The John Marshall Law Review

Volume 51 | Issue 3 Article 4

2018

Biometrics and Federal Databases: Could You Be In It?, 51 J. Marshall L. Rev. 589 (2018)

Angelica Carrero

BIOMETRICS AND FEDERAL DATABASES: COULD YOU BE IN IT?

BY: ANGELICA CARRERO*

I. INTRODUCTION

Technology is constantly changing, especially when it involves identification of individuals. Nowadays, things such as fingerprint scanning, facial recognition, and iris scanning are being used in everyday technology like cell-phones and building entries. Not many people think that these types of identification are a big deal. Yet, the biometric identification system uses an individual's personal information such as facial structure, eye color, size, shape, etc. Soon your personal information may not be so personal anymore.

This article serves to raise awareness of what biometrics is and how important it is to today's society. It will focus mostly on the use of facial recognition and iris scanning.[1] Not many people are aware of the dangers of using facial recognition and iris scanning; this needs to change. There are some serious privacy and security dangers concerning the storage of personal information in areas such as federal databases. However, solutions to these dangers do exist. People should be notified if their information is being stored in a federal database and consent should be required. Protections to biometric security should become more common as some people may not want their personal information to be compromised. Because today's society is filled with different types of increasingly common technological advances, people should not only be aware of the use

*Ave Maria School of Law, Juris Doctor (2018); Mount Aloysius College, Bachelor of Arts and Paralegal Certification (2015).

1. Biometrics concerns many areas, but I am solely focusing on the biometrics of facial recognition and iris scanning. If you would like to read more information about biometrics please *see generally What is Biometrics?*, IDEMIA, www.morpho.com/en/biometrics (last visited Jan. 11, 2018).

and storage of their personal information, but also should be able to prevent such use and storage from occurring against their will.

This article contains various sections and subsections. Part I describes the different types of biometrics and how biometrics are used and implemented in society. Additionally, this section will lay out the specific type of biometrics this article will address. Part II defines facial recognition and explains how it works, while Part III defines what iris scanning is and explains how it works. Next, Part IV addresses how biometrics are stored in federal databases. Part V addresses some of the privacy concerns and contains subsections describing current solutions and my solution. Lastly, Part VI introduces the security concerns to biometrics and also includes subsections describing current solutions and my solution. Please be aware that my solutions to the privacy and security concerns are just preliminary solutions that can be expanded or improved upon.

II. PART I: WHAT IS BIOMETRICS AND HOW DOES IT WORK?

"Biometrics is the measurement and statistical analysis of an individual's physical and behavioral characteristics."[2] It is usually used for identification of individuals or giving individuals access to numerous things such as cell phones or buildings.[3] Typically, there are two main classes of biometrics: physiological characteristics and behavioral characteristics.[4] Physiological characteristics concern the shape or composition of the body while behavioral characteristics concern the behavior of an individual.[5] Physiological biometrics includes facial recognition, fingerprint scanning, hand geometry, iris scanning, and DNA.[6] Behavioral biometrics include an individual's keystroke, signature, and voice recognition.[7] This article will focus on the physiological biometrics of facial recognition and iris scanning.

Many areas within the corporate, security, and consumer fields are incorporating biometrics as a form of authentication.[8]

---

2. Margaret Rouse, *Biometrics*, www.searchsecurity.techtarget.com/definition/biometrics (last visited Oct. 27, 2017); *see generally What is Biometrics?*, IDEMIA, www.morpho.com/en/biometrics (last visited Jan. 11, 2018) (referring to biometrics as all processes used to recognize, authenticate, and identify persons based on certain physical or behavioral characteristics. The characteristics are universal, unique, invariable, recordable, and measurable).

3. *Id.*

4. *Id.*

5. *Id.*

6. Tarun Agarwal, *Biometric Sensors—Types and Its Workings*, ELPROCUS, www.elprocus.com/different-types-biometric-sensors/ (last visited Oct. 27, 2017).

7. *Id.* at ¶2.

8. Rouse, *supra* note 2.

Additionally, biometric technology has played a large role in policing over the last century.[9] For example, biometrics such as facial recognition has become commonly used by law enforcement.[10] Law enforcement uses biometrics to select individuals in large crowds with considerable reliability.[11] Additionally, "there is a rapid expansion of biometric databases among the intelligence community, the U.S. military, and in the public and private sectors generally."[12] Biometric data is collected by both state and federal agencies for various purposes in the civil and criminal contexts.[13] The advances in computing has also led to the increase of a wide variety of mobile DNA and other biometric collection devices in addition to a more cost efficient solution for storing and sharing biometric data between agencies and organizations in both the federal and state levels.[14]

The whole purpose of using biometric verification for authentication purposes is because everyone is unique; therefore, individual people can easily be identified.[15] It gives an extra sense of security to the individuals using biometrics to verify that the subjects are who they say they are.[16] Biometric verification is usually a two-step process.[17] The first step consists of a record of the individual's unique characteristic being captured and then stored in a database.[18] The second step usually occurs at a later time when the verification is required.[19] In this step, a new record is taken and is usually compared to the previous record that was initially stored in the database.[20] If the newly collected data matches the previously recorded data, the individual's identity is then confirmed.[21]

---

9. Wilneida Negrón *et al*, *Biometric Technologies in Policing*, DATA & CIVIL RIGHTS: A NEW ERA OF POLICING AND JUSTICE, 1 (2015), www.datacivilrights.org/pubs/2015-1027/Biometrics_Primer.pdf (last visited Nov. 20, 2018).

10. Margaret Rouse, *Biometric Verification*, TECHTARGET NETWORK, www.search.security. techtarget.com/definition/biometric-verification.

11. *Id.*

12. Margaret Hu, *Biometric Cyberintelligence and the Posse Comitatus* Act, 66 EMORY L.J. 697 (2017), www.law.emory.edu/elj/_documents/volumes/66/3/hu.pdf.

13. *Id.*

14. Negrón, *supra* note 9.

15. Rouse, *supra* note 2; IDEMIA, www.morpho.com/en/biometrics (last visited Jan. 11, 2018).

16. *See generally* Margaret Rouse, *Biometric Authentication*, www.search.security.techtarget.com/definition/biometric-authentication (last visited Oct. 27, 2017) (discussing how biometric authentication works).

