"FACEPRINTS" AND THE FOURTH AMENDMENT: HOW THE FBI USES FACIAL RECOGNITION TECHNOLOGY TO CONDUCT UNLAWFUL SEARCHES

Elizabeth Snyder†

CONTENTS

INTRODUCTION

On September 15, 2014, the Federal Bureau of Investigation (FBI) announced the full operational capacity of its Next Generation Identification (NGI) system.[1] The system was designed to replace the Integrated Automated Fingerprint Identification System (IAFIS), which facilitated tenprint and latent fingerprint searches.[2] To broaden the scope

† J.D. Candidate, Syracuse University College of Law, 2018; M.A., University of Virginia, 2014; B.A., Bowdoin College, 2011.

1. Press Release, FBI, FBI Announces Full Operational Capability of the Next Generation Identification System (Sept. 15, 2014), https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-full-operational-capability-of-the-next-generation-identification-system.

2. *Next Generation Identification (NGI)*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (last visited Oct. 21, 2017).

of biometric data available for query, the NGI system added, among other capabilities, a facial recognition component, called the Interstate Photo System (IPS).[3] Most troublingly from a constitutional perspective, the IPS collects civil photographs provided for the purposes of employment background checks, among other innocuous submissions.[4] While the FBI maintains that these photos are not searched against photos in the criminal database, and law enforcement users cannot search these photos against probe photos, civil photos are nonetheless searched against the unsolved photo file, a category containing photos of unknown subjects.[5]

More invasive still, the FBI operates a unit, Facial Analysis, Comparison, and Evaluation (FACE) Services, that applies facial recognition technology to match photographic submissions against not only the NGI-IPS database, but also those databases maintained by external partners.[6] Unlike the NGI-IPS database, which contains mostly criminal photos, these external databases contain mostly civil photos, derived from visa applicant photos and states' driver's license photos, among other sources.[7]

Civilian subjects of a search conducted through either instrumentality are not only largely unaware that their images have been provided to the government, but they are also unaware that their images have been implicated in a criminal investigation.[8] In this way, the FBI's IPS and FACE programs offend the Fourth Amendment rights of the individuals pictorially present in the civil database against unreasonable searches. This Note will demonstrate that the FBI's practice of searching the images of incognizant citizens against the biometric data of known or suspected criminals constitutes an impermissible violation of the reasonable expectation of privacy, not in their image, but rather in their status. In this way, this Note represents a departure from the predominant discourse on the role of emerging FRT technology in the realm of privacy.

3. *Id.*

4. Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 431 (2014); Christopher De Lillo, Note, *Open Face: Striking the Balance Between Privacy and Security with the FBI's Next Generation Identification System*, 41 NOTRE DAME J. LEGIS. 264, 280 (2014).

5. Ernest J. Babcock, *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System*, FBI (Sept. 2015), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/interstate-photo-system [hereinafter Babcock I].

6. U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY 15 (2016).

7. *Id.*

8. De Lillo, *supra* note 4, at 281–82.

Whereas much scholarship has been devoted to the idea of remote biometric identification (RBI), of which FRT is a subset, as "something different in kind—not degree—to what has come before," rendering it necessarily incompatible with an antiquated Fourth Amendment jurisprudence, this Note will argue that it is the status of the individual, rather than the nature of the technology, which is different.[9] FRT, and IPS and FACE in particular, render a definitional conversion of the citizen from civilian to criminal, innocent to guilty. Civilian anonymity is not the analogue of criminal notoriety, and at the moment a query of the impermissibly-sourced civil database effects this change, the citizen's reasonable expectation in the definitional stability of his identity has been violated.

In reconceptualizing the expectation of privacy at issue, diverting focus from the right to privacy in one's image, which the Supreme Court is not prepared to recognize, to focus instead on the reasonable expectation of privacy in individual incorruption, itself a presumptive bedrock of the American criminal justice system, it may be possible that IPS and FACE might still run afoul of existing Fourth Amendment jurisprudence.[10]

To this end, this Note will proceed in five parts. Part I will examine the present capabilities and application of the IPS and FACE programs.

Part II will then undertake a discussion of what constitutes a search. In Part II, this Note will argue that the application of algorithms to measure, analyze, and compare the photograph of an unidentified individual against a database of civil photos, from which a yield of up to fifty results is retrieved, constitutes a search of the biometric components of that image, and must be so considered under existing Fourth Amendment case law.

Part III will then categorize this search as unreasonable, using the test articulated in Justice Harlan's concurrence in *Katz v. United States*, in which he predicated the constitutionality of a search, for Fourth Amendment purposes, on the reasonableness of that search, both from a subjective and an objective perspective.[11] Specifically, the IPS and FACE programs offend both the subjective expectation of privacy of the individuals depicted (notwithstanding third-party record doctrine concerns), and the objective expectation of privacy society maintains in the convertive appellations of guilt and innocence. In other words,

9. *See, e.g.*, Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 508 (2012).

10. *See, e.g.*, United States v. Dionisio, 410 U.S. 1, 14 (1973).

