OPEN FACE: STRIKING THE BALANCE BETWEEN PRIVACY AND SECURITY WITH THE FBI'S NEXT GENERATION IDENTIFICATION SYSTEM

Notre Dame Journal of Legislation

By Christopher De Lillo†

INTRODUCTION

Privacy in the United States has never been an explicit general right for every citizen.[1] Federal grants of privacy protection exist for specific instances or areas, but generally have been left to the province of the States.[2] Some states, but not all, have general privacy laws granting citizens privacy rights beyond the scope of content-specific legislation.[3] Thus, the privacy law regime in the United States is best characterized as a patchwork: rights or protections exist in numerous areas without much to connect those areas together as an interlocking protective framework for the national citizenry.

The European Union, on the other hand, offers one example of an overarching privacy framework. Its Data Protection Directive (the Directive) offers EU citizens comprehensive transparency and protections in the handling of consumer and personal data.[4] It confers general privacy rights and outlines responsibilities for data

† Candidate for Juris Doctor, University of Notre Dame Law School, 2016; B.B.A., University of Notre Dame, 2013. I would like to thank Professor Woodrow Hartzog for his assistance in the development of this note, Professor Leslie D'Arcy Callahan for her help in the editing process, the men of Marilyn M. Keough Hall for their support, and the members of the Journal of Legislation for their guidance and feedback. Lastly, I want to thank my family, especially: Kevin, Kathy, Michelle, and Brandon for their patience, support, and love.

1. The U.S. Supreme Court has interpreted the Constitution to grant individuals "zones of privacy." Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (outlining the "zones of privacy" created by "penumbras," i.e. shadows, in the First, Third, Fourth, and Fifth Amendments).

2. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936. *See also*, Katz v. United States, 389 U.S. 347 (1967). In *Katz*, the Court held that the Fourth Amendment is not "a general constitutional 'right to privacy.'" *Id*. at 350. However, "[o]ther provisions of the Constitution protect personal privacy from . . . forms of governmental invasion. But the protection of a person's general right to privacy—his right to be let alone by other people—is like the protection of his property and of his very life, left largely to the law of the individual States." *Id.* at 350-51 (citations omitted). For specific areas, the Court offered such examples as the First Amendment (in the protection of privacy in association) and the Third Amendment (in the protection of the privacy of the home from being forced to quarter government soldiers). *Id.* at 350 n. 5 (citation omitted).

3. *See, e.g.*, CAL. CONST., art. I, §1.

4. *See* Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. L 28131 [Hereinafter Directive on Protection of Personal Data]. While the Directive was passed by the European Parliament, it lacks the force of law in each individual European Union member state, and is thus more advisory or akin to a Uniform Law in the United States. Subsequent statutes enacted in individual Member

handlers.[5] While offering protections, it also allows for efficient and necessary utilization of data by various entities, including the government and law enforcement.[6]

The various forms of content-specific privacy protections are typically only applicable to entities dealing in commercial data. Furthermore, the reality is that increased legislative protections inevitably lag behind abuses of citizen privacy. In the case of the United States, it might take Congress years to respond to a potential invasion of citizen privacy, and it could take even longer to deliberate, draft and agree on an appropriate bill to provide protection in that specific area. In the meantime, real threats to privacy are allowed to flourish in the spaces between the pockets of protections in the Nation's patchwork privacy regime. Today, law enforcement use of easily accessible and searchable facial recognition technology (FRT) in databases and in-person identification is such a threat. While the use of video surveillance may be constitutional, the creation and utilization of a massive facial recognition and biometric database by the Federal Bureau of Investigation (FBI), which compares innocent citizens to suspected criminals each time there is an investigation, implicates different privacy concerns than the mere use of video in surveillance operations or similar searches for fingerprints.

On September 15, 2014, the FBI announced that its Next Generation Identification (NGI) program was fully operational in more than 18,000 Bureau offices around the country.[7] One component of the NGI is the new Interstate Photo System (IPS), which incorporates facial recognition and search capabilities into a new and upgraded photo database.[8] This photo database will incorporate photos from several different sources, including criminal mug shot photos, as well as photos from non-criminal sources such as employment records and background check databases.[9] The IPS will also provide for more photo submissions per each individual profile.[10] These aspects of the new programs have raised concerns and drawn criticism from privacy advocates.[11]

Facial recognition is just one of the many new technologies in a larger category known as biometric identification. Facial recognition and other methods of biometric identification, such as iris recognition, are highly accurate and can therefore supplement or even replace existing identification methods, such as fingerprinting. The low probability of someone being able to alter his or her facial features or eye-

States embodying the Directive have brought its principles into law enforceable in each state.

5. *Id.* art. 1 & 2.

6. *Id.*

7. Press Release, Fed. Bureau of Investigation, FBI Announces Full Operational Capability Of The Next Generation Sys. (Sept. 15, 2014), *available at* http://www.fbi.gov/news/pressrel/press-releases/fbi-announces-full-operational-capability-of-the-next-generation-identification-system.

8. *Id.*

9. Russell Brandom, *The FBI just finished building its facial recognition system*, THE VERGE (Sept. 15, 2014, 10:51 AM), http://www.theverge.com/2014/9/15/6152185/the-fbi-just-finished-building-its-facial-recognition-system.

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

11. *Id.*

ball to fool facial or iris recognition software makes biometric identification an attractive tool for law enforcement to use in identification of suspects.

The FBI's NGI program raises privacy concerns in its incorporation of non-criminal photos for its facial recognition database, and the existing privacy regimes in the United States do not provide individuals with adequate, if any, protection. Federal law requires the Attorney General to collect and maintain identification and criminal records.[12] The FBI cites 28 U.S.C. § 534 as the basis for its authority to implement and operate the NGI, IPS, and related programs.[13] Rather than granting the FBI limited power, § 534 is broad enough to encompass any piece of information that relates to identification records, which presents considerable potential for abuse of the scope or intention of the statute, the public trust and individual liberties.[14]

Section I of this note gives an overview of the technology and process involved in biometrics generally and facial recognition specifically. Additionally, it discusses the current landscape of case law and the applicable literature. Section II outlines the development of the NGI system and its IPS component. Section III analyzes the current privacy legal regime in the United States, at both the state and federal level. Section IV argues that individuals have a right to privacy, at least in some sense, in their face prints for non-criminal photo submissions. Section V discusses the European Union's privacy protections in the Data Protection Directive. Section VI argues that Congress should act and amend 28 U.S.C. § 534 to limit the nature of the information the FBI can collect for identification, limit its use of the information, and incorporate principles from the EU Directive.

I. BACKGROUND

A. Facial Recognition Technology: The New Thumbprint

Biometrics is defined as "the measurement and analysis of unique physical or behavioral characteristics (as fingerprint or voice patterns)[,] especially as a means of verifying identity."[15] Alternatively, biometrics is the field of science studying the utilization of "physiological and behavioral characteristics" for verification or identification.[16] In this way, biometrics can be broken down into two different types:

12. 28 U.S.C. § 534(a) ("The Attorney General shall . . .").

13. Privacy Impact Assessment, Fed. Bureau of Investigation, Privacy Impact Assessment for the Next Generation (NGI) Interstate Photo System (2008), http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system. Assessments are typically released by the FBI in response to new programs or technology to advise the public as to the specific nature and impact of the program, and what measures the FBI is considering or using to minimize the privacy impact of the program.

14. 28 U.S.C. § 534(a)(2) & (3). The statute contains the language "preserve any information which would assist" in connection with the identification of deceased or missing persons, which can be interpreted quite broadly.

15. WEBSTER'S NEW TWENTIETH CENTURY DICTIONARY 184 (2d ed. 1983).

16. Robin Feldman, *Considerations on the Emerging Implementation of Biometric Technology*, 25 HASTINGS COMM. & ENT. L.J. 653, 654 (2003). For the purposes of this note, "biometrics" will be discussed as the

identification and verification. Identification is the use of physiological or behavioral characteristics to identify an unknown person.[17] Verification is the use of characteristics to verify a known person's identity.[18]

Biometric identification has been used in various forms for over a century. Early in the twentieth century, state and federal prison systems in the United States began using fingerprinting techniques to identify, and maintain profiles for, prison inmates.[19] Additionally, the New York Police Department adopted fingerprinting to aid in investigations and criminal records.[20] Fingerprinting was quickly adopted by the military for use in identification records of soldiers and sailors.[21] As the twentieth century continued, fingerprinting became the standard for identifying individuals, or verifying their identity, and automated fingerprint matching followed with technological advances, gaining widespread use.[22] What began as ink and paper fingerprinting has transformed into the subject placing his or her finger on a digital scanner, which uploads the scanned fingerprints into an electronic database. Fingerprinting makes up about half of the biometric identification technology market.[23] In the last two decades, new biometric identification technologies have emerged, including facial recognition.