17. *See generally* Rouse, *supra* note 10 (discussing how biometric verification works and discusses how it is usually a two-step process).

18. *Id.*

19. *Id.*

20. *Id.*

21. *See generally* Rouse, *supra* note 10; *see also Facial Recognition*, TECHTARGET (Dec. 13, 2016), www.whatis.techtarget.com/definition/facial-recognition at 1 (discussing how Facebook uses facial recognition software to

III. PART II: WHAT IS FACIAL RECOGNITION?

Facial recognition can identify an individual from a digital image by comparing and analyzing facial patterns.[22] It compares live captures of individuals or their digital image data to the record of the individual that is stored in the database.[23] This is commonly used in security systems.[24] Most current facial recognition systems will use numeric codes called face prints.[25] "Current facial recognition systems will work with the face prints and can recognize eighty different nodal points, end points used to measure variables on individual's faces such as length and width of the nose, cheekbone shape, and eye socket depth."[26] The facial recognition systems will then capture the data from the nodal points on a digital image of the individual's face and store the images as a face print.[27] The face print can then be used as a basis for comparison with faces from an image or video.[28] Ultimately, the facial recognition systems that use the face prints tend to quickly and accurately identify the targeted individual, but only when conditions are favorable.[29] The drawback of the facial recognition system is that if an individual has his or her face partially obscured, or is facing to the side rather than the front, or the lighting is not proper, the verification will be less reliable.[30]

IV. PART III: WHAT IS IRIS SCANNING?

The iris is a visible but protected structure that does not usually change over time, making it unique enough for biometric

---

help automate user tagging in photographs. Each time an individual is tagged in a photograph, the software application stores information about that person's facial characteristics. When enough data has been collected about a person to identify them, the system uses that information to identify the same face in different photographs, and will subsequently suggest tagging those pictures with that person's name).

22. Agarwal, *supra* note 6.

23. *Facial Recognition*, *supra* note 21.

24. Agarwal, *supra* note 6.

25. *Facial Recognition*, *supra* note 21.

26. Agarwal, *supra* note 6.

27. *Facial Recognition*, *supra* note 21.

28. *Id.*

29. *Id.*

30. *Facial Recognition*, *supra* note 21; *see also* Lauren Davis, *Fashion that will hide you from face-recognition technology*, (Jan. 6, 2014), www.io9.gizmodo.com/how-fashion-can-be-used-to-thwart-facial-recognition-te-1495648863 (stating that "Asymmetrical haircuts can obscure one eye and radically change the way your face is framed. Makeup that doesn't enhance your features but instead places against the usual tones and symmetry of your features can make it difficult for a facial recognition system to identify cheekbones or a forehead.").

identification.[31] Even surgery cannot change the uniqueness of the iris.[32] Furthermore, blind people can use iris scanning as long as their iris is still visible.[33] Additionally, most eyeglasses and contacts will not interfere with iris scanning.[34] Iris scanning is most often used in security-related issues just like facial recognition.[35] It can be used at border crossings and by United States soldiers via handheld devices to identify the enemy.[36] Additionally, iris scanning can be used by many law enforcement agencies.[37]

Iris scanning is basically a high-resolution image of an individual's eye that can examine the uniqueness of the iris.[38] It is used to identify individuals based on their unique patterns within the ring-shaped region surrounding the pupil of the eye known as the iris.[39] When the eye is inspected at a close range, one can see that the iris has a blue, brown, gray, or green color with different patterns.[40]

To identify an individual using iris scanning, one would need a high-resolution digital camera at visible or infrared wavelengths.[41] Iris scanning uses both visible and infrared light to take a clear, high-contrast picture of the individual's iris.[42] With the camera, an individual gathers one or more detailed images of the eye.[43] The near-infrared light makes the individual's pupil very black which would then make it easier for the computer to isolate the pupil and iris.[44] When the camera takes the picture, the computer locates the center of the pupil, the edge of the pupil, the edge of the iris, and the eyelids and the eyelashes.[45] Once the picture is taken, the computer will analyze the patterns in the iris and create a code.[46]

---

31. Tracy V. Wilson, *How Biometrics Works*, HOWSTUFFWORKS, www.scient.howstuffworks.com/biometrics4.htm (last visited Oct. 27, 2017); *see also What is Biometrics?*, *supra* note 1 (stating "The iris is the colored part of the eye, behind the cornea. It is formed before birth and its appearance changes very little during a person's life.").

32. *Id.*

33. *Id.*

34. *Id.*

35. *Iris Recognition,* TECHTARGET (Mar. 5, 2012), www.whatis.techtarget.com/definition/iris-recognition.

36. Julia Angwin, *Iris Recognition: the New Fingerprinting?*, WALL ST. J. (July 13, 2011, 11:40 AM), www.blogs.wsj.com/digits/2011/07/13/iris-recognition-the-new-fingerprinting/.

37. *Id.*

38. *Id.*

39. *Iris Recognition*, *supra* note 35.

40. *Iris Recognition*, *supra* note 35; *see also* Agarwal, *supra* note 22 (describing the different iris colors and patterns and how iris recognition works).

41. *Iris Recognition*, *supra* note 35.

42. Wilson, *supra* note 31.

43. *Iris Recognition*, *supra* note 35.

44. Wilson, *supra* note 31.

45. *Id.*

46. *Id.*

After the images are captured, they are compared to an individual's iris pattern in a database that uses a specialized computer program called a matching engine.[47] The matching engine is then able to compare millions of images per second with extreme precision that is comparable to digital fingerprinting.[48]

However, in order to be accurate and dependable, the iris scanning must be performed at a fairly close range, usually within a few meters from the camera.[49] Lighting must also be suitable because it cannot produce reflections from the cornea which can then obscure part of the iris.[50] Additionally, the individual must remain fairly stationary so that the camera can take a picture of the eye.[51] Despite its drawbacks, iris scanning can be fairly accurate and useful as seen with the San Bernardino Sheriff's Department.[52] Iris scanning was found to have an error rate of one in a million as stated in a January 2011 study conducted by the National Institute of Standards and Technology.[53]

V. PART IV: FEDERAL DATABASES

One may ask, how is biometric information stored? Well, it is stored in what is known as a database. A database is an organized collection of information that is easily accessible, managed, and updated regularly.[54] The collected information is usually organized into rows, columns, and tables that are indexed to make the

47. *Iris Recognition*, *supra* note 35.