11. 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

citizens have a reasonable expectation of the definitional stability of their identity as civilian or criminal, an expectation to be free from governmental intrusion into the conversion of their legal status, absent any imputation of wrongdoing.

Part IV will therefore recast the seeming inapplicability of existing Fourth Amendment jurisprudence, the "pre-digital age" origination of which scholars criticize as necessarily unresponsive to changing technology, as counterintuitively inclusive of changing identities, if not technologies, to question whether the IPS program might not still fall under the current doctrinal framework.[12]

Having answered this question in the affirmative, Part V will conclude that the IPS and FACE programs violate the reasonable expectation of privacy in the convertive use of civil images. In this way, both programs fail to pass constitutional muster. It is not necessary to wait for the Court to undertake a consideration of FRT, for as the Court noted in *Katz*, "the Fourth Amendment protects people" and all of their iterations.[13]

I. How the IPS and FACE Systems Work

A. Facial Recognition Technology and "Faceprints"

The IPS is part of the FBI's NGI system, which employs FRT to create a "faceprint" that can be compared against other photos in the database.[14] This faceprint is the result of "five discrete steps."[15] For the purposes of IPS and FACE, the system must first acquire a digital image.[16] The operational software must then identify all faces in that image.[17] Next, "[c]omputer analysis must be done to map the spatial geometry of the face(s) in the image for distinguishing features to create a template of the face, known as a face print."[18] The system then compares this faceprint against other photos contained within the database.[19] Finally, a determination is made, either by automation or human verification, as to whether two images constitute a match.[20]

The FBI characterizes this faceprint as the result of two sequential

12. Brown, *supra* note 4, at 466.
13. *See Katz*, 389 U.S. at 351.
14. Brown, *supra* note 4, at 427–28; De Lillo, *supra* note 4, at 268.
15. De Lillo, *supra* note 4, at 267.
16. *Id.*
17. *Id.*
18. *Id.* at 267–68.
19. *Id.* at 268.
20. De Lillo, *supra* note 4, at 268.

processes: enrollment and matching.[21] During enrollment, facial recognition technology creates a faceprint for a known person, storing it with other biographical data in a corresponding database of known persons.[22] During matching, facial recognition technology creates a faceprint for a probe photo, meaning a photo of an unknown person, and searches it against the faceprints in the database of known persons.[23] When two photos are "sufficiently similar," they are returned as a match.[24] The matching process is automated, that is, photos are compared without initial human analysis, and a ranked list of candidates is returned to the requesting agency, whereupon further human analysis must be undertaken.[25]

B. How the FBI is Using "Faceprints"

The civil faceprints created by IPS and FACE show up in yields germane to criminal queries.[26] When a search is performed against the photo of an unidentified individual, anywhere from two to fifty photos will be returned.[27] Thus, the FBI is conducting "[s]earches for investigatory identification purposes," which implicate the records of millions of non-criminal citizens.[28]

In the case of IPS, there is a criminal identities and a civil identities database.[29] The criminal database contains photos submitted incident to lawful detention, arrest, and incarceration.[30] Conversely, the civil database is populated with photos submitted for non-criminal justice purposes, such as licensing, employment, security clearances, military service, volunteer service, and immigration benefits.[31] The criminal database accounts for over eighty percent of the photos.[32] According to the FBI, while civil faceprints are maintained in the civil database, civil photos are not searched against photos contained in the criminal identities database, and law enforcement agencies cannot search probe photos

21. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 6, at 5.
22. *Id.*
23. *Id.* at 5–6.
24. *Id.* at 6.
25. *Id.* at 6, 14.
26. De Lillo, *supra* note 4, at 280.
27. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 6, at 14 n.36.
28. De Lillo, *supra* note 4, at 280.
29. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 6, at 11.
30. *Id.*
31. *Id.*
32. *Id.*

against civil photos.[33] However, the FBI concedes that civil photos are searched against the unsolved photo file, where photos of unknown perpetrators of "felony crimes against persons" are stored.[34] Furthermore, civil photos depicting an individual with a criminal database identity will also be searched and returned to the requesting agency.[35]

FACE, on the other hand, implicates majority civil photos. There are currently 411.9 million photos available for facial recognition matching across all FACE databases.[36] Depending on the database, FACE Services can either directly query the database, or, alternatively, it may request a search of an external partner's database.[37] FACE Services received over 142,000 probe photos from August 2011 to December 2015, impelling 215,000 searches on various databases to identify a match.[38]

As the size of datasets increase, so too does the risk of false positives, and, at present, an accurate match will only be returned eighty-six percent of the time when a true match exists in the top fifty candidates retrieved using IPS.[39] Civil photos are therefore "submitted as part of searches completely apart from any criminal investigation, and are then stored for use beyond their initial purpose," all the while subjecting those depicted to the risk of false identification.[40]

II. THE FBI IS CONDUCTING A SEARCH WITHIN THE FOURTH AMENDMENT WHEN IT QUERIES IPS AND FACE

Nonetheless, the FBI contends that it is statutorily empowered by 18 U.S.C. § 3052, 28 U.S.C. §§ 533, 534, 42 U.S.C. § 3771, and 44 U.S.C. § 3301 to undertake searches under IPS and FACE, empowerments unimpeded by the Privacy Act of 1974 or the E-Government Act of 2002.[41] These arguments are unavailing in an American jurisprudential context where the Constitution is the supreme law of the land. Even assuming, arguendo, that the FBI is on solid statutory ground, if IPS and FACE violate the Constitution, they are necessarily invalid as a matter of

33. Babcock I, *supra* note 5.

34. *Id.*

35. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 6, at 48.