Facial recognition technology consists of: "(1) a mechanism comprised of sensors that capture the facial biometric data from the subject; (2) a mechanism to extract identifying features from the captured facial image; and (3) a matching methodology that processes and compares the presented facial data to reference data in order to make a recognition decision."[24] Breaking it down more technically, facial recognition involves five discrete steps.[25] First, the system must acquire a digital image.[26] This can be done with a still photograph or an image from a video, or in some cases even with live video.[27] Next, the software works to detect any and all faces in that image.[28] This kind of software capability is already in use commercially, most notably by Facebook.[29] Computer analysis must be done to map the spatial

utilization of physiological characteristics for verification or identification.

17. *Id.* at 655-56.

18. *Id.*

19. Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 418 (2012).

20. *Id.*

21. *Id.* at 418-19.

22. *Id.* at 419. The first national repository was actually created in 1924, which collected and stored fingerprint records.

23. WILLIAM SLOAN COATS ET AL., THE PRACTITIONER'S GUIDE TO BIOMETRICS 4 (William Sloan Coats ed., 2007).

24. Mohammed Osman & Edward Imwinkelried, *Facial Recognition Systems*, 50 CRIM. LAW BULLETIN 3, art. 11 at I (2014).

25. *Id.* at IV.

26. *Id.*

27. *Id.*

28. *Id.*

29. Russell Brandom, *Why Facebook is beating the FBI at facial recognition*, THE VERGE (July 7, 2014, 3:17 AM), http://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition. Facebook has already been using a system that suggests possible matches for "tagging" friends in

geometry of the face(s) in the image for distinguishing features to create a template of the face, known as a face print.[30] The face print consists of measuring the size, angle, and distance between facial features.[31] Next, the software compares the face print with other templates in the database of known images.[32] It generates scores for how closely the face print matches the others in the database. Lastly, there is a decision about whether the scores are high enough to be considered a "match."[33] This last step of deciding whether the "match" scores meet a pre-determined threshold can be done via automation software, or with a human operator reviewing the results.[34]

Fingerprints and facial recognition are both part of biometric identification, but are of two different, distinct subsets. Fingerprints are a well-known example of Immediate Biometric Identification (IBI).[35] Law enforcement and other entities have used IBI for years, and the courts and legislatures have already addressed concerns regarding immediate identification techniques.[36] IBI "tends to be focused (1) on a single individual; (2) close up; (3) in relation either to custodial detention or in the context of a specific physical area related to government activity; (4) in a manner often involving notice and consent; and (5) is a one-time or limited occurrence."[37]

Facial recognition, on the other hand, is one method of Remote Biometric Identification (RBI).[38] In Remote Identification, the subject, or suspect as is the case with law enforcement use of FRT, possibly does not even know they are being identified since it can be done from a distance, whether that distance is physical or temporal.[39] It "requires no suspicion of any individual; it functions as warrantless

photos that users upload. Using FRT, when a user uploads a photo to their profile, Facebook recognizes if there is a face in the picture and suggests possible matches (from the user's list of friends) for each face in the photo. Facebook presented the DeepFace system at the IEEE Computer Vision conference in July 2014, and demonstrated that given two pictures, the system can tell "with 97 percent accuracy whether they're the same person, roughly the same accuracy as a human being in the same spot." *Id.* Discussed in more detail in Section II, by comparison, the FBI's NGI returns a ranked list of 50 possibilities (potential matches) and "only promises an 85 percent chance of returning the suspect's name in the list." *Id.* Therefore, roughly one in seven suspects in an FBI database search will not be included in the search results, even given 50 chances or guesses. Several reasons may explain the difference in the accuracy of the systems: for one, Facebook has a much larger network of data to use and improve on the process, and the actual possibilities it has to compare from is smaller given that it uses each user's friend list, so it does not necessarily have to search the entire network. Thus far, Facebook's network and DeepFace system have remained proprietary. *Id.*

30. Osman & Imwinkelried, *supra* note 24, at IV.

31. Donohue, *supra* note 20, at 409.

32. Osman & Imwinkelried, *supra* note 24, at IV.

33. *Id.*

34. *Id.*

35. Donohue, *supra* note 19, at 415.

36. *See, e.g.*, DNA Fingerprint Act of 2005, Pub. L. No. 109-162, 119 Stat. 2960 (authorizing DNA sample collection from persons arrested or detained under federal authority); Maryland v. King, 133 S. Ct. 1958 (2013) (holding a State's collection of buccal swab DNA during processing of arrestees constitutional).

37. Donohue, *supra* note 19, at 415-16.

38. *Id.* at 415.

39. *See id.* at 409.

mass surveillance."[40] The identification can be accomplished for multiple subjects, and can be continuous or ongoing.[41] Also, since the identification is accomplished from a distance, it can be done in the public space where existing law does not protect the subject from being surveilled or identified without notice to them.[42] Remote Biometric Identification is therefore best characterized as "different in kind, not degree, from what has come before."[43]

Facial recognition has been used in the public arena to monitor and identify large congregations of individuals. In 2001, the Tampa Bay Police Department deployed FRT at the Super Bowl in Tampa Bay, Florida.[44] Police used FRT to scan faces in the crowd as fans entered the stadium the day of the game and to compare the facial images to profiles of individuals in the Department's database.[45] This led to Tampa installing 36 surveillance cameras in an entertainment district in the city, continuously surveilling passersby, and comparing their faces to those in the Department's database.[46] Even then, concerns were raised regarding invasion of privacy and the potential for abuse by the government.[47]

Following the terrorist attacks on September 11, 2001, there was "an increase in calls for the use of biometrics,"[48] and "[a]lmost every major department tasked with national security and law enforcement initiated some sort of biometric activity."[49] At first, the focus of the identification efforts was on individuals entering and leaving the United States,[50] but use of the technology expanded into other identification areas such as domestic law enforcement, surveillance, and counterterrorism.[51] In fact, Congressional action mandated federal agencies to develop and implement new technologies to help identification at the border, and protect against terrorist attacks.[52]

Facial recognition is but the first in a potential series of the next generation of biometric identification. Examples of budding future methods, some of which are in development or limited use already, include: hand geometry, iris, vascular patterns, hormones, and gait.[53] Many, if not all, of these can be utilized remotely, with little-to-no notice to the subject of the identification procedure. Given our current privacy law and policy landscape in the United States, this presents significant questions

40. *Id.*

41. *Id.*

42. *See* discussion *supra* Part I, B.

43. Donohue, *supra* note 19, at 410.

44. Jessica Reaves, *Tampa Gets Ready for Its Closeup*, TIME (July 16, 2001) content.time.com/time/nation/article/0,8599,167846,00.html.

45. *Id.*

46. *See id.*

47. *See id.*

48. COATS ET AL., *supra* note 23, at 1.

49. Donohue, *supra* note 19, at 425.

50. *Id.* at 426.

51. COATS ET AL., *supra* note 23, at 11.

52. *See* Uniting and Strengthening America by Providing Appropriate Tools Requiring to Intercept and Obstruct Terrorism (USA PATRIOT Act) of 2001 Pub. L. No. 107-56, §§401-18, 115 Stat. 272.

53. *See* Donohue, *supra* note 19, at 415; COATS ET AL., *supra* note 23, at 4.

and challenges moving forward.