48. *Id.*

49. *Id.*

50. *Id.*

51. *Id.*

52. *See generally* Colin Lecher & Russell Brandom, *The FBI has collected 430,000 iris scans in a so-called pilot program*, THE VERGE (July 12, 2016), www.theverge.com/2016/7/12/12148044/fbi-iris-pilot-program-ngi-biometric-database-aclu-privacy-act (stating "As a modestly sized department—policing 2 million citizens with just over 1,800 sworn officers—the San Bernardino Sheriff's Department doesn't seem like it would be on the cutting edge of surveillance technology. But the department has quietly become one of the most productive nodes in a nationwide iris-scanning project, collecting iris data from at least 200,000 arrestees over the last two and a half years, according to documents obtained by *The Verge*. In the early months of 2016, the department was collecting an average of 189 iris scans each day. San Bernardino's activity is part of a large pilot program organized by the Federal Bureau of Investigation, one that began as a simple test of available technology but has quietly grown into something far more ambitious. Since its launch in 2013, the program has stockpiled iris scans from 434,000 arrestees, an FBI spokesperson confirmed.").

53. Julia Angwin, *Iris Recognition: the New Fingerprinting?*, WALL ST. J. (July 13, 2011, 11:40 AM), www.blogs.wsj.com/digits/2011/07/13/iris-recognition-the-new-fingerprinting/.

54. Margaret Rouse, *Database*, TECHTARGET (Feb. 20, 2017), www.searchsqlserver.techtarget.com/definition/database.

information easily accessible.[55] From there, the database will process workloads to update the information regularly.[56] Varying levels of information on any individual can be found on a database based on the level of interaction with the government.[57] For example, the IRS keeps details of your income from year to year, the Department of Education has information on your federal student loan payments, and if you are in the military, your fingerprints will also be on their record.[58] Additionally, if you have been in prison, the federal database would also have a file on any tattoos you may have; or if you have applied for a security clearance, your picture, as well as your friends' and family's pictures, is stored on the database.[59]

Back in the 1970s, when Bob Gellman sat in the U.S. House of Representatives, data was being stored in different areas.[60] In recent years, there has been a trend for the federal government to collaborate internally to combine the different areas to one large database accessible to different agencies.[61] This created a "mosaic effect" in which all the information that is combined creates a more complete picture of the individual.[62] Ed Felton, a Princeton computer scientist who has served as deputy chief technology officer of the United States during the Obama administrations, explained the storing of data as, "one file may contain detailed information about behavior and another might contain precise identity information. Merging those files links behavior and identity together."[63] With this more complete data, the government's focus can be on one individual rather than multiple.[64]

Since the terrorist attacks of 9/11, the federal database of Americans has turned to including biometric data that contains information from irises to palm prints to facial recognition.[65] In 2010, the Federal Bureau of Investigation (FBI) created a system called the "Next Generation Identification System" (NGI) to replace its older fingerprint system.[66] The NGI System is a $1 billion

55. *Id.*

56. *Id.*

57. Nancy Scola, *A Picture of You, in Federal Data*, POLITICO (Oct. 11, 2017), www.politico.com/agenda/story/2017/10/11/federal-data-individual-portrait-000540.

58. *See generally* Aaron Mackey, Dave Maass & Soraya Okuda, *5 Ways Law Enforcement Will Use Tattoo Recognition Technology*, ELECTRONIC FRONTIER FOUNDATION (June 2, 2016), www.eff.org/deeplinks/2016/05/5-ways-law-enforcement-will-use-tattoo-recognition-technology (describing how prisoners' biometric data is stored in a database for identification).

59. Scola, *supra* note 57, at 2.

60. *Id.*

61. *Id.*

62. *Id. at 2, 3.*

63. *Id.* at 3.

64. *Id.*

65. *Id.* at 4; *see also* Hu, *supra* note 12, at 708-09.

66. Scola, *supra* note 57, at 4; *see also generally Next Generation*

program designed by defense contractor, Lockheed Martin.[67] This system combines data such as fingerprints, iris scans, photographs, and voice data into a searchable platform used by both federal and state agencies.[68] In 2014, the FBI announced a plan to increase the collection of biometric data to account for the accuracy found in technological advances.[69] Any individual who is in this database, whether a criminal or non-criminal, will be given a universal control number (UCN) to link the data points.[70] It has even been discussed that individuals in the NGI be assigned a unique identifying number to link data to DNA profiles that are held within the National DNA Index System (NDIS), which is the national DNA database that holds DNA profiles contributed by federal, state, and local participating forensic laboratories.[71] "In May of 2016, a Government Accountability Office (GAO) study found that around thirty million photographs of nearly seventeen million people had been placed into the NGI System with about seventy percent of the photographs being mugshots and the rest being pulled from security-clearance applications and immigration records."[72]

The collection of biometric data is not restricted to just one government agency.[73] Agencies such as the Department of Homeland Security, FBI, DEA, NSA, TSA, as well as private companies all collect biometric data.[74] The biometric data is also shared between these agencies as well as the different levels of government.[75] Biometric data such as photographs and fingerprints are inputted into the NGI System database in many ways.[76] Because of this, "individuals may find their biometric information in a criminal justice database whether they directly encountered any law enforcement members or not."[77] The NGI System was developed, in part, to retain civil fingerprint submissions as well as other biographic data to create an identity record of individuals.[78] The FBI has noted the benefits of retaining the civil fingerprints with the criminal database as "providing an ongoing background check that permits employers, licensors, and other authorized

---

Identification (NGI), FBI, www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (describing the creation of the FBI Next Generation System).