36. *Id.* tbl.4.

37. *Id.* at 48.

38. *Id.*

39. *Id.* at 27.

40. De Lillo, *supra* note 4, at 281.

41. Babcock I, *supra* note 5; Ernest J. Babcock, *Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit*, FBI (May 2015), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit [hereinafter Babcock II]; Donohue, *supra* note 9, at 463.

law.

Due to the recentness of IPS and FACE operational capability, there is no case law addressing the constitutionality of their employment of FRT. In fact, it is unlikely that the subjects of biometric analysis would know that their images had been analyzed, so as to bring the issue to bar, given that the majority of individuals depicted in civil photographs are neither alerted that their pictures have been provided to the federal government, nor that they have been queried against the photograph of an unidentified individual in a criminal investigation. For this reason, it is necessary to analyze the constitutionality of the FBI's use of IPS and FACE against the current Fourth Amendment jurisprudence that defines the contours of reasonable searches.

By this measure, the outlook would seem bleak for Fourth Amendment challenges to the IPS and FACE programs. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[42]

The limited number of courts that have considered the applicability of Fourth Amendment protections to photographs have largely declined to find a search where a camera captures that which an individual publishes to the public.[43] However, the search at issue here is of a qualitatively different nature than that previously considered by the courts.

While it is clear that the courts have not found a search where the surveilled object is visually accessible to the general public, the intrusion at issue here is not merely one of visual observation.[44] Rather, the search inheres in the creation and analysis of a faceprint against those of known and suspected criminals. The search occurs when the biometric data of a civilian subject is searched against the peaks and ridges of another

42. U.S. CONST. amend. IV.

43. *See, e.g.*, Mollett v. State, 939 P.2d 1, 11 (Okla. Crim. App. 1997) (declining to find a search where photographed body parts, namely defendant's wrist and chest, were "readily visible to the public"); United States v. Dionisio, 410 U.S. 1, 14 (1973) ("Like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. 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.").

44. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."); California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (finding no search where police officers' observations of curtilage were from public vantage point).

person's spatial geometry. The FBI is essentially searching the contours of a subject's face for criminality.

For this reason, the appropriate analytical framework is necessarily transactional. The violation is not the creation of the faceprint. Rather, the constitutional violation inheres in the comparison, in the searching for similarities, between a vessel of known and unknown criminality. The inquiry is bilateral—how are two dispositive pieces of information connected, and what are the constitutional protections afforded their interaction? This situation most frequently inheres in the case of the third-party record doctrine, which has been invoked by courts to circumvent privacy expectations for information voluntarily conveyed, here in the form of a photograph, to third parties.[45]

The third-party record doctrine presupposes that those who voluntarily convey information to a third party have no privacy interest in the fate of that data, even if the third party turns the information over to the government.[46] It was upon this basis that the Supreme Court in *Smith v. Maryland* found that the use of a pen register, which records all numbers dialed from a phone, does not constitute a search under the Fourth Amendment, not because the collection of dialed numbers is not a search for definitional purposes, but because the phone customer has no reasonable expectation of privacy in numbers dialed.[47] According to the Court, telephone users know that they must necessarily transmit the numbers they dial to the phone company, both so that their calls can be completed, and for billing purposes.[48] The Court particularly emphasizes the voluntariness of this conveyance as dispositive, believing that an individual who voluntarily conveys data to a third party has no reasonable expectation in the continued privacy of that data.[49]

It is upon this basis, that of voluntariness, that the lawfulness of a search under IPS and FACE depends. Under IPS, the FBI states that civil applicants whose photos have been entered into the system "will be provided with notice via a Privacy Act statement on a hard copy or electronic form," supplementing the notice it perceives to derive from publication of a Privacy Impact Assessment.[50] Attempting to further bolster its argument, the FBI suggests that while employers may require photos as a condition of employment, applicants may decline to provide

45. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

46. ARTHUR L. BERNEY, WILLIAM C. BANKS, STEPHEN DYCUS, PETER RAVEN-HANSEN & STEPHEN I. VLADECK, NATIONAL SECURITY LAW 707 (6th ed. 2016).

47. 442 U.S. at 745–46.

48. *Id.* at 742–43.

49. *Id.* at 743–44 (citing United States v. Miller, 425 U.S. 435, 442–43 (1976)).

50. Babcock I, *supra* note 5.

them, insinuating that applicants may instead apply for a position that does not require such photos.[51] This argument suffers from a positional infirmity: it is the conveyance to the third party, not the government, that must be understood as voluntary, and here it cannot be so.