B. Legal Landscape

As the NGI just reached full operational capacity, there is no significant body of case law on point for facial recognition use in the database. Individuals and organizations are still in the process of understanding the true scope and operation of the NGI and IPS. The latest Privacy Impact Assessment (PIA) released by the FBI regarding the IPS was released in 2008 before many of its new features were implemented or fully developed.[54] The few cases involving the NGI and IPS are requests under the Freedom of Information Act for release of records relating to the program.[55]

Essential to understanding the NGI's potential implications on privacy rights is a discussion of rights under the Fourth Amendment. 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.[56]

The Fourth Amendment gives citizens the right to be protected from warrantless searches by the government, essentially creating a protection of privacy from the government in that respect.[57] This "penumbra" of privacy[58] has been expanded to include privacy for other areas beyond the explicit statement of "persons, houses, papers, and effects," while not going so far as to create a "general constitutional 'right to privacy.'"[59] As the Supreme Court has said, "the overriding function of the Fourth Amendment is to protect personal privacy and dignity from unwarranted intrusion by the State."[60] However, it does not protect against all intrusions, but only "against intrusions which are not justified in the circumstances, or which are made in an improper manner."[61] Further, it only applies to intrusions by the government, not those of private entities or industry.[62]

54. *See generally* Fed. Bureau of Investigation, *supra* note 13. This PIA outlined the initial objectives and potential effects of the NGI and IPS. The FBI did not reference or include the full scope of FRT capabilities that the NGI and IPS now implements, and the report did not discuss the full ability of NGI/IPS to cross-reference with other federal agencies and the states.

55. *See, e.g.*, Elec. Privacy Info. Ctr. v. Fed. Bureau of Investigation, No. 2103-cv-00442, 2014 WL 5713859 (D.D.C. 2014) (requesting records relating to the NGI).

56. U.S. CONST. amend. IV.

57. *See* Mapp v. Ohio, 367 U.S. 643, 656-57 (1965) (holding the Fourth Amendment creates a right of privacy in freedom from "unconscionable invasions").

58. *Id.*

59. Katz v. United States, 389 U.S. 347, 350 (1967).

60. Schmerber v. California, 384 U.S. 757, 767 (1966).

61. *Id.* at 768.

62. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

The Court has recognized two different aspects of privacy rights afforded by the Fourth Amendment. In one sense, the Fourth Amendment protects "expectations of privacy . . . the individual's legitimate expectations that in certain places and at certain times he has the right to be let alone."[63] In another, it specifically protects against "unreasonable searches and seizures."[64] Therefore, privacy cases, in the context of the Fourth Amendment, center on two key issues: first, whether the challenged activity actually constitutes a "search" under the Fourth Amendment, incorporating expectations of privacy, and whether the search was unreasonable. "[T]he ultimate measure of the constitutionality of a government search is 'reasonableness.'"[65] Courts balance the "privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable."[66]

This analysis has been developed and applied over time in different factual scenarios. In *Schmerber v. California*, the Court held a warrantless search, collecting a blood sample, constitutional where the defendant was arrested and brought to the hospital on probable cause for driving under the influence.[67] The search in *Schmerber* was reasonable due to the potential that the evidence, the blood alcohol level of the defendant, would disappear if the search was not conducted or was delayed until a warrant could be obtained.[68] In *Kyllo v. United States*, surveillance of the defendant's house using a thermal-imaging device constituted a search, and the search was unconstitutional because the government used the device to explore details of the home that would have been otherwise unknowable without physical intrusion."[69]

In some instances, analysis of government action stops at the first prong: the action does not constitute a "search" under the Fourth Amendment because a right to privacy did not exist in the situation.[70] This question implicates Fourth Amendment rights to privacy in a normative sense. Generally, rights of privacy and reasonableness under the Fourth Amendment have a grounding in our societal norms, as the Court noted in *Kyllo*: "a Fourth Amendment search occurs when the govern-

63. Winston v. Lee, 470 U.S. 753, 758 (1985) (citation and quotation marks omitted).

64. Kyllo v. United States, 533 U.S. 27, 31 (2001) (quotation marks omitted).

65. Maryland v. King, 133 S. Ct. 1958, 1969 (2013) (citation omitted).

66. *Id.* at 1970 (citation omitted).

67. Schmerber v. California, 384 U.S. 757, 758-59 (1966).

68. *Id.* at 770-71.

69. *Kyllo*, 533 U.S. at 35-40. In *Kyllo*, law enforcement used the evidence of unusual heat signatures on the outside surfaces of the house to obtain a warrant to conduct a physical search of the home. *Id.*

70. *See, e.g.*, Dow Chemical Co. v. United States, 476 U.S. 227, 235-39 (1986) (holding the aerial surveillance of the inside of an industrial complex otherwise hidden from ground view constitutional under the Fourth Amendment, despite arguments for application of the "curtilage" doctrine because the complex was open to the view and observation of persons lawfully in the public airspace above). The curtilage doctrine line of cases extended the boundary of reasonable expectation of privacy beyond the physical walls of the home or structure. *Id.* at 235 (citation omitted). In contrast, the open fields doctrine holds that observations made "out of doors in fields" beyond the area "immediately surrounding the home" are not searches under the Fourth Amendment because there is no reasonable expectation of privacy for activity in that setting. *Id.* at 235-36 (citation omitted). The Court narrowed the *Dow* holding in *Kyllo*, noting the distinction between the industrial setting and that of a person's home: "an industrial complex, which does not share the Fourth Amendment sanctity of the home." *Kyllo*, 533 U.S. at 37.

ment violates a subjective expectation of privacy that society recognizes as reasonable."[71]

In *Davis v. Mississippi*, a detention for the sole purpose of obtaining the subject's fingerprints fell under the nature of Fourth Amendment protections.[72] The Fourth Amendment applies even at the investigatory stage.[73] "Nothing is more clear than that the Fourth Amendment was meant to prevent wholesale intrusions upon the personal security of our citizenry, whether these intrusions be termed 'arrests' or 'investigatory detentions.'"[74] In *Davis*, at least twenty-four African-American teenagers were taken to police headquarters and questioned in connection with a rape investigation.[75] The police also collected fingerprints from all of the youths, including the defendant.[76] The fingerprints were analyzed with a print taken from the crime scene, and the defendant's print was determined to be a match.[77] While the detention in *Davis*, and hence the evidence gleaned from it, was held unconstitutional,[78] the Court declined to "determine whether the requirements of the Fourth Amendment could be met by narrowly circumscribed procedures for obtaining, during the course of a criminal investigation, the fingerprints of individuals for whom there is no probable cause to arrest."[79] This question left open in the context of fingerprinting has not been properly resolved in the biometrics context.

In some contexts however, warrantless biometric searches are constitutional.[80] Most recently, the Supreme Court upheld requiring DNA buccal swabs of arrestees for serious crimes in the state of Maryland.[81] The Maryland DNA Collection Act required all arrested persons charged with serious crimes to provide a DNA sample taken from the inside of the cheeks with a buccal swab.[82] The Court balanced the "legitimate government interest served by the [Act]": "the need for law enforcement officers . . . to process and identify the persons . . . they take into custody . . ."[83] with the mere "extension of methods of identification long used in dealing with persons under arrest."[84] In connection with processing an arrestee, DNA collection was viewed as just an update to old-school fingerprint identification; therefore precedent involving the constitutionality of fingerprinting during processing

71. *Kyllo*, 533 U.S. at 33 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

72. Davis v. Mississippi, 394 U.S. 721, 727-28 (1969).

73. *Id.* at 726.

74. *Id.* at 726-27.

75. *Id.* at 722.

76. *Id.* at 722-23.

77. *Id.* at 723.

78. Davis v. Mississippi, 394 U.S. 721, 728.

79. *Id.*

80. However, these warrantless searches are generally supported by an initial finding of probable cause. *See, e.g.*, Schmerber v. California, 384 U.S. 757, 758 (1966) (where the subject was arrested at the hospital on suspicion of driving under the influence while receiving treatment for injuries sustained in a car accident).

81. Maryland v. King, 133 S. Ct. 1958, 1980 (2013).

82. *Id.* at 1970.

83. *Id.*

84. *Id.* at 1977 (citing U.S. v. Kelly, 55 F. 2d 67, 69 (1932)).

was translated to the collection of DNA.[85] The issue with the reasoning in *King* is the reliance on the lack of "surgical intrusion beneath the skin" and that the practice posed "no threat to the arrestee's health or safety."[86] "Such a distinction will apply to many existing and emerging technologies, including – importantly – almost all other biometric identification technology."[87] Accordingly, just because "a method of collection has improved or become[s] less intrusive does not necessarily negate or diminish the intrusively private nature of the data collected."[88]

A person has a reasonable expectation of privacy to their own body because "[s]earch warrants are ordinarily required for searches of dwellings . . . no less could be required where intrusions into the human body are concerned."[89] In contrast, there is no reasonable expectation of privacy under the Fourth Amendment for one's face, for as the Supreme Court has said, "[n]o person . . . can reasonably expect that his face will be a mystery to the world"[90] because "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[91] *Dionisio* dealt with an individual's voice, but the Court also recognized the same logic applies to a person's face and their handwriting, which are constantly exposed to the public in everyday life.[92] Given these precedents, it would seem that any Fourth Amendment challenge with respect to one's face would fail. However, the question remains whether data obtained outside the context of a law-enforcement purpose would be an unreasonable search if then later utilized in a criminal investigation.