67. Wilneida Negrón *et al*, *Biometric Technologies in Policing*, DATA & CIVIL RIGHTS: A NEW ERA OF POLICING AND JUSTICE, 1 (2015), www.datacivilrights.org/pubs/2015-1027/Biometrics-Primer.pdf.

68. *Id.*

69. *Id.* at 2.

70. *Id.*

71. *Id.* at 2, 3.

72. Scola, *supra* note 57, at 4.

73. Negrón, *supra* note 9, at 3.

74. *Id.*

75. *Id.*

76. *Id.*

77. *Id.*

78. Negrón, *supra* 9, at 3.

individuals to learn criminal conduct by that individual."[79] The NGI System is growing faster than what was originally projected.[80]

Biometric databases are also being used at the local level.[81] Many states are already participating in the NGI, or are making their databases compatible to others to become more efficient and facilitate easier sharing of data.[82] States and individual police departments are using the biometric technology in the law enforcement field more frequently and with little public oversight.[83] For example, the Center for Investigative Reporting and the Electronic Frontier Foundation have detailed how facial recognition software used previously by the United States military and intelligence agencies in Iraq and Afghanistan, are now being used in San Diego to identify individuals suspected of a crime.[84] These officers use the "Tactical Identification System," which is a mobile facial recognition technology, to take pictures of suspects with their mobile phones and search within the existing criminal databases for the suspect's profile.[85] Another example would be Los Angeles County building a new multimodal biometric identification system that would become the largest biometric repository outside of the FBI, and would hold records of up to fifteen million individuals.[86] Additionally, Michigan and Maryland have signed Memoranda of Understandings with the FBI to share and access facial recognition data through the NGI system.[87]

"States are expanding their biometric data collection programs by widening the criteria for those individuals whose DNA or other biometric data will be entered into state and federal databases."[88] For example, the Supreme Court ruled in *Maryland v. King* to extend the conditions under which police officers could collect DNA from suspects not-yet-charged or convicted.[89] Rhode Island also has a new DNA sampling law from 2014, which now requires anyone

79. Ernest J. Babcock, *Next Generation Identification (NGI) – Retention and Searching of Noncriminal Justice Fingerprint Submissions*, FBI, www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

80. Negrón, *supra* note 9.

81. *Id.*

82. *Id.*

83. *Id.*

84. *See generally* Lyndsay Winkley, *8 Ways Police Can Spy on Crime, and You*, SAN DIEGO UNION-TRIBUNE, www.sandiegouniontribune.com/sdut-police-technology-devices-surveillance-privacy-2015may21-story.html (last visited June 2018) (describing how military identification systems have converted to police use for identifying individuals).

85. Negrón, *supra* note 9.

86. *Id.*

87. *Id.*

88. *Id.*

89. Negrón, *supra* note 9; *see generally* Maryland v. King, 569 U.S. 435 (2013).

who is arrested for a violent crime to provide a DNA sample to the police in which the sample would be placed into the state database upon arraignment or if the individual fails to appear at his or her next court proceeding.[90]

"Law enforcement groups are also implementing programs to collect as much data as possible during routine policing work."[91] For example, in areas such as Orange County in Los Angeles, California, police have asked suspects to turn over their genetic information to bargain for reduced charges or even dismissal of the charges.[92] This tactic is known as "spit and acquit" and is being used to help expand the biometric database.[93] However, this program has been limited to only drug cases that involve possession for personal use charges.[94] Additionally, biometric data is collected from crime scenes for comparison to data that is already in the database or to create a new entry.[95]

In addition to the federal and state levels storing biometric information, numerous countries retain individual's biometric information for various reasons as well.[96] For example, Argentina collects data such as fingerprints and photographs for the purposes of criminal investigation and national security.[97] The Federal Police, Border Patrol, Coast Guard, Airport Security Police, National Registry of Individuals, and the National Directorate of Migration are the only entities that have access to the biometric data.[98] Australia has what is called the "Australian Passport Database" that stores information about passport applicants including digitized photographs.[99] These photographs are digitally matched against facial biometric information held within the database to ensure that the person has not applied for a travel document in another name.[100]

Brazil has a passport database known as "Sistema Nacional de Passaporte" and it includes personal data and biometric information such as a facial image and two fingerprints.[101]Its database is used to process passports and for record keeping.[102] Usually only the Federal Police would have access to the data unless

90. *Id.*
91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.*
95. *Maryland*, 569 U.S. 435.
96. *See generally* Ruth Levush, *Biometric Data Retention for Passport Applicants and Holders*, THE LAW LIBRARY OF CONGRESS (Mar. 12, 2014), www.loc.gov/law/help/biometric-data-retention/biometric-passport-data-retention.pdf.
97. *Id.*
98. *Id.*
99. *Id.*
100. *Id.*
101. Levush, *supra* note 96.
102. *Id.*

another agency has entered into an agreement with them.[103] Finally, Canada has a facial recognition database that uses biometric data to help screen passport or travel document applicants by matching the photographs submitted by passport applicants against facial biometric information held in the Passport Database.[104]

VI. PART V: WHAT ARE THE PRIVACY ISSUES OF BIOMETRICS?

Privacy in the United States is not an explicit right for every citizen.[105] There is privacy protection for specific instances, but generally, it has been left up to the states to determine a more extensive privacy protection.[106] Some states have general privacy laws that grant citizens privacy rights beyond the federal privacy protection.[107] The root of the right to privacy lays within the Fourth Amendment of the United States Constitution.[108] The Fourth Amendment gives citizens the right to be protected from warrantless searches by the government.[109] Basically, 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."[110] "As the Court noted in *Kyllo*: 'a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.'"[111]

The only general rights to privacy given to individuals are specifically applied to personal information stored within government systems.[112] These general rights are protected through the Privacy Act.[113] The Privacy Act operates on the idea that the individual's information is already on the government database and, therefore, offers protections on how that information should be

103. *Id.*

104. *Id.*

105. Christopher DeLillo, Note, *Open Face: Striking The Balance Between Privacy and Security With The FBI's Next Generation Identification System*, 41 J. LEGIS. 264 (2015).

106. *Id.*

107. *Id.*

108. *Id.* at 270 (stating how 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").

109. *Id.*

110. *Id.*

111. *Id.* at 271-72.