Photos were conveyed to employers and state agencies in their discrete, final form. That is, they were conveyed as a finality, not as a potentiality. Unlike the numbers dialed in *Smith*, which were essential to the successful operation of the telephone, the object and the instrumentality of the search, the same agentic spin cannot be put on the photographs implicated here. There is no necessary transactional dimension of the photographs, and their operative performance is insular, necessary only to prove the identity of the depicted individual—not his twinning to an unknown probe. In this way, it becomes irrelevant for purposes of the third-party record doctrine that the FBI notified individuals of the potential searching of their photos—the photos were never voluntarily conveyed in the legal sense defined in *Smith v. Maryland*, vitiating any recourse to the third-party record doctrine.

Having therefore satisfied the definitional demands of searching, not to be undone by the third-party record doctrine, the analysis must then turn to this question of reasonableness, and the lack thereof, to subject the IPS and FACE programs to the dictates of Fourth Amendment protections (namely a warrant).

III. THE SEARCH AUTHORIZED UNDER IPS AND FACE IS UNREASONABLE UNDER THE *KATZ* STANDARD

In *Katz*, Justice Harlan enunciated the test in a concurrence that would come to define the constitutionality of searches under the Fourth Amendment.[52] According to Harlan, "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[53] As to the subjective requirement, owners of a civil photo in the IPS and FACE databases have a reasonable, subjective expectation of privacy in the circumscription of its usage. In other words, citizens who submit images for driver's licenses, passports, and employment checks have a reasonable expectation that these photos will be used for that purpose, and that purpose only.

As to the objective requirement, society is prepared to accept as reasonable the individual expectation to privacy in the non-criminal

51. *Id.*

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

53. *Id.*

justice use of his photo. Scholars have found protections for faceprints from analogizing existing protections for bodily integrity and anonymity, and from a so-called "shadow majority" in *United States v. Jones*.[54] In *Jones*, though a search using a GPS tracking device was narrowly invalidated as a physical trespass, five Justices are nonetheless understood to have applied the "mosaic theory," where the sum of the search is more invasive than its parts.[55]

As a result, FBI searching under IPS and FACE is unreasonable, and therefore unlawful, barring procurement of a warrant.

A. The FBI's Use of Facial Recognition Technology Violates Subjective Expectations of Privacy

Individuals depicted in civil photographs in the IPS and FACE databases have an objective expectation of privacy in the non-criminal justice use of their photos. In the case of IPS, this expectation is bolstered by certain operational features exposed by the Electronic Frontier Foundation (EFF). The EFF sued the FBI under the Freedom of Information Act (FOIA) in order to gain information on the NGI.[56] As part of the records received from that lawsuit, the EFF learned that, in addition to the 46 million criminal images and 4.3 million civil images contained in the database, up to 1 million images derive from categories for which the FBI has provided no explanation: 750,000 images from a "Special Population Cognizant" (SPC) category, and 215,000 images from "New Repositories."[57]

If individual citizens do not know what these categories represent, let alone how their data points are sourced, then they must necessarily have a reasonable expectation that participation in ordinary civilian life will preclude their inclusion in this amorphous aberrancy. The FBI hinged its initial claim to legality on the fact that applicants included in the IPS database were notified of their inclusion; yet, the FBI ventures no such claim for these shadow images. However consensually these images may have been obtained, their subsequent searching against a criminal database "would re-create the conditions of a consensual encounter—

54. *See, e.g.*, De Lillo, *supra* note 4, at 282; Donohue, *supra* note 9, at 506–07.

55. *See, e.g.*, De Lillo, *supra* note 4, at 282; Brown, *supra* note 4, at 456; Donohue, *supra* note 9, at 506–07.

56. Jennifer Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, ELECTRONIC FRONTIER FOUND. (Apr. 14, 2014), https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year.

57. *Id.*

without carrying any of the consensuality otherwise involved."[58]

Under IPS, the FBI states that civil applicants whose photos have been entered into the system "will be provided with notice via a Privacy Act statement on a hard copy or electronic form," supplementing the notice ostensibly provided by the fact of publication.[59] The FBI suggests that while employers may require photos as a condition of employment, applicants may seek alternative employment at a workplace that declines to solicit such photos.[60]

This argument is undermined on two fronts: first, though the FBI launched the NGI-IPS pilot in December 2011, this privacy impact assessment was not completed until September 2015.[61] Second, while applicants are provided with a notice following their inclusion in IPS, this notice is issued after the photo has already been integrated into the civil identities database, and potentially searched against criminal photos. The notice becomes a post hoc balm that cannot put the constitutional rabbit back in the hat. The search, and thus the violation, has already occurred.