Since the development of facial recognition technology and the initial proposal for the NGI, there has been scholarship in the space of biometrics. Most related articles focus on the constitutional implications of law enforcement's use of facial recognition technology, through analysis under Fourth Amendment searches and seizures.[93] Others analyze facial recognition technology and privacy rights with respect to anonymity for biometric information, and present the argument that existing constitutional protections are sufficient to assuage concerns over the new technologies.[94] Helpful in this note's discussion is Laura Donohue's 2012 article, in

85. *See id.*

86. *Id.* at 1963 (citing Winston v. Lee, 470 U.S. 753, 760-63 (1985)).

87. Anne T. McKenna, *Symposium 2013: Where There is No Darkness: Technology and the Future of Privacy: Article: Pass Parallel Privacy Standards or Privacy Perishes*, 65 RUTGERS L. REV. 1041, 1055 (2013).

88. *Id.* McKenna describes the intrusive and private nature of the DNA information collected in *King*, however her argument can be analogized to the collection of a face print because of the permanent and personal nature of the information collected in a faceprint.

89. Schmerber v. California, 384 U.S. 757, 770 (1966).

90. United States v. Dionisio, 410 U.S. 1, 14 (1973).

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

92. *Dionisio*, 410 U.S. at 14.

93. *See, e.g.*, Susan McCoy, Comment, *O' Big Brother Where Art Thou?: the Constitutional Use of Facial-Recognition Technology*, 20 J. MARSHALL J. COMPUTER & INFO. L. 471 (2002). McCoy argues the use of facial recognition technology is not a search prohibited by the Fourth Amendment because there is not a reasonable expectation of privacy that would be violated.

94. *See, e.g.*, Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409 (2014). Brown discusses privacy as it relates to anonymity and argues that the intersection of First

which she analyzes remote biometric identification generally.[95] Donohue puts forth the argument that "the current statutory and constitutional framing is inadequate to address the new conditions that accompany these emerging technologies."[96] Her proposed remedy is immediate consideration of the issues on the federal level.[97]

In contrast to the existing literature, this note puts forth several novel items for consideration in the discussion of the NGI and IPS. First, while allowing for the lack of Fourth Amendment protection for one's face generally, this note argues that individuals do have a right to privacy, on some level, of their face prints, especially so far as to require adequate notice and information so that individuals included in federal databases through civil submission channels have the opportunity to be informed and potentially remove their biometric data. Second, given that federal law is the basis for the FBI's collection of data, Congress should act to clarify and limit the nature of data the FBI collects, how it is used and stored, and allow certain classes of citizens' profiles to be removed from the database. Specifically, this notes argues that can be accomplished through Congressional amendment of 28 U.S.C. § 534, incorporating principles borrowed from the EU Data Protection Directive.

II. NGI AND IPS DEVELOPMENT

The FBI first announced its plan to develop the NGI as an improvement to existing federal biometric, predominantly fingerprint, databases in 2007.[98] Partnering with government contractors who had already worked on building large databases for other agencies, such as the State Department,[99] the NGI carried an initial price tag of $1 billion.[100] The NGI falls under the purview of the FBI's Criminal Justice Information Services (CJIS) Division, the "focal point and central repository for criminal justice information services in the FBI."[101] The CJIS encompasses the existing information infrastructure: the Integrated Automated Fingerprint Identification System (IAFIS), the National Crime Information Center (NCIC), and the Interstate Identification Index (III).[102] The NGI would incorporate and replace several separate databases, creating one massive, central repository for many types of biometric data and other identification information.

After initial plans for the program were developed, the Bureau compiled and

and Fourth Amendment protections as they currently exist is sufficient to apply to facial recognition technology.

95. Donohue, *supra* note 19, at 416.

96. *Id.*

97. *Id.* at 558-59.

98. Ellen Nakashima, *FBI Prepares Vast Database of Biometrics*, WASH. POST, Dec. 22, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/12/21/AR2007122102544.html.

99. Lynch, *supra* note 10.

100. Nakashima, *supra* note 98.

101. Fed. Bureau of Investigation, *supra* note 13, § I.1.

102. *Id.* at §I.2. The III is the national criminal history record index, accessible across state and federal boundaries by various law enforcement agencies. *Id.* It maintains an index of persons arrested for felonies or misdemeanors under both State and Federal law. *Id.* at §I.4.

released a Privacy Impact Assessment in 2008.[103] At the time, the NGI IPS seemed intended as merely an upgrade to the existing IAFIS fingerprint database, allowing for more photo submissions with criminal mug shots, while increasing efficiency and effectiveness of fingerprint identification techniques.[104] The Privacy Impact Assessment outlined the challenges law enforcement was facing using the existing IAFIS system which precipitated the development of the NGI:

The IPS service is significantly under-populated due to the current policy restrictions limiting the number of photos that can be maintained per FBI record, limiting the type of photo submissions to facial (i.e., mug shots), prohibiting bulk photo submissions from existing contributor databases, requiring photo set submissions be accompanied by "ten-print" arrest cards (containing prints of all ten fingers), and prohibiting photo submissions with civil fingerprint submissions; and [t]he IPS service is under-utilized because it is difficult to search and retrieve photographs from the system. Currently, IAFIS users desiring photographs from the IPS must make a special CPR request to obtain such photographs, which must be manually processed by CJIS. Additionally, system search capabilities are minimal; searches can only be made by name or other identifying number, and cannot be made by entering precise physical descriptors or by using facial recognition technology.[105]

The Assessment identified numerous enhancements to be implemented with the NGI: increasing the limit of photos per record; allow bulk submission of photos; allow photos with civil transactions; allow non-facial photos, e.g. scars, marks, and tattoos; allow user retrieval of photos from the IPS through the NCIC; allow investigative searches using biographical information; and automated facial recognition, and search, capability.[106] According to the Assessment, the enhancements will allow for more photos to be retained, better algorithms for searches, facial recognition technology capability, and more direct retrieval of photos.[107]

The nature of the information collected as part of the NGI includes information that was already maintained in the IAFIS system: names, addresses, social security numbers, telephone numbers, e-mail addresses, gender, race, dates of birth, license numbers, and others.[108] The NGI expands the data by allowing more mug shot photos per profile, photo and biometric data from civil submissions, facial features for use in FRT searches, and photos of scars and tattoos.[109] Another new capability of the NGI is called the Rap Back service. The Rap Back system allows authorized employers to submit collected biometric data of their employees to the FBI.[110] The FBI then includes the employees' information in the database and notifies the employer of any criminal, or even civil, activities that come up for that employee on an

103. *Id.*

104. *Id.*

105. *Id.* at § I.7.

106. *Id.* at § I.7.

107. *See id.*

108. Fed. Bureau of Investigation, *supra* note 13, at §1.1.1.

109. *Id.*

110. *See Next Generation Identification (NGI),* FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited March 1, 2015).

ongoing basis.[111]

While the NGI and IPS represent significant advances in FRT, the development and improvement of the technology is ongoing. Natural factors, aside from the technological capabilities of the system, can still affect the use and accuracy of facial recognition. The lighting conditions of the environment in which the image was taken and the extent to which the subject of it was cooperative, or even visible, can inhibit the ability of a facial recognition system to obtain a face print and subsequently harm the evaluation and probability of "matches."[112] While further engineering and development will in all likelihood, eventually overcome these challenges, for now the accuracy of FRT is affected by simple things such as whether the subject was in a shadow, turned away from the camera or only presented part of their face.