112. *Id.* at 277.

113. DeLillo, *supra* note 105, at 277-78.

handled and who should have access to the information.[114] The Act's focus is on protecting individuals' personal data within government systems to prevent inadvertent or malicious disclosure of personal information to parties not permitted to have access to such data.[115] After the terrorist attacks on 9/11, the USA Patriot Act was passed.[116] This Act gave the government more powers of surveillance and information collection which tend to intrude upon the privacy of individuals due to national security concerns.[117]

Because of this, there are few legal limitations on how the government can collect and share biometric data.[118] In 2013, in *Maryland v. King*, the Court ultimately decided that an arrestee's interest in keeping his or her biometric information private does not outweigh the legitimate government interest in obtaining that biometric information.[119] This permits the police to collect biometric information from anyone arrested for any reason.[120] In addition to the arrestee's personal information being stored in databases, there is also a legal theory known as the Third Party Doctrine.[121] The Third Party Doctrine has been upheld in numerous Supreme Court rulings and states anything that an individual has shared with another party no longer holds an expectation of privacy such that it is not considered a "search" under the Fourth Amendment and thus permits the government to collect the information.[122] This legal theory allows the government to collect the biometric information without a search warrant as long as individuals opt to share their biometric information either for immigration purposes or even for employment purposes.[123]

As of August 31, 2017, the FBI's NGI System database is exempt from certain parts of the Privacy Act.[124] For example, "the public will not be able to find out if their fingerprints, iris scans, and other biometric information is stored in the Next Generation Identification System."[125] The reasoning behind this new rule is that the knowledge of the records the FBI has on file about an individual could "specifically reveal investigative interest by the

114. *Id.* at 278.
115. *Id.*
116. *Id.*
117. *Id.*
118. Negrón, *supra* note 9.
119. *Id.*
120. *Id.*
121. *Id.*
122. *Id.*
123. Negrón, *supra* note 9.
124. Mohana Ravindranath, *If the FBI Has Your Biometrics, It Doesn't Have to Tell You*, NEXTGOV (Aug. 2, 2017), www.nextgov.com/cio-briefing/2017/08/if-fbi-has-your-biometrics-it-doesnt-have-tell-you/139952/print/.
125. Justin Lee, *FBI's biometrics database to be exempt from parts of Privacy Act*, BIOMETRIC UPDATES (Aug. 3, 2017), www.biometricupdate.com/201708/fbis-biometrics-database-to-be-exempt-from-parts-of-privacy-act.

FBI or agencies that are recipients of the disclosures."[126] The NGI System raises privacy concerns because it incorporates noncriminal photos for its facial recognition database.[127] The existing privacy protections in the United States do not provide individuals with adequate protection for this concern.[128] Federal law requires the Attorney General to collect and maintain identification and criminal records.[129] To allow the exemption, the FBI cited 28 U.S.C. § 534 to permit the implementation and operation of the NGI System.[130] This statute is broad enough to allow any piece of information that relates to identification records to be stored in a database which would lead to potential abuse of the scope or intention of the statute.[131]

A. ARE THERE ANY SOLUTIONS?

Essentially, the existing United States privacy laws do not offer much protection from government collection and misuse of biometric data.[132] The current law requires the collection of biometric data for the purposes of identification with few limitations.[133] The United States government has been looking at the possibility of consent and ways to oversee biometrics, but it is still legal in 47 states for software to identify an individual using images taken without consent while the individual is in the public.[134] Because the United States has few legal limitations on how the government can collect and share biometric data, we can look towards the law of other countries.

For example, the European Union offers a privacy framework.[135] This privacy framework is known as the Data Protection Directive and it grants general privacy rights and outlines responsibilities for data handlers.[136] In addition to the protections, the Directive allows for efficient and necessary use of data by various entities including the government and law

126. *Id.*
127. DeLillo, *supra* note 105, at 264-65.
128. *Id.* at 266.
129. *Id.*
130. DeLillo, *supra* note 105, at 266; *see generally* 28 U.S.C. § 534 (2011).
131. *Id.*
132. *Id.* at 285.
133. *Id.*
134. April Glaser, *Biometrics Are Coming, Along With Serious Security Concerns*, WIRED (Mar. 9, 2016), www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns; *see also* Dan Tynan, *What are the risks of biometric identification?*, THE PARALLAX (Feb. 21, 2017), www.the-parallax.com/2017/02/21/risks-biometric-identification (stating how Connecticut, Texas, and Illinois are the only states that have enacted privacy laws for individuals' biometrics. Specifically, Texas and Illinois prohibit software to identify individuals without their consent).
135. DeLillo, *supra* note 105, at 264.
136. *Id.* at 264-65.

enforcement.[137] The Directive provides various restrictions on entities collecting or processing data.[138] The first obligation placed on entities is that the data collected must be collected for an explicit and legitimate purpose and used according to that specific purpose only.[139] Next, the data that has been collected must be adequate, relevant, and not excessive in relation to the purpose for which it was originally collected.[140] If there is any inaccurate or irrelevant data, that data must be deleted or corrected.[141] Finally, the personal information that is used cannot be kept longer than what was strictly necessary for the specific purpose for which it was obtained.[142]

In addition to laying out obligations for the entities collecting the data, the Directive also provides individual rights for those who are the subject of the collected data.[143] The individual who is the subject of the collected data must be informed at the time of the collection.[144] He or she must be informed about the information that is being processed, the purpose for the collection, and to whom the data could be transferred to.[145] The individual is also given the opportunity to request deletion of the data, to request the blocking of the data, or to request for modifications of any inaccurate information.[146] The main purpose of the Directive is to ensure that there is notice, consent, security, and transparency of the stored data.[147]

When looking outside of the European Union, countries such as Argentina implement time constraints on the collected biometric data.[148] Even Australia has implemented a system where if the collected biometric information is no longer needed for the purpose for which it was collected, reasonable steps are taken to destroy the information or to ensure that the information is de-identified.[149] Additionally, South Korea provides a procedure where the keeping and managing of biometric data cannot exceed three months.[150] And finally, New Zealand enacted the Privacy Act of 1993 to apply to biometric information and requires that the personal information not be held longer than what is required to complete the purpose of