Even assuming, arguendo, that despite the seemingly reasonable expectation that conveyance of photos to departments of motor vehicles and places of employment does not constitute a voluntary accession to the criminal investigatory use of those same photos in perpetuity, expectations of privacy are nonetheless vitiated under IPS by a system of record notice published in the Federal Register, notices issued pursuant to a Privacy Act, and publication of a privacy impact assessment,[62] no such argument can be made on behalf of FACE. The civil photos contained in the databases accessible by FACE were submitted without any criminal import, and it is unreasonable to believe that an applicant for a driver's license would expect his photo to be provided to the federal government for biometric imaging that would compare the distance between his eyes in determination of current or future criminality.[63] In its Privacy Impact Assessment for the FACE program, the FBI concedes that individuals are not notified of the collection of their photos, and are not given an opportunity to consent to this collection.[64] The FBI only provides that notice was issued pursuant to a systems of record notice published in the Federal Register.[65] However, the notice contains no

58. Donohue, *supra* note 9, at 533.
59. Babcock I, *supra* note 5.
60. *Id.*
61. *Id.*; U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 6, at 21.
62. Babcock I, *supra* note 5.
63. *See* Lynch, *supra* note 56.
64. Babcock II, *supra* note 41.
65. *Id.*

reference to FACE, matching, biometrics, or facial recognition technology, undermining the degree to which the notice truly provides any opportunity to consent to the searches being conducted by the FBI.[66]

Additionally, individual citizens have a reasonable expectation of privacy in their inculpability, where the government has not enunciated the scope and capability of its law enforcement programs. Here, scholars contend, "[t]he absence of individualized suspicion in particular changes the context."[67] These "photos were not obtained in connection with any criminal suspicion, investigation, search, arrest, or processing," vitiating any "cognizable law-enforcement interest" where the photos merely represent "a potential for future investigatory use in connection with identifying subjects."[68] Citizens, therefore, have a reasonable expectation of freedom from governmental intrusion when that intrusion has been neither enunciated, nor conceptualized. To contend otherwise would be to hold citizens hostage to the vagaries of a government which may or may not actualize, at the expense of constitutional rights under the Fourth Amendment.

While it is true that the few cases that have arisen under the NGI and IPS are mere requests for information under FOIA, and therefore do not contend with the reasonableness of searches conducted thereunder, the *Katz* analysis, which finds a reasonable expectation of privacy in conversations, recorded for a limited purpose and duration, via an articulable medium (wiretapping),[69] would analogically support a finding here of a subjective expectation of privacy. The Court noted that "the surveillance was limited, both in scope and in duration, to the specific purpose of establishing the contents of the petitioner's unlawful telephonic communications."[70] It went on to say, "[t]he agents confined their surveillance to the brief periods during which he used the telephone booth, and they took great care to overhear only the conversations of the petitioner himself."[71] And yet, notwithstanding all the safeguards to Katz's privacy interest in his telephone calls, the Court recognized a

66. *See generally* Privacy Act of 1974; Notice of Modified Systems of Records, 63 Fed. Reg. 8659 (Feb. 20, 1998); Privacy Act of 1974; System of Records, 66 Fed. Reg. 33558 (June 22, 2001); Privacy Act of 1974; System of Records, 72 Fed. Reg. 3410 (Jan. 25, 2007) (revealing that neither the original notice published in the Federal Register, nor updates issued in 2001 and 2007, contain language referencing FACE, matching, biometrics, or facial recognition technology).

67. Donohue, *supra* note 9, at 532.

68. De Lillo, *supra* note 4, at 282.

69. *E.g.*, Elec. Privacy Info. Ctr. v. FBI, 72 F. Supp. 3d 338, 341 (D.C. Cir. 2014); Katz v. United States, 389 U.S. 347, 354 (1967).

70. *Katz*, 389 U.S. at 354.

71. *Id.*

reasonable expectation of privacy that had been infringed upon in violation of the Fourth Amendment.[72]

To analogize, if the Court found a reasonable expectation of privacy in the face of governmental intrusions narrowly tailored to detection of a circumscribed amount of data from a single individual, then surely a court hearing a challenge to the IPS must also find a reasonable expectation of privacy when a vast and undefined program aims to collect indeterminate information from millions of people. It is in this way that the subjective expectation of privacy informs and augments the objective expectation of privacy identified by Harlan in the second prong of the *Katz* test, whereby society must be prepared to accept the expectations of the individual as reasonable.

B. The FBI's Use of Facial Recognition Technology Violates Objective Expectations of Privacy

The second prong of the *Katz* reasonableness standard dictates not only that the individual subjected to a government intrusion understand that behavior as violative of his reasonable expectation of privacy, but society must also validate the collective reasonableness of his evaluation.[73] In other words, society as a whole must agree with an aggrieved individual that the government searched him despite his expectation to be reasonably free from intrusion in the relevant behavior. Scholars fear this formulation sets the IPS and FACE up for victory under current Fourth Amendment jurisprudence, which does not recognize a privacy interest in one's image.[74]

The seminal Supreme Court case on this point is *United States v. Dionisio*, which though ultimately concerned with voice exemplars, also broached the reasonableness of expectations to privacy in one's image.[75] In *Dionisio*, the defendant was subpoenaed to provide a voice recording for comparison with recorded conversations germane to violations of criminal gambling statutes.[76] The defendant argued that the directive to record his voice violated his Fourth Amendment rights.[77] However, the Court found that expectations of privacy as regards physical characteristics, such as a voice (but also facial characteristics), are outside