The FBI recently announced that the NGI and IPS are fully operational, and can be utilized by more than 18,000 offices nationwide.[113] The process began in 2011, using a phase-in approach over the last three years.[114] Response time for searching and matching for the IPS is now as efficient as within minutes of a request, but it can vary with the seriousness or urgency attached to the request.[115]

Another crucial aspect of the NGI is cooperation and access by state law enforcement agencies. Numerous states are already participating in the NGI, and some participated in the pilot programs during the phase-in. During the pilot program, states such as North Carolina and Oregon utilized their Departments of Motor Vehicles databases' FRT and linked their databases to the NGI.[116] Ideally, the NGI would allow state law enforcement to search the national database federal agencies to access and search existing state databases that are now, or would be, linked to the NGI. The linked databases would then incorporate FRT in addition to the existing fingerprint search capability.[117]

111. *See 5 Things You Should Know About the FBI's Massive Biometric Database (Alternet)*, UNCOVER THE TRUTH (Jan. 8, 2012), http://uncoverthetruth.org/press/5-things-you-should-know-about-the-fbis-massive-new-biometric-database-alternet/.

112. Nakashima, *supra* note 98 (citing a German government study from 2006-2007 that found only sixty percent FRT accuracy during the day, with significantly less, only 10 to 20 percent accuracy, at night using FRT).

113. Fed. Bureau of Investigation, *supra* note 7.

114. *Spotlight on Surveillance - December 2013*, ELECTRONIC PRIVACY INFO. CENTER, https://epic.org/privacy/surveillance/spotlight/ngi.html (last visited March 2, 2015).

115. *Next Generation Identification (NGI) Fact Sheet*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/next-generation-identification-fact-sheet (last visited March 2015).

116. *See* Lynch, *supra* note 10. The DMVs initially used FRT to combat identity theft and fraud in their driver's license registries.

117. Craig Timberg & Ellen Nakashima, *State photo-ID databases become troves for police*, WASH. POST (June 16, 2013), http://www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.html.

III. EXISTING PRIVACY LEGAL REGIME

A. State Law

Less than a third of states have their own general privacy law.[118] However, most every state recognizes privacy torts, to protect the interests first framed by Warren and Brandeis in their seminal article, *The Right to Privacy*.[119] Each individual state's law incorporates all or most of the four recognized privacy torts as common law rights of action.[120] These torts provide causes of action between individuals for the violation of a right to privacy.

Some states grant their citizens a general right to privacy through the state's constitution.[121] California's gives each citizen "an 'inalienable right' to pursue and obtain 'privacy.'"[122] Florida gives every person "the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided [in the Florida Constitution]."[123] The Montana Constitution describes the right of privacy as "essential to the well-being of a free society," and provides "[it] shall not be infringed without the showing of a compelling state interest."[124] These constitutional provisions grant individuals a right of privacy, while leaving the door open for government violation thereof, requiring varying degrees of demonstration to do. Further, each state has its own numerous laws governing specific areas of privacy.[125] Much like general grants of privacy, area-specific privacy laws tend to be focused on protection of privacy in the public[126] or commercial setting, but these laws do not extend protection to an individual whose data is already handled by the government.

B. Federal Law

In federal law, besides the "penumbra" of privacy rights under the Constitution discussed above,[127] the only "general" privacy rights granted to individuals are specially tailored to apply to personal information stored in government systems, pro-

118. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 32 (Wolters Kluwer Law & Business 4th ed. 2011).

119. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). Warren and Brandeis articulated the basis for the "right to be let alone." *Id.* at 195. While not proscribing the specific rights encompassed within privacy, they outlined some limits to the general right. *Id.* at 214-19.

120. *See* Solove & Schwartz, *supra* note 118, at 32. The four recognized torts are: (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) dissemination of false or misleading information, and (4) misappropriation of name or likeness.

121. *See, e.g.*, CAL. CONST., art. I, § 1.

122. *Id.*

123. FLA. CONST., art. I, § 23.

124. MONT. CONST., art. II, §10.

125. *See, e.g.*, CAL. CIV. CODE § 1798.90.1 (limiting the purposes for which businesses may swipe a driver's license or ID card in electronic devices).

126. "Public" is used here to mean the opposite of private, i.e. in the open, rather than in a governmental sense.

127. *See* discussion *supra* Part I.

vided by the Privacy Act.[128] The Privacy Act operates on the premise that the individual already has information in government databases, and therefore the Act requires protections for the handling of the data and access to it. The Privacy Act is focused on protecting individuals' data in government systems from inadvertent or malicious disclosure to unauthorized parties.[129] Following the Privacy Act, various other laws were enacted to provide individuals more protection of their information in specifically tailored areas such as educational records;[130] health information;[131] and information contained in driver's license registries.[132] Other laws actually limit or curtail the privacy right of individuals.[133] Following the September 11th terrorist attacks, the USA PATRIOT Act gave the government greater powers of surveillance and information collection, which intrudes upon the privacy of individuals, with the primary motivation of national security.[134]

While federal legislators have become aware of the issue of FRT use and the need for legislative action,[135] no laws have yet addressed the use of FRT directly.[136] It is in this legislative lag period that the FBI, as well as the commercial world, continues to operate using FRT with relatively few limits.

IV. RIGHT TO FACE PRINT PRIVACY

A. Criminal mug shot photos

It is well established that criminal mug shot photos are public record. A person can actually walk into convenience stores around the country and purchase their local mug shot photo periodical, or even more conveniently, go online to various

128. Privacy Act of 1974, 5 U.S.C. § 552 (2009).

129. *See id.* The Act essentially functions as a statute for data security, which has an underlying or simultaneous goal of privacy.

130. *See* Family Education Rights and Privacy Act, 20 U.S.C. § 1232g (1974).

131. *See* HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

132. *See* Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2012). The DPPA protects individuals' information stored by state departments of motor vehicles, and restricts the purposes for which it can be released. The Act does have a broad carve-out for other government agencies, state and federal, including law enforcement. 18 U.S.C. § 2721(b)(1).

133. *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

134. *See* SOLOVE & SCHWARTZ, *supra* note 118, at 331-33.

135. Brian Heaton, *Facial Recognition Technology Spurs Privacy Concerns for Feds*, GOV'T TECH. (Oct. 21, 2011), http://www.govtech.com/public-safety/Facial-Recognition-Privacy-Concerns-Feds.html (discussing Sen. John D. Rockefeller, IV's request for the Federal Trade Commission to consider the privacy impact of FRT and deliver a report by February 2012). The FTC's 2012 report made recommendations for industry and for legislators. FED. TRADE COMM'N, PROTECTION CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS (2012) *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

136. Instead, laws have continued to be introduced and passed regarding examples of Immediate Biometric Identification, such as fingerprinting and DNA collection. *See, e.g.*, DNA Fingerprint Act of 2005, Pub. L. No. 109-162, §§ 1001-1005 (allowing for the removal of DNA information from the national database and explicitly authorizing DNA collection from any person detained or arrested for violation of federal law).

websites that collect and publish the photos.[137] Therefore, by statute, in practice, and by common knowledge, it is understood that criminal mug shots are public record. As such, courts have held that individuals do not have a right to privacy in them.[138]

Even if the photos themselves were not published in the public record, case law under the Fourth Amendment allows for the collection of facial biometric data during the processing of arrestees.[139] As such, law enforcement agencies have created and maintained mug shot photo databases for years, including the FBI's old IAFIS database, which allowed for inclusion of a mug shot photo with each profile.[140] Therefore, this note does not argue that individuals have a right to privacy in their face prints obtained through criminal mug shot photos, on the basis that an individual's possible involvement in criminal activities gives rise to the presumption that they are on notice that there may be "collection of information incident to law enforcement response to those activities."[141] Because collection of identification information is a natural part of the booking procedure at almost any jail in the country, individuals likely have no reasonable expectation of privacy in face prints taken as part of a criminal arrest.

Further, the logic for the lack of a right to privacy in face prints in criminal mug shot photos can be extended to photos obtained through lawful criminal investigations, provided the methodology used by law enforcement complies with the requirements of the Fourth Amendment, as discussed above.[142] Where law enforcement is investigating a suspect, and through surveillance of the suspect remotely obtains an image, the individual does not have, nor should they have, a right to privacy that protects against the creation of a face print from that image. The Supreme Court has said that individuals do not have a reasonable expectation of privacy in their face.[143] By extension, a non-intrusive digital mapping of that image, if challenged, would probably be held constitutional as well, or would not be considered a search under the Fourth Amendment, given the passive nature of such collection.

B. Non-criminal and civil photos

According to the FBI's 2008 Privacy Impact Assessment for the NGI and IPS:

Authorized noncriminal justice agencies and entities will be permitted to submit civil photographs along with civil fingerprint submissions that were collected

137. *E.g.*, MUGSHOTS.COM, http://www.mugshots.com (last visited March 29, 2015).