137. *Id.* at 265.
138. *Id.* at 284.
139. *Id.*
140. DeLillo, *supra* note 105, at 284.
141. *Id.*
142. *Id.*
143. *Id.*
144. *Id.*
145. DeLillo, *supra* note 105, at 284.
146. *Id.*
147. *Id.*
148. Ruth Levush, *Biometric Data Retention for Passport Applicants and Holders*, THE LAW LIBRARY OF CONGRESS (Mar. 12, 2014), www.loc.gov/law/help/biometric-data-retention/biometric-passport-data-retention.pdf.
149. *Id.* at 2.
150. *Id.* at 5, 6.

the data collection.[151]

B. MY SOLUTION TO THE PRIVACY ISSUE

When looking at the government's reasoning to permit the collection of biometric information for criminals or for national security reasons, it would be plausible to allow the government to collect the personal information without needing a warrant or obtaining consent.[152] The reasoning behind this aspect is to refrain from impeding on the government's task of providing protection to its citizens. However, it is a different story when the biometric data is collected on regular citizens just because they are walking out in the public or using technology that collects the biometric data.[153] When it comes to collecting the personal biometric data of regular citizens, there should be a combination of the European Union's Data Protection Directive as well as the adoption of time limitations that various countries such as Argentina, Australia, and New Zealand implement.[154] Therefore, notice and consent should be obtained as well as the requirement of informing the individual of what information is being stored. Additionally, there should be a provision to provide the individual an opportunity to correct any inaccurate information.

There should also be a permission form that requires the individual's signature that would allow the government to keep the stored information for any potential criminal use. If the form is not signed, then the time limitation should be implemented where the information that was collected for a specific purpose should be deleted within a reasonable time such as one to three months. Notice of the deletion of the information should also be sent to the individual in which the information was taken and stored for accountability purposes. The point of this solution is to still allow the government to do its job when it comes to national security issues, but also provide a fair opportunity to the other law-abiding citizens of the United States who may not even be aware that their biometric data is being taken and stored in a federal database.

---

151. *Id.* at 6.

152. *See generally* Negrón, *supra* note 9 (indicating a national security reason for collecting biometric information from criminals); *see also generally* DeLillo, *supra* note 105 (supporting the national security reason for collecting biometric information from criminals).

153. *See generally* Negrón, *supra* note 9 (discussing that the government is also collecting biometric information from law-abiding citizens without their knowledge).

154. *See generally* Levush, *supra* note 96.

VII. PART VI: WHAT ARE THE SECURITY ISSUES OF BIOMETRICS?

Biometric security has significant advantages over other forms of authentication because it is fast and easy to use unlike logins or passwords.[155] Biometric authentication is seen as being safer to use than the everyday password because everyone's biometric data is unique, thus making it more difficult to hack.[156] Even though biometrics have their advantages, such as not having to remember a password, it also has characteristics that raise new security concerns.[157] Biometrics differ from passwords because the data collected is slightly different each time.[158] Therefore, biometric systems must adapt to such variations.[159]

The systems adapt to the variations by relying on pattern recognition.[160] To use pattern recognition, the biometric data that is collected at the first use is stored on the device for comparison with the additional data that is introduced at other times to create a pattern that can be identified.[161] This can cause a security hole because an attacker who gains access to the device can also have access to the biometric data that had been collected.[162] A large security concern arises because a person cannot generate new biometrics when their biometric data has been compromised.[163] There are a variety of threats to biometric systems at various points of the data collection and retention.[164] For example, individual biometric collection modules can be tampered with by attackers by including a fake feature extraction module that produces pre-selected features that will permit the attacker to gain access to the biometric data.[165] Other examples include dishonest entities like servers that will impersonate a user or perform data mining to gather information.[166]

In August of 2016, at a Usenix security conference, security

155. Charles Williams, *Biometric Authentication: An Added Layer of Security or Security Risk?*, DIGICERT (Apr. 11, 2016), www.digicert.com/blog/biometric-authentication-methods.

156. Alienor, BIOMETRIC AUTHENTICATION: ISSUES & INNOVATIONS, www.plixer.com/blog/cybersecurity/biometric-authentication-issues-innovations/ (last visited Jan. 1, 2018).

157. Anthony Vetro, et al., *Securing Biometric Data*, MITSUBISHI ELECTRIC RESEARCH LABORATORIES, (Apr. 2009), www.citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.436.5889&rep=rep1&type=pdf. (last visited Nov. 15, 2018).

158. *Id.* at 1.

159. *Id.*

160. *Id.*

161. *Id.*

162. Vetro, *supra* note 156.

163. *Id.*

164. *Id.* at 2.

165. *Id.*

166. *Id.*

and computer vision specialists from the University of North Carolina successfully showed how it was possible for a 3-D rendering of a face, through virtual reality, could fool facial recognition authentication systems into allowing access to a cell-phone.[167] The specialists from the University of North Carolina created digital 3-D facial models based on publicly available photos from places such as Facebook, Linked In, and Google+.[168] They then used a virtual reality system to show the model to the facial recognition authentication systems.[169] The five authentication systems that were used were KeyLemon, Mobius, TrueKey, BioID, and 1D.[170] These systems were chosen because they can be used by anyone and can be easily downloaded from Google Play vendors or from iTunes.[171] The specialists had the volunteers program their smartphone to detect their real faces after downloading the authentication system onto the cellphone.[172] From there they showed 3-D renders of each volunteer through virtual reality to the facial recognition systems to see if the system would accept the facial rendition.[173] The specialists were able to trick all five systems each time it was tested when they used indoor headshots of each participant for the 3-D facial models; they were also able to trick four out of the five systems when using photos obtained from Facebook, Linked In, or Google+ for the 3-D facial models.[174]

Overall, it has been proven that biometric data is easier to hack than passwords because the data is subjected to all current attacks and was never designed to be kept a secret.[175] A drawback with

---

167. Lily Hay Newman, *Hackers Trick Facial-Recognition Logins With Photos From Facebook (What Else?)*, WIRED (Aug. 19, 2016), www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/. (last visited Nov. 20, 2018).

168. *Id.*

169. *Id.*

170. *Id.* at 5.

171. *Id.*

172. Newman, *supra* note 167.

173. *Id.*

174. *Id.* at 5-6.

175. Alienor, BIOMETRIC AUTHENTICATION: ISSUES & INNOVATIONS, at 3, www.plixer.com/blog/cybersecurity/biometric-authentication-issues-innovations/ (last visited Jan. 1, 2018) (discussing the potential problems biometric authentication can have); *see also* Jeremy Bergsman, *Biometrics are less secure than passwords—this is why*, BETANEWS (Aug. 24, 2016), www.betanews.com/2016/08/24/unsafe-biometrics (indicating how biometric authentication is less secure than a regular password); *see also* Kevin Howell, *3 Reasons Biometrics Are Not Secure*, DEFRAG THIS (Aug. 28, 2017), www.blog.ipswitch.com/3-reasons-biometrics-are-not-secure (some additional examples of successful hacking include: famous hacker Jan Kressler unlocking iPhones by creating a fake finger. He also obtained high resolution photos of German Minister of Defense Ursula von der Leyen's fingerprint from press conferences and reconstructed the thumbprint by using specific software. Additionally, hackers fooled Samsung's S8 iris recognition system by placing a contact lens over a photo of a user's eye and unlocking the phone); *see also*

biometrics is that as new security technology progresses, so does the sophistication of attacks on biometric systems.[176] This creates a problem with compromises to biometric systems because biometric data is both unique and personal, and if someone were to steal the data, it could be used to falsify travel and legal documents as well as criminal records.[177] Additionally, biometric data is not revocable, meaning that it cannot be thrown away and replaced like a password or a credit card number if a compromise occurs.[178] Ultimately, biometric data is permanently associated with the individual.[179] Therefore, data breaches are very common and storing any kind of personal data poses enticing rewards to hackers as seen when 5.6 million fingerprints of United States federal employees were stolen in September of 2015.[180]

"There are three ways in which a biometric system can be compromised: system circumvention, verification fraud, and enrollment fraud."[181] System circumvention avoids using the biometric system as it was intended.[182] For example, "the system could be bypassed for administrative purposes by using a 'backdoor' to provide easy access that can give a hacker a vulnerability to exploit."[183] The verification fraud attempts to bypass the biometric systems during the verification process itself.[184] Some examples of this fraud includes forcing individuals to verify their identity to gain access by presenting a copy of the actual biometric data.[185] Enrollment fraud consists of the basic question of whether the individuals are who they say they are, which is similar to identity theft.[186]

A. ARE THERE ANY SOLUTIONS?

To combat some security issues, companies have tried to

Killian Bell, *iPhone's Touch ID hacked with Play-Doh*, IPHONE HACKS (Feb. 6, 2016), www.iphonehacks.com/2016/02/iphone-touch-id-hacked-with-play-doh.html (Jason Chaikin, president of mobile security firm Vkansee, illustrated in a video how it is possible to unlock an iPhone with a Play-Doh fingerprint from a cast of a finger that was made in dental paste).

176. Alienor, *supra* note 156.

177. *Id.*

178. Bergsman, *supra* note 175.

179. *Id.*

180. Olivia Solon, *The end of passwords: biometrics are coming but do risks outweigh benefits?*, THE GUARDIAN 1, 3 (Dec. 8, 2015), www.theguardian.com/technology/2015/dec/08/the-end-of-passwords-biometrics-risks-benefits.

181. Wayne Penny, *Biometrics: A Double Edged Sword – Security and Privacy*, SANS INSTITUTE INFOSEC READING ROOM 1, 6 (2002), www.sans.org/reading-room/whitepapers/authentication/biometrics-double-edge-sword-security-privacy-137.

182. *Id.*

183. *Id.*

184. *Id.*

185. *Id.*

186. Penny, *supra* note 181.

implement new ways to secure the storage of biometric data.[187] For example, Mitsubishi has aimed to secure biometric systems by using an approach that uses "syndrome" bits from a Slepian-Wolf code as a secure biometric.[188] The syndrome bits by themselves do not contain enough information to trace the user's biometric data back to them.[189] However, when it is used with a second reading of the user's biometric information, the syndrome bits would enable the system to recover and verify the user's biometric data.[190] Another method to secure a biometric system is the "transformation-based" method.[191] This method extracts features from the collected biometric data by using a complicated transformation.[192] Authentication of the data would be performed by the pattern matching of the transformed data whereby security comes from the good transformation, which masks the original biometric data.[193] Some examples of this method are score matching-based techniques and threshold-based biohashing.[194]

The helper data method is another method that can be used to secure biometric systems.[195] This method is user-specific and the helper data is created and stored from the original biometric data.[196] The created helper data can actually be known to people and does not need to be kept a secret.[197] For authentication purposes, the helper data is used to reconstruct the original biometric data from other biometric data.[198] This method, however, is not sufficient by itself and a cryptographic hash of the original biometric data should also be used.[199]

---

187. Vetro, *supra* note 157.

188. *Id.*; *see also* Brian M. Kurkoski, *Slepian-Wolf coding*, SCHOLARPEDIA, www.scholarpedia.org/article/Slepian-Wolf-coding (illustrating how Slepian-Wolf coding deals with the lossless compression of two or more correlated data streams. Each stream is encoded separately and the compressed data from all of the encoders are jointly decoded by one single decoder into two correlated streams. Lossless compression means that the source outputs can be constructed from the compression version with arbitrary small error rates).

189. Vetro, *supra* note 157.

190. *Id.*

191. *Id.*

192. *Id.*

193. *Id.*

194. Vetro, *supra* note 157.

195. *Id.*

196. *Id.*

197. *Id.*

198. *Id.*

199. Vetro, *supra* note 157; *see also* Tim De Chant, *The Boring and Exciting World of Biometrics*, NOVA NEXT (June 18, 2013), www.pbs.org/wgbh/nova/next/tech/biometrics-and-the-future-of-identification/ (stating how "Hashes are widely used in computing as a way of encoding data that masks information about the original. They are commonly used to store passwords in databases. Each hashed password is unique, and changing just one character in a password produces a hash that is completely different. Depending on the hashing function, decoding a hash can be extremely time consuming. You can

Some other solutions to help prevent compromises in biometric systems is using cryptography and using digital signatures.[200] Cryptography used in conjunction with biometrics is known as biometric encryption.[201] It is an emerging technology that can securely bind a digital key to biometric data so that no actual biometric image or template is stored.[202] What is actually stored in the database is helper data.[203] Other solutions include using a PIN number or something unique that the individual knows in correlation with the biometric system to provide more security.[204] "Many business, government, and institutional sites require a second factor to biometrics such as a SecurID fob to provide additional security."[205]

B. MY SOLUTION TO THE SECURITY ISSUE

Providing the utmost security for individuals looking to be a participant in biometric systems is important. As stated earlier, biometric data is very personal and is unchanging.[206] Preventing hackers from accessing such important information is a reason why biometric systems should have a great deal of security measures.

---

cryptographically hash any digital file, including images of fingerprints and other biometrics. Hashes are relatively secure because they are computed using one-way functions, which means they are computationally easy in one direction (encrypting) but hard in the other (decrypting)").

200. Penny, *supra* note 181.

201. Ann Cavoukian & Alex Stoianov, *Biometric Encryption Chapter from the Encyclopedia of Biometrics*, OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER 1, 2, www.ipc.on.ca/wp-content/uploads/Resources/bio-encrypt-chp.pdf (stating that biometric encryption is a process that securely binds a digital key to a biometric or generates a key from the biometric. In essence, the key is "encrypted" with the biometric, and the resulting biometrically encrypted key, also called BE template or helper data, is stored. The digital key can be "decrypted" on verification if a correct biometric sample is presented).

202. *Id.* at 1.

203. *Id.*

204. *Id.* at 7.

205. Dr. Thomas P. Keenan, *Hidden Risks of Biometric Identifiers and How to Avoid Them*, CANADIAN GLOBAL AFFAIRS INSTITUTE 1, 2 (2015) (discussing ways to avoid some of the risks that biometric identification can create.), www.blackhat.com/docs/us-15/materials/us-15-Keenan-Hidden-Risks-Of-Biometric-Identifiers-And-How-To-Avoid-Them-wp.pdf; *see also RSA SECURED HARDWARE TOKENS*, RSA, www.rsa.com/content/dam/rsa/PDF/h13821-ds-rsa-securid-hardware-tokens.pdf (stating how a SecurID Fob is an authentication mechanism that consists of a token—either hardware or software—which is assigned to an individual that creates an authentication code at fixed intervals using a built-in clock and the card's factory encoded key (or fob)).

206. *See generally* Alienor, *supra* note 156 (illustrating how biometrics is unique and personal.); *see also* Jeremy Bergsman, *Biometrics are less secure than passwords—this is why*, BETANEWS (Aug. 24, 2016), www.betanews.com/2016/08/24/unsafe-biometrics/ (discussing how biometrics is unique and personal).

An important step is to attempt to make it more difficult for hackers to be able to access the biometric data when the biometric database is hacked. Individuals should not have to worry every day about whether a hacker has stolen their biometric data. Therefore, the first thing that can be done to make a biometric system more secure is attempt to keep certain information about the system a little more private so it can be less appealing to hackers or more difficult for hackers to compromise.[207] Essentially, the less that hackers know, the more difficult their work will become in trying to obtain an individual's biometric data stored in a biometric system database.

With that being said, as a possible solution to ensure a more secure biometric system, the combination of cryptography and the transformation method where the original biometric data is transformed to a different pattern would likely be the most beneficial.[208] Cryptography itself has proven to be effective, but it would still be possible to hack when a hacker has plenty of time to attempt to decrypt the codes.[209] To enhance the security of both methods, one could attempt to transform the created patterns into new ones in cycles of every three or four months. This could prevent a hacker from trying to access the data because the different codes and patterns connected to the biometric data would be constantly changing, thus making it more difficult for hackers to gain access to the biometric system. To create a sense of transparency and security between the user and the organization holding the biometric data, letters giving notices and updates about their biometric data may also prove to be beneficial.

VIII. CONCLUSION

Many people enjoy the idea of using biometrics because it makes tasks such as entering buildings or unlocking their phones much easier than having to type in passwords or using a key fob. Even though biometrics is easy to use and is portrayed as being secure, there are still several risks involved with biometrics.[210] These risks come in the form of both privacy and security concerns.

---

207. *See generally* Alienor, *supra* note 156 (discussing ways to make biometrics more secure.); *see also generally* Bergsman, *supra* note 175 (supporting the discussion that steps can be taken to make a biometric system more secure and less hackable).

208. *See generally* Penny, *supra* note 181 (discussing how cryptography and the transformation method works to make important information less hackable).

209. *See generally* Cavoukian & Stoianov, *supra* note 201 (discussing the basics of cryptography).

210. *See generally* Alienor, *supra* note 156; (illustrating some of the risks of biometrics); *see also* Bergsman, *supra* note 175 (illustrating how biometrics can be hackable); *see also* Vetro, *supra* note 157 (providing additional illustrations of how biometrics is hackable).

Biometric information is stored in databases that are widely used by multiple agencies, such as the Department of Homeland Security, FBI, DEA, NSA, TSA, as well as private companies.[211] This shows the accessibility of an individual's biometric data and raises privacy concerns. Essentially, the United States offers little protection to individuals from government collection and misuse of biometric data on a federal level.[212] Because of this, it is important to find a solution to combat such privacy concerns. This would include an opportunity to inform individuals about their biometric data being stored in databases and sending a consent form to individuals to permit such use of their biometric data. The storage of such information should only be that of what is deemed necessary at the time that the biometric data collection is needed.

Biometrics also raises security concerns. Hackers have an interest in biometrics because the technology is progressing quickly and the information about biometric systems is not kept a secret.[213] If hackers were to gain access to an individual's biometric information, the repercussions would be great. This is because, unlike passwords or logins, biometric data cannot be changed. It is essentially identity theft and the individual affected would suffer