72. *Id.* at 359.
73. *Id.* at 361 (Harlan, J., concurring).
74. *See, e.g.*, Brown, *supra* note 4, at 441–42; De Lillo, *supra* note 4, at 282.
75. 410 U.S. 1, 14 (1973).
76. *Id.* at 2–3.
77. *Id.* at 13–14.

the reasonable interaction of the individual with the greater world.[78] According to the Court, "[n]o 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."[79] The Court instead analogized voice recordings to fingerprinting, which "involves none of the probing into an individual's private life and thoughts that marks an interrogation or search."[80]

It is this caveat that provides hope for constitutional challenges to the IPS and FACE programs under the existing Fourth Amendment framework. This is because a faceprint is fundamentally different than a face.[81] Some commentators have analogized a faceprint to an intrusive bodily search, more in the vein of blood draws and bodily searches than flash photography.[82] For example, Christopher De Lillo argues, in his evaluation of the constitutionality of the NGI system, that "[w]hile anyone walking down the street can subjectively analyze a stranger's face with their brain, standing there with a camera and taking digital images of them to create a mathematical representation of their face is another story entirely."[83] He continues, "[o]ne can even analogize making the face print to surgically opening a person to view their bone structure underneath the skin, since that is what facial recognition software can essentially do: create a digital wireframe, or skeleton, of a person's face."[84]

Others take a different tack, analogizing the protections for anonymity contained within existing First Amendment jurisprudence to Fourth Amendment situations, where "anonymity implies a freedom from being recognized—versus just being seen."[85] Courts regularly protect anonymous speech.[86] For this reason, scholars like Kimberly Brown have argued that the Court's treatment of anonymity draws "a distinction between mere observance of 'physical identities' and recognition," with only the latter garnering constitutional protections.[87] According to Brown, '"a surrender of anonymity' takes place when the face is linked

78. *Id.* at 14.

79. *Id.*

80. *Dionisio*, 410 U.S. at 15 (quoting Davis v. Mississippi, 394 U.S. 721, 727 (1969)).

81. De Lillo, *supra* note 4, at 282.

82. *Id.*

83. *Id.*

84. *Id.*

85. Brown, *supra* note 4, at 457.

86. *See, e.g.*, Talley v. California, 362 U.S. 60, 60–61, 65 (1960) (voiding a city ordinance requiring the names and addresses of the authors of handbills to be printed on them).

87. Brown, *supra* note 4, at 457–58.

to other identifying information, such as a name on a pamphlet."[88] Brown believes that "although a faceprint algorithm in and of itself is just a numerical record of something that has already been made public, the correlation of that data with other information for predictive surveillance is altogether different."[89] "The data," she continues, "may not even explicitly seem like personal information, but with big-data processes it can easily be traced back to the individual it refers to. Or intimate details about a person's life can be deduced."[90]

Thus where De Lillo attempts to analogize FRT to a physical probing of the individual, and Brown a more ideological intrusion, both nonetheless attempt to fit new technological challenges into the existing contours of Fourth Amendment jurisprudence in a seeming episode of *Jones* redux. In *United States v. Jones*, the Court was asked to determine the constitutionality of government GPS monitoring of a suspect's vehicle following the expiration of a warrant authorizing the activity.[91] Ultimately, the Court decided the case on narrow grounds, holding that the government perpetrated a physical trespass of Jones' property, and in so doing violated his Fourth Amendment rights.[92] However, the case is famous for its concurrence by Justice Sotomayor, wherein she questioned the ability of existing Fourth Amendment jurisprudence to respond to evolving technological realities.[93] According to Justice Sotomayor, "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[94] "The net result," she says, "is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[95] She concludes, "I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements," questioning the responsiveness of the Court's Fourth Amendment jurisprudence to ever-changing technologies.[96]

88. *Id.* at 458.

89. *Id.* at 459.

90. *Id.*

91. 565 U.S. 400, 402–03 (2012).

92. *Id.* at 404–05.

93. *Id.* at 415–18 (Sotomayor, J., concurring).

94. *Id.* at 416.

95. *Id.* (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated*, 565 U.S. 1189 (2012)).

96. *Jones*, 565 U.S. at 416.

Justice Sotomayor and her disciples therefore question the applicability of Fourth Amendment protections against unreasonable searches in the digital age.[97] These scholars maintain that "[a]lthough pre-digital-age Fourth Amendment case law appears to paint FRT surveillance into a doctrinal corner, in the right case the Supreme Court may well find constitutional limits on surveillance conducted with cutting-edge technology like FRT and publicly available data."[98] A reconceptualization of the relevant expectation of privacy, however, would recast the dispositive change as one of identity, as opposed to one of technology. In this way, existing Fourth Amendment jurisprudence is responsive to the intrusions of the IPS and FACE programs, rendering a finding of constitutional infirmity present, as opposed to future.