138. *E.g.*, Pemberton v. Bethlehem Steel Corp., 502 A.2d 1101, 1119 (Md. Ct. Spec. App. 1986) (holding, "[mug shots are] by law, a public record to which the public may have . . . access.").

139. *See* Maryland v. King, 133 S. Ct. 1958 (2013) (holding constitutional a Maryland law requiring DNA buccal swabs from the arrestee's cheek, almost certainly a more "intrusive" procedure than merely taking an arrestee's photo).

140. Fed. Bureau of Investigation, *supra* note 13, at § 1.1.1.

141. *Id.* at § 6.1.1.

142. *See supra* Part I, B. *See, e.g.*, Davis v. Mississippi, 394 U.S. 721, 727-28 (1969) (holding Fourth Amendment protections apply at the investigatory stage).

143. United States v. Dionisio, 410 U.S. 1, 14 (1973).

for noncriminal purposes. These photos may either be provided to the submitting agency by the individual or taken directly by the submitting agency. Civil photos will supplement the biographical information and narrative physical descriptions that are already provided under existing practices.[144]

The PIA goes a step further and evaluates the impact to individuals' privacy that civil-submitted photos will have: "merely adding photos to civil files is not considered to be a substantial expansion of the existing civil files, so long as the photos will only be retrieved *incident* to the authorized retrieval of the underlying record of a *specified* individual."[145] There are several issues with this provision of the PIA. First, it was compiled in 2008, before the full phase-in of the IPS even began, and before its (current) full capabilities were properly outlined.[146] The Assessment overlooks the significant part, this note argues, of the new capability the IPS offers: facial recognition searching of a combined civil and criminal database. Specifically with regards to searching images submitted through civil avenues, the Assessment does not consider the privacy implications of FRT searching of the civil files, but acknowledges that it would be a "significant new privacy consideration," a consideration that has become a reality with the effective deployment of the NGI.

Non-criminal photos can come from various sources, and are not as clear-cut with respect to implication of privacy rights. While there has not been an official estimate from the FBI, sources indicate that by 2015, there will over 4.3 million non-criminal photos in the IPS.[147] This includes information and biometric data submitted for background checks, most often for purposes as innocent as checks prior to offer of employment. Previously, the criminal and non-criminal profiles were kept separate and distinct from each other; however, the IPS combines both types in a single, large database. This mixing of photos means that non-criminal photos could be included in results yielded for criminal searches.

The mixing in practice acts contrary to the FBI's stated limitation: retrieving photos "incident to the authorized retrieval of the underlying record of a specific individual." Where a search is conducted in the database, the 50 results' photos will be retrieved as part of a search for an unidentified individual. This individual will neither be specific, or he/she could possibly not even have a record in the database. Multitudes of individuals' records will be accessed in searching for a possible match to an unspecified and unknown photo. This limitation is only satisfied in cases where the search is used for *verification* purposes, rather than identification, because the photo being matched to is already attached to a specific record, and the search is merely used to confirm the identity of the specific individual. Searches for investigatory identification purposes go completely beyond the FBI's stated limitation in the 2008 PIA, and beyond their consideration of potential privacy issues.

144. Fed. Bureau of Investigation, *supra* note 13, at § 1.2.1.

145. *Id.* at § 2.3 (emphasis added).

146. *Id.*

147. *See* Lynch, *supra* note 10.

The FBI maintains that there will be no "positive identifications," i.e. one hundred percent matches, but rather that the set of results will include profiles fitting a high probability of similarity with the subject photo.[148] Further, it says that the results would be used for investigative purposes, rather than determining guilt.[149] However, concerns are heightened by the results of research done through the Center for Catastrophe Preparedness and Response at New York University that shows that the risk of false positives increases as the data set increases in size.[150]

Of other concern is that a portion of the photos in the IPS will come from unnamed or ambiguous sources. It is estimated that almost 1 million photos, by 2015 alone, will come from three sources whose origins and makeup have not been clearly defined by the FBI.[151] These include 215,000 photos from the Repository for Individuals of Special Concern; 750,000 photos from a "Special Population Cognizant" category; and 215,000 photos from so-called "New Repositories."[152]

Individuals without a criminal background should have a right to privacy with regards to not being implicated in a criminal investigation unnecessarily. On the surface, the Fourth Amendment does not afford protection for one's face in this context, discussed in more detail above.[153] However, Fourth Amendment precedent deals with government action in the criminal space, whether during the investigatory or post-arrest phases.[154] Application of these principles to the civil photos in the NGI/IPS is not a perfect "match." For example, the civil photos in the NGI are submitted as part of searches completely apart from any criminal investigation, and are then stored for use beyond their initial purpose. Further, in the Fourth Amendment cases analyzing constitutional invasions of privacy, there was underlying probable cause for the search and seizure as the subjects were detained or arrested prior to the search. In the case of the NGI, there will be no probable cause finding for the commission of the crime for which the search is conducted, especially for those who are in the database as part of an employment background check. Admittedly, the voluntary act of submitting one's photo, as in the case of a background check in exchange for an offer of employment, could be construed to forfeit any right to privacy in the photo. However, the government may not have a legitimate interest in the continued use of civil photos in criminal searches that is sufficient to survive scrutiny under the Fourth Amendment.

The NGI's use of civil photos is different from the circumstances present in

148. *See* Feb. Bureau of Investigation, *supra* note 13. No specific number has been given for what the numeric accuracy threshold would be for the NGI to return possible results.

149. *Id.*

150. *See* Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues* (2009), http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf. This concern is relevant because presumably the FBI will continue to expand the NGI database as it gathers more data.

151. Lynch, *supra* note 10. The FBI does actually describe where the photos contained in these categories will come from, or (other than the Individuals of Special Concern) why the photos are different from the normal database population. Indications are that the sources will come from other government agencies, but it is not entirely clear at this point. *See id.*

152. *Id.*

153. *See* discussion *supra* Part I, B.

154. *See, e.g.*, Maryland v. King, 133 S. Ct. 1958 (2013); Davis v. Mississippi, 394 U.S. 721 (1969).

cases that the Supreme Court has reviewed and found to be beyond the scope of Fourth Amendment privacy rights. First, the photos were not obtained in connection with any criminal suspicion, investigation, search, arrest, or processing. In determining whether a search was reasonable, the Court weighs the law-enforcement interest.[155] However, with the civil photos there is no cognizable law-enforcement interest. The photos only represent a potential for future investigatory use in connection with identifying subjects, which does not lend much weight. Second, the limit for potential "detentions" does not exist. 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. This would all be done without any probable cause as to their involvement in an alleged crime, other than their photo being in the database. Given the lingering deficiencies in the analysis and technology, the privacy concerns weigh quite heavily against the potential security benefits.

It is established that individuals do not have a reasonable expectation of privacy in their face.[156] However, a face print is distinguishable from one's publicly viewable face. While 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. One 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.

Remote biometric identification, specifically facial recognition, has separate concerns regarding data collection than other methods of identification because of the permanence of the characteristic involved and personal nature of the technique. Absent significant surgical procedures or catastrophic injury, it is highly improbable a person would be able to change the features of their face enough to trick a facial recognition program. Once born, we are therefore stuck with our face, and once that is made into a face print there is no changing it. This distinguishes facial recognition from other, already accepted, databases of biometric identification such as fingerprints.

Another way of conceptualizing the harm to an individual's privacy caused by creating face prints of individuals without transparency or consent is through the view of a dignity interest.[157] Traditionally, the Fourth Amendment is viewed as protecting against a burden the government places on an individual through searches and seizures. Where a burden exists, it necessarily requires the subject of the search to know of and feel the burden. However, a dignity interest is violated even if the subject does not know a warrantless or suspicion-less search has been conducted.[158]

155. *King*, 133 S. Ct. at 1970.

156. *See* United States v. Dionisio, 410 U.S. 1, 14 (1973); Katz v. United States, 389 U.S. 347, 351 (1967).

157. *See* Kevin Miller, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, 19 J. TECH. L. & POL'Y 105, 127 (2014).

158. LAWRENCE LESSIG, CODE 211 (version 2.0 2006), *available at*

Taken a step further, one can think of privacy, as a concept, as something that restricts what the government can do with respect to the individual.[159] Where individuals have a right to privacy, the government cannot constitutionally act. This conception of privacy would apply best to the expanding uses of technology and government overreach that threaten to create a national police or surveillance State. Given that privacy law is based in part on society's understanding or expectations of privacy, if society developed an expectation that privacy exists to limit where and how the government can act, then programs that encroach into surveillance State territory, such as the NGI IPS, would be harder to justify.

V. PRINCIPLES FROM THE EU DATA PROTECTION DIRECTIVE

The European Union Data Protection Directive of 1995 created "common rules for data protection among Member States of the European Union."[160] While not mandatory or enforceable on European citizens by itself, member states have adopted their own codification of the Directive to enforce in their jurisdiction.[161] The Directive endowed individuals with substantial rights in controlling the use of their information.[162] The essence of the Directive can be found in its name: *data protection*. It names as an objective the protection of the "right to privacy with respect to the processing of personal data."[163] The Directive covers commercial collection and use of data, with a carve-out for governmental entity action.[164]

Article 7 of the Directive generally applies to the corporate and public worlds' handling of customer data. Where the situation is not one of five specific uses outlined, the individual must unambiguously give his or her consent, after being adequately informed.[165] Data processing is allowed outside of the Directive's protections where necessary to perform tasks of public interest, or those carried out by the government or law enforcement.[166] The Directive more clearly defines the respon-

http://codev2.cc/download+remix/Lessig-Codev2.pdf.

159. *Id.* at 213.

160. SOLOVE & SCHWARTZ, *supra* note 118, at 1109.

161. *See* Directive 95/46, art. 4, 1995 O.J. (L 281) 31, 50 (EC) (directing each Member State to adopt their own national provisions pursuant to the Directive).

162. *See, e.g.*, Directive 95/46/ art. 12, 1995 O.J. (L 281) 31, 50 (EC) (Right of Access to Data).

163. Directive 95/46 art. 1 1995 (L 281) 31, 50 (EC). *See* SOLOVE & SCHWARTZ, *supra* note 110 at 1110.

164. *See id.* at art. 3.

165. *See id.* at art. 7. "Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)." *Id.*

166. *See id.* at art. 3. "This Directive shall not apply to the processing of personal data: - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of

sibilities of data collection entities, data controllers, and the rights of individuals.[167]

The Directive places numerous obligations on "data controllers," i.e. those entities collecting or processing data.[168] The data must be collected for explicit and legitimate purposes, and used according to those purposes.[169] The data collected must be adequate, relevant, and not excessive in relation to the purposes for which it was collected.[170] Inaccurate data must be allowed to be deleted or correct.[171] Personal information cannot be kept longer than is strictly necessary for its purposes.[172]

The Directive also grants numerous rights to individuals as the subjects of collected data. The subject must be informed at the collection point, and the information must include what is being processed, for what purpose, and to whom it might be transferred to outside of the data controller.[173] The subject must also be allowed to request deletion of the data, to block the data, or to modify inaccuracies.[174] Essential tenets of the Directive thus focus on notice, consent, security, and transparency as to the storage of the data.

With the many grants and protections the Directive offers to data subjects, it also provides significant exceptions. The Directive was enacted in the context of the European Community; therefore its scope is limited to the area of competence, essentially the jurisdiction, of the Community. Data processing activities concerning defense, national security, and the Member States' criminal law therefore fall outside the scope of the EC and the Directive.[175] Nevertheless, the principles set forth in the Directive influenced the EU Member States in enacting and upgrading their own privacy laws, and provide a blueprint for enhanced legislation in the United States.

Since the Directive's inception however, EU law has developed data protection rules in the law enforcement and criminal justice field.[176] The CoE "Police Recommendation" provides limits for police collection and use of personal data.[177] Specifically, it restricts European law enforcement from collection of data unless it is "necessary for the prevention of a real danger or the suppression of a specific

the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law." *Id.*

167. *See id.* at art. 6.

168. *Id.* at art. 2. "Data controller" is defined as "the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." *Id.* at art. 2(d).

169. Directive 95/46 art. 6 § 1(b), 1995 O.J. (L 281) 31, 50 (EC).

170. *Id.* at art. 6(1)(c).

171. *Id.* at art. 6(1)(d).

172. *Id.* at art. 6(1)(e).

173. *Id.* at art. 10.

174. *Id.* at art. 12.

175. SOLOVE & SCHWARTZ, *supra* note 118, at 1111.

176. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW, 143 (2014), *available at* http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

177. *Id.* at 146

criminal offence."[178] "Processing of sensitive data should be limited to that which is *absolute[ly] necessary* in the context of a particular inquiry."[179] The Recommendation even provides for notification of the data subject for collection of data without their knowledge, provided that disclosure or notice would not inhibit an investigation, even for surveillance.[180]

VI. STATUTORY AMENDMENT

The existing United States privacy law regime does not offer protection from government collection and misuse of biometric data. In fact, current law actually requires collection of such data for the purposes of identification, without any limits whatsoever.[181] The FBI cites 28 U.S.C. § 534 in its Privacy Impact Assessments as the statutory basis for its authority to collect criminal and general identification data and to develop the NGI and IPS.[182] More generally, the Supreme Court years ago held constitutional the collection of data and maintenance thereof in a database by the government.[183]

Despite the growing trend and increase in the array of biometric techniques available for use in identification, some states have actually limited, or even prohibited, law enforcement access to facial recognition capability.[184] Some have even restricted the mere collection of biometric data.[185] This is evidence of recognition of the dangers of biometric information and legislatures acting to protect their citizens.

Likewise, given that the basis for the authority of the NGI lies in the realm of federal statutory law, and the FBI as a federal agency is self-interested to take its power of identification records to its full limit, responsibility for protecting the individual's privacy falls to Congress as the grantor of the FBI's underlying authority. This note does not propose a sweeping new privacy law, nor does it propose a grandiose legislative or oversight plan limiting the FBI's ability to fulfill its purpose as a law enforcement agency. Rather, Congress can simply amend the "grant" of power that the FBI relies on for the authority to collect and maintain identification data: 28 U.S.C. § 534.

Unless we, or a particular court taking up a challenge, look at § 534 through the statutory canon of construction *ejusdem generis*,[186] the general phrases used in the

178. *Id.*

179. *Id.* (emphasis added).

180. *Id.*

181. *See, e.g.*, 28 U.S.C. § 534 (requiring the Attorney General to collect and maintain identification data, not just for criminal profiles and records, but generally).

182. Fed. Bureau of Investigation, *supra* note 13, at § 2.2.

183. Whalen v. Roe, 429 U.S. 589 (1977) (holding New York's collection of all prescriptions filed and personal information for the patients involved constitutional, so long as proper measures are taken to safeguard citizens' data).

184. *See* Timberg & Nakashima, *supra* note 117 (providing Minnesota, Oregon, and Washington state as examples).

185. *See id.* New Hampshire categorically prohibits its DMV from collecting biometric data. *Id.*

186. *Ejusdem generis* is a statutory "canon of construction holding that when a general word or phrase follows a list of specifics, the general word or phrase will be interpreted to include only items of the same

section could be interpreted to an indefinite breadth.[187] Subsection (a)(1) mandates that the Attorney General "acquire, collect, classify, and preserve identification . . . and other records."[188] While some of the general terms are more specifically defined later in the section,[189] "other records" is conspicuously not. Congress chose to define, or at least provide examples for, some of the general terms it used at the end of the lists in subsection (a), but not "records". If viewed in its plain meaning, and taken to the extreme, that provision essentially grants, actually compels,[190] the FBI to collect and preserve records, the nature of which it seems free to choose on its own by the lack of specification. In context, and employing *ejusdem generis*, it seems natural that the "other records" be somewhat related to the other listed terms in (a): "identification", "criminal identification", and "crime".[191] However, with advances in technology, the scope of "identification" itself has changed, and so has the potential breadth of "records."

Regardless of the last term in (a)(1),[192] § 534 does at least enumerate a list of the types of records to be collected and maintained by the FBI. However, it neglects to provide the types of *information* these records should, or may, contain. Where it concerns identification of a deceased individual, as discussed in (a)(2), or assisting in locating a missing person, as discussed in (a)(3), "information" is included without limit, (un)specifically as "any information".[193] There are obvious normative and policy reasons for not wanting to limit the universe of data available to the FBI in performing its role to identify the deceased and help return the missing.[194] However, given the potential use of *noscitur a sociis*[195] to resolve any ambiguity as to what information can be collected under (a)(1), it would be best, at least for privacy concerns, to more clearly demarcate what information should be collected for the "identification, criminal identification, crime, and other records." This would prevent policy rationales for identifying deceased or missing persons from encroaching on living persons' privacy through information contained in the civil records.

class as those listed." BLACK'S LAW DICTIONARY 594 (9th ed. 2009).

187. Interpreting § 534 through the lens of *ejusdem generis* would limit the general phrases (e.g., "other records") to those related in kind to the preceding items.

188. 28 U.S.C. § 534(a)(1).

189. *See, e.g.*, 28 U.S.C. § 534(a)(4) ("exchange such records and information with, and for the official use of, authorized officials of the Federal Government, including the United States Sentencing Commission, the States, including State sentencing commissions, Indian tribes, cities, and penal and other institutions."); 28 U.S.C. § 534(e) ("For purposes of this section, the term 'other institutions' includes- - (1) railroad police departments . . . ").

190. 28 U.S.C. § 534(a) ("The Attorney General *shall*") (emphasis added).

191. 28 U.S.C. § 534(a)(1).

192. *Id.* ("records").

193. 28 U.S.C. § 534(a)(2) & (3).

194. The government, and our society generally, want to be able to identify deceased persons rather than having John/Jane Doe's. Also, there is a powerful interest in finding, and potentially rescuing, missing persons with the help of identification records. These two types of profiles have very different purposes and uses than do those from the criminal and civil submissions.

195. *Noscitur a sociis* is a statutory "canon of construction holding that the meaning of an unclear word or phrase should be determined by the words immediately surrounding it." BLACK'S LAW DICTIONARY 1160-61 (9th ed. 2009).

Given the argument for an individual's right to privacy with respect to keeping the submission of a civil photo for a background check, or other innocuous function, from becoming a face print permanently lodged in the NGI IPS database, Congress should amend § 534(a)(1) to limit collection of remote biometric identification data for civil submissions. The proposed amendment could resemble the following, with this note's proposed additions in bold:

> § 534. Acquisition, preservation, and exchange of identification records and information; appointment of officials
>
> The Attorney General shall—
>
> acquire, collect, classify, and preserve identification, criminal identification, crime and other records;
>
> for criminal identification and crime records under this section, the Attorney General may collect, in keeping with constitutional requirements for data collection:
>
> all personally identifiable information related to the profile of the individual and maintenance thereof;
>
> all immediate biometric identification[196] data incident to the arrest and processing of the individual, including, but not limited to, fingerprints, palm prints, and DNA.
>
> for general identification and other records under this section, the Attorney General may collect, in keeping with other legal requirements for data collection:
>
> all personally identifiable information related to the profile of the individual and maintenance thereof;
>
> biometric identification data, limited to any data submitted with the file initially (e.g. fingerprints or headshot photograph), with the data to be maintained in the condition it was submitted, without creating or compiling data of a different nature or form, including but not limited to a digital face print, from that submitted without express consent or stated purpose of the provider of the data, and subject to subsequent removal by the data subject/provider;
>
> other information related to the specific purpose for which the profile was originally submitted to the Office, by express or implied consent of the provider of the data;

196. IBI here would have the same definition as it has elsewhere in this note.

> acquire, collect, classify, and preserve any information which would assist in the identification of any deceased individual who has not been identified after the discovery of such deceased individual;
>
> acquire, collect, classify, and preserve any information which would assist in the location of any missing person (including an unemancipated person as defined by the laws of the place of residence of such person) and provide confirmation as to any entry for such a person to the parent, legal guardian, or next of kin of that person (and the Attorney General may acquire, collect, classify, and preserve such information from such parent, guardian or next of kin); and
>
> exchange such records and information with, and for the official use of, authorized officials of the Federal Government, including the United States Sentencing Commission, the States, including State sentencing commissions, Indian tribes, cities, and penal and other institutions.

These subsections would accomplish several goals and assuage potential privacy concerns regarding the NGI and IPS. First, while the "physical" profiles might be included in the same software system, the subsections would clearly demarcate different standards of data collection and use for criminal identification profiles as opposed to those profiles submitted for civil purposes, such as background checks. Second, it would allow the FBI to continue to use biometric identification, both immediate and remote, for criminal subjects, but limit the collection, or creation, of remote biometric identification data for civil submissions.

By incorporating the EU Directive's principles of consent and notice the amendment could still potentially allow the FBI the same capability to include civil photos in searches with criminal photos, but with reasonable limits. It would create an "opt-out" system where currently there is no such option or control for civil data subjects in the NGI. This amendment would also limit the FBI's use of civil submissions to the purpose for which they were created: whether it be background checks or otherwise. This would halt the threat of the FBI's programs creating a de facto surveillance state where every person's face is instantaneously searchable without any legitimate showing or investigative procedures, or at the very least prevents a state in which the face becomes the identification card. Face prints could not be created from photos submitted through civil background checks without consent because the face print is "data of a different nature or form" than just a simple photo image.

VII. CONCLUSION

The FBI's new Next Generation Identification program, specifically its Interstate Photo System component, raises serious privacy concerns over its incorporation of non-criminal photos in the database and their inclusion in possible facial

recognition criminal searches. Given that the privacy rights framework in the United States is a patchwork made up of narrow, specific areas of protection, the NGI can currently navigate the spaces in between individuals' right to privacy. While individuals do not generally have a reasonable expectation of privacy to their faces under existing Fourth Amendment case law, individuals should have a right to privacy of their face prints in their civil photos submitted to the FBI. These photos should be used only as they originally consented to, which in most cases is for pre-employment background checks, rather than allowing the subsequent step of retaining the photos and depositing them into the NGI along with criminal photos. Further, the additional procedure of digitally mapping the facial features of each photo goes beyond the non-intrusiveness of observing someone's face from a distance in public. At the very least, those releasing their photos should be fully informed, by the FBI itself, as to the full use of their information, its inclusion in the NGI, and the possible ramifications of being included in FRT searches.

The EU's Data Protection and Privacy Directive grants individuals stronger controls over the collection and storage of their data, and impose stringent transparency and communication mandates on data controllers. Their existing framework would provide useful principles to be incorporated into a U.S. statutory amendment. This amendment could address the general language of 28 U.S.C. § 534, which requires the FBI, through the Attorney General, to collect and maintain identification and criminal records. The provisions of § 534 currently could be, and in practical situations such as the NGI/IPS seem to be, construed to allow for broader data collection power. This broad construction could lead to broader intrusions of individual privacy and liberty.

An amendment would address the concerns raised by the inclusion of civil submissions into the larger overall NGI database by delineating different information collection limits and different protocols for the criminal submissions and civil submissions. Criminal submissions would allow for broader collection of biometric data during the processing of criminal arrestees, within the limits imposed by the Constitution and Supreme Court precedent. Civil submissions, however, would be limited to the scope or purpose for which they were originally submitted. If an employment background check required the submission of a photo with the application to verify the identity of the person involved, then after verification is completed notice would be given to the subject and they could opt-out of their facial image being stored in the NGI or IPS. Further, modification of the data or creation of new data, such as compiling a face print from a digital image, would be prohibited outside the criminal context, unless by expressed consent or purpose for the civil context. This amendment would essentially incorporate notice and consent principles from EU privacy law that are not currently exercised in much of the US legal regime. The proposal, while still allowing the FBI to perform necessary tasks relating to identification of criminals, would also give the individual more control on the front-end due to increased access to information regarding the potential use of their facial image, and the ability to do something about it by exercising control over their biometric data.

The FBI's Next Generation Identification program and the facial recognition

capabilities of the Interstate Photo System have raised unique legal and policy concerns regarding what is private to an individual and off limits to the government. While innocent individuals do not have a right to privacy in their public faces, facial recognition technology's process of creating a face print of an image represents a foray into grayer waters than it would seem on the surface. Congress should therefore act in response to the development of new biometric technologies and limit the FBI's collection of biometric information through amendment of 28 U.S.C. § 534.

Justice Scalia noted in his dissent to *Maryland v. King*, "I doubt that the proud men who wrote the charter of our liberties would have been so eager to [submit their bodies] for royal inspection."[197] Whether talking about the Fourth Amendment to the Constitution, would-be limits under federal statute, or societal understanding of individual privacy rights, the NGI's collection, storage, and use of civil face prints represents a concerning infringement of individual liberty.

197. Maryland v. King, 133 S. Ct. 1958, 1989 (2013) (Scalia, J., dissenting).