed to an officer is tied to the amount contained in the underlying database and the confidence interval set by the officer.[290] A face identification search could potentially return hundreds of images from different sources. Is that unreasonable? What if an FRS returned hundreds of photos, but only from a traveler's border crossings? And as the hypothetical demonstrated, an FRT search might display only a small number of images that each directly reveal private information. Would that search be unreasonable? Such a line-drawing expedition will inevitably result in arbitrary decisions about what constitutes a reasonable search.[291]

---

286. Riley v. California, 573 U.S. 373, 398 (2014).

287. KERR, *Implementing* Carpenter, *supra* note 111 (manuscript at 28).

288. *Cf. Riley*, 573 U.S. at 399 (declining to adopt a rule permitting an officer to search for evidence relevant to the crime of arrest, officer safety, or an arrestee's identity because it would "impose few meaningful constraints on officers . . . and officers would not always be able to discern in advance what information would be found where"). For a helpful illustration of this issue, see KERR, *Implementing* Carpenter, *supra* note 111 (manuscript at 29–34).

289. The "mosaic theory" of the Fourth Amendment posits that even if certain information, on its own, is not entitled to a reasonable expectation of privacy, the aggregation of such information might trigger the Fourth Amendment. *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (analyzing the implications of a mosaic theory of the Fourth Amendment). In practice, this approach also poses difficult line-drawing questions. *See id.* at 343–50 (describing the "mosaic theory" as a "vague middle ground").

290. *See, e.g.*, *supra* notes 76–77 and accompanying text; Satisky, *supra* note 245 (describing a data set with "more than 2 million image frames of around 2,000 students from eight cameras placed around [Duke's] campus").

291. *Compare* 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

A bright-line standard, however, suffers from the risk of being overinclusive. The reasonable suspicion standard would apply to an entire database simply because it contains images that *could* reveal "the privacies of life."[292] But the images returned for any one individual might not actually reveal information that private. The reasonable suspicion standard would apply even if a database contained no images of a particular person. But as the Court stated in *Arizona v. Hicks*,[293] "[a] search is a search, even if it happens to disclose nothing but the bottom of a turntable."[294]

Though it is beyond the scope of this Note to suggest a full-fledged doctrine, a per se rule based on whether the source database contains any *protected* third-party information, such as the information in many commercial FRSs, might be the most administrable standard.[295] Under this approach, border officials would have clear guidance. If officials have reasonable suspicion of any crime related to the border exception's underlying purposes—such as drug trafficking—they could use a commercial FRS without fear that any derivative evidence will be tainted.[296] Courts would not need to split hairs evaluating when the information revealed became too intrusive. The court would need to evaluate only the merits of the officer's reasonable suspicion.[297] Lastly, travelers would have at least some assurance that border officers could not peer into their private lives without a measure of suspicion giving them a reason to do so.

In the end, classifying the use of facial identification at the border as a nonroutine search is not a cure-all. In many cases, border officials will satisfy the reasonable suspicion standard and gain a window into

search."), *with id.* at 2267 (Gorsuch, J., dissenting) ("Why seven days instead of ten or three or one?").

292. *See* KERR, *Implementing* Carpenter, *supra* note 111 (manuscript at 40).

293. Arizona v. Hicks, 480 U.S. 321 (1987).

294. *Id.* at 325.

295. *See* KERR, *Implementing* Carpenter, *supra* note 111 (manuscript at 40–42) ("The most administrable way to implement a test that treats digital surveillance as a search . . . is to treat the fruits of digital surveillance as categorically different.").

296. *See* Wong Sun v. United States, 371 U.S. 471, 484–85 (1963) (holding evidentiary fruits of a Fourth Amendment violation are, generally, inadmissible as "fruit of the poisonous tree"). Though this fear is likely diminished given the expansion of the good-faith exception to the exclusionary rule. *See, e.g.*, United States v. Aigbekaen, 943 F.3d 713, 725 (4th Cir. 2019) (affirming the suppression motion's denial based on the good-faith exception).

297. *Compare* United States v. Wanjiku, 919 F.3d 472, 487–89 (7th Cir. 2019) (concluding reasonable suspicion existed), *with Aigbekaen*, 943 F.3d at 723–24 (concluding officer lacked reasonable suspicion).

our lives. Albeit imperfect, the reasonable suspicion standard places at least some obstacle in the way of a "too permeating police surveillance" and safeguards "'the privacies of life' against '*arbitrary* power.'"[298] When applying "the blunt instrument of the Fourth Amendment," that sometimes is the best for which one can hope.[299]

CONCLUSION

Facial recognition technology is already being used to support enforcement operations at the border.[300] Considering the sheer amount of contraband seized at the border, it is only a matter of time before a scenario like the one described in this Note plays out in a federal courthouse.[301] When it does, federal courts should proceed carefully to avoid "uncritically extend[ing] existing precedents," which the Court warned against in *Carpenter* and *Riley*.[302] Unfortunately, the Fourth Amendment claims calling for limits on FRT at the border will probably only arise during suppression hearings involving "not very nice people."[303] Given FRT's obvious benefits, courts might be tempted to shoehorn the use of FRT into the routine border-search doctrine.

But consider again the San Ysidro Port of Entry. The *overwhelming* majority of the nearly one hundred thousand people who enter this country are not importing contraband or otherwise violating the law. Crossing the border, for many of them, is part of daily life. They travel between San Diego and Tijuana to work, study, and visit family. Countless others are merely passing through to pursue the American Dream in places like Salinas, California; Amarillo, Texas; and Nashville, Tennessee.[304] Whatever their connection to the border, each and every one of them is entitled to the Fourth Amendment's protection—regardless of the efficiency that modern technology offers. After all, the border should be a gateway, not an "authoritarian twilight zone."[305]

---

298. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (emphasis added).

299. Riley v. California, 573 U.S. 373, 408 (2014) (Alito, J., concurring in part).

300. Emily Birnbaum, *CBP Identifies over 100 'Imposters' out of 19 Million with Face Scans at Airports, Border*, HILL (June 14, 2019, 3:57 PM), https://thehill.com/policy/transportation/448643-cbp-says-it-has-caught-over-100-imposters-out-of-19-million-scanned-by [https://perma.cc/T4P4-DGJF].

301. In fiscal year 2020, CBP seized 533,708 pounds of illegal narcotics. *See CBP 2021 Statistics*, *supra* note 276.

302. *Carpenter*, 138 S. Ct. at 2222 (citing *Riley*, 573 U.S. at 386).

303. United States v. Rabinowitz, 339 U.S. 56, 69 (1950) (Frankfurter, J., dissenting).

304. A journey familiar to this Author's own parents.

305. United States v. Montoya de Hernandez, 473 U.S. 531, 564 (Brennan, J., dissenting).