IV. IDENTITY, NOT TECHNOLOGY, DRIVES THE FOURTH AMENDMENT ANALYSIS OF THE IPS AND FACE PROGRAMS

The key to a Fourth Amendment analysis of the IPS and FACE programs resides in the observation by the *Katz* Court that "the Fourth Amendment protects people, not places."[99] It is thus those intrusions against the person to which the protections of the Fourth Amendment must be directed. It is the reasonable expectation of privacy, both of the individual and of the society to which he belongs, in the presumption of his innocence, that is, in his definitional identity, that finds protection under the auspices of existing Fourth Amendment doctrine. It is the very stability of civilian identity that lends stability to a jurisprudence that would otherwise exist in a state of constant flux, forever susceptible to the caprice of technological evolution.

This is the first point of importance inclining a reevaluation of the analytical framework to which scholars must subject the IPS program in particular, and FRT in general. Technology is forever changing. To predicate the protections offered victims of government trespass to privacy rights upon ever-evolving technological configurations would be to undermine the principle of stare decisis upon which the American legal system hinges. Same facts, same result renders. This is the touchstone of predictability upon which the American legal system depends. And yet, to operate under the escapeways advocated by Fourth Amendment scholars would be to render constitutional protections unique to the technology involved, with attendant unpredictable results.

Personhood, however, is stable, and while personal identity may not

97. Brown, *supra* note 4, at 457; *Jones*, 565 U.S. at 417–18 (Sotomayor, J., concurring).

98. Brown, *supra* note 4, at 455.

99. Katz v. United States, 389 U.S. 347, 351 (1967).

be inert, the collective civilian status creates a barometer by which to achieve a predictable expectation of cultural reasonableness. In other words, the subjective expectation of privacy in any Fourth Amendment challenge is easy to satisfy. So long as a person believes that his right to privacy has been impermissibly intruded upon, the subjective prong of the *Katz* test is satisfied. The viability of the claim comes down to the objective expectation of privacy—that is, whether society is ready to validate that individual.

Unlike the other schools of thought, detailed above, that would find this right in a caveated right to one's image, or alternatively, in a transpollination of First Amendment protections for anonymity, the analytical locus of this Note is the person, rather than the technology. To borrow from evidentiary law, the search of civil photos executed by the IPS system can be conceptualized as a kind of verbal act, a fictive transaction with legal significance, essentially effectuating the conversion of the queried individual from civilian to criminal.[100]

According to De Lillo, the civil photos contained in the IPS database "were not obtained in connection with any criminal suspicion, investigation, search, arrest, or processing."[101] These photos, therefore, defy any "cognizable law-enforcement interest."[102] "The photos," he says, "only represent a potential for future investigatory use in connection with identifying subjects . . . ."[103] For this reason, "[a] person's photo could be used in countless searches of the database, and included in countless results lists, most likely without them ever knowing."[104] He concludes, "[t]his would all be done without any probable cause as to their involvement in an alleged crime . . . ."[105] The EFF puts the pieces together to reveal that "[t]his means that many people will be presented as suspects for crimes they didn't commit. This is not how our system of justice was designed and should not be a system that Americans tacitly consent to move towards."[106]

The result is an unwitting conversion of civilian identity. Civilian becomes criminal. Innocent becomes guilty. The presumptions of the criminal justice system are necessarily inverted in a way that imperils the structural integrity of the law itself. And yet, this Note does not seek to

100. *See* DANIEL J. CAPRA, GRAHAM C. LILLY & STEPHEN A. SALTZBURG, PRINCIPLES OF EVIDENCE 155 (7th ed. 2006).

101. De Lillo, *supra* note 4, at 282.

102. *Id.* at 282.

103. *Id.*

104. *Id.*

105. *Id.*

106. Lynch, *supra* note 56.

argue that identity must necessarily remain static, so as to cripple any fluidity between the statuses of culpability and inculpability. Every instance of guilt is preceded by one of innocence, such that this theory recognizes the potential ephemerality of identity. The crux of this alternative theory of constitutional interpretation is that this ephemerality inhabits the zone of privacy unique to the citizenry, as opposed to the government.

To elaborate, every individual has a reasonable expectation of privacy in the determination of his own definitional appellation. Again, this is not to say that the state does not have legitimate law enforcement interest in the exercise of its police powers, including, but not limited to, preventive action. Rather, the argument here is that the convertive operation, whereby a citizen's face is biometrically analyzed, measured, and matched—the process by which he is criminalized without warning and without probable cause—changes his definitional identity in violation of his reasonable expectation of privacy in his autonomy. It is therefore within the reasonable right of the individual to determine whether and when to effectuate a change in his identity. When an individual commits a crime, it is at that moment that he effects this change. In the case of the IPS, and FRT more generally, however, the government makes this choice for the individual. At the moment the FBI, or another such agency, queries an image, in the absence of probable cause, the government changes the identity of the searched. The subject of the search has no agential role in this process, and it is the intrusion upon the reasonable right to be free from governmental condemnation that must be addressed by Fourth Amendment protections. In operating the IPS system, the government is effecting an unreasonable search against our potentiality, our future criminality, as yet nascent, and nonetheless engineered and mined in flagrant disregard of the subjective and objective expectation of freedom from prescribed personality.

This theory is admittedly susceptible to challenges of excessive abstraction. And yet, an appeal to the reasonableness standard of the *Katz* test proves its workability. To recall, the *Katz* test has both a subjective and an objective prong. Here, the subjective prong is satisfied in logical presumption of most individuals' desire to be viewed as free of wrongdoing, particularly in the case where it was their benign activity that exposed them to censure. However, the more difficult to satisfy objective test also finds a home in this person-centric approach to the Fourth Amendment. This is because the proof of society's willingness to accept the individual expectation against intrusion into personal probabilities is manifest in the charter of our criminal justice system. The American criminal justice system is centered around the presumption of

innocent until proven guilty.[107] This formulation is inverted in the yield results page of the IPS and FACE programs, and it is this central tenet of our legal system that might very well sustain a finding of unreasonableness should a plaintiff find occasion to challenge the programs on Fourth Amendment grounds.

V. FOURTH AMENDMENT CONSEQUENCES OF IPS, FACE, AND FRT

This Note will conclude with a contemplation of the consequences of future engagement with the IPS and FACE programs, and FRT, in the Fourth Amendment context. First, it cannot be understated that it will be very difficult to bring a challenge of this nature up through the courts. As the EFF discovered in its FOIA suit against the FBI, the NGI program "will allow law enforcement at all levels to search non-criminal and criminal face records at the same time."[108] To recall, the database is "shared with other federal agencies and with the approximately 18,000 tribal, state and local law enforcement agencies across the United States."[109] The result is innumerable opportunities for the querying of civilian photographs, of which it is unlikely (barring prosecution) that any implicated will ever become aware.

Furthermore, it must be noted that in addition to the definitional damage perpetrated against unwitting civilians every time their images are searched, there are other dangers associated with the proliferation of FRT. Kimberly Brown identifies three main dangers.[110] Specifically, she cautions that "ongoing identification and tracking can adversely influence behavior."[111] According to Brown, "[p]eople involuntarily experience 'self-censorship and inhibition' in response to the feeling of being watched."[112] She next notes that "dragnet-style monitoring can cause emotional harm."[113] "Living with constant monitoring," she says, "is stressful, inhibiting the subject's ability to relax and negatively affecting social relationships."[114] Finally, she states, "constant surveillance through modern technologies reduces accountability for those who use the data to make decisions that affect the people they are monitoring."[115] Brown extrapolates to argue that "[t]he individuals whose

107. *See* U.S. CONST. amends. V, VI.
108. Lynch, *supra* note 56.
109. *Id.*
110. Brown, *supra* note 4, at 434.
111. *Id.*
112. *Id.* at 434–35.
113. *Id.* at 435.
114. *Id.*
115. Brown, *supra* note 4, at 435.

images are captured do not know how their data is being used and have no ability to control the manipulation of their faceprints, even though the connections that are made reveal new facts that the subjects did not knowingly disclose."[116] The result is that "FRT enhances users' capacity to identify and track individuals' propensity to take particular actions, which stands in tension with the common law presumption of innocence embodied in the Due Process Clause of the Fifth and Fourteenth Amendments."[117] Unlike the author of this Note, however, Brown ultimately distills the aforementioned conclusions to determine that "prevailing constitutional doctrine does not account for the use of technology to identify, track, and predict the behavior of a subject using an anonymous public image and big data correlations."[118]

This Note instead argues that prevailing constitutional doctrine does and can account for the use of novel technologies in data acquisition, but that it is the focus on the nature of the person, and not of the technology, which triggers Fourth Amendment protections. Again, any protections deriving from this alternative conception of existing Fourth Amendment jurisprudence will be hard-won given the difficulty of bringing suit under IPS or FACE. However, "the FBI and Congress have thus far failed to enact meaningful restrictions on what types of data can be submitted to the system, who can access the data, and how the data can be used."[119] In fact, "[w]hile federal legislators have become aware of the issue of FRT use and the need for legislative action, no laws have yet addressed the use of FRT directly."[120] Rather, "[i]t is in this legislative lag period that the FBI, as well as the commercial world, continues to operate using FRT with relatively few limits."[121]

Any attempt to restrict the FBI's unrestricted assignments of criminality would thus benefit from, if not require, the intervention of the legislature. One remedial step might include a statutory requirement that the FBI inform those submitting photos of the uses to which they will be put in the IPS database.[122] Amendment of 28 U.S.C. § 534, the statute under which the Attorney General claims authority to collect identification records, and therefore operate programs such as the IPS, to more precisely define what types of information may be collected, is

116. *Id.* at 436.
117. *Id.*
118. *Id.*
119. Lynch, *supra* note 56.
120. De Lillo, *supra* note 4, at 278.
121. *Id.*
122. *See id.* at 289.

another option.[123]

CONCLUSION

In any case, the cause is not hopeless. While the FBI's current application of facial recognition technology runs afoul of the Fourth Amendment, the Constitution is not powerless to remedy this and other technological transgressions. Unlike those scholars who bemoan the inability of the Fourth Amendment to deal with unreasonable searches occasioned by the emergence of novel technologies, such as FRT, this Author does not believe that we must necessarily wait for the pronouncement of new case law. Sotomayor's world in *Jones* is a possibility, but not an inevitability.

123. *Id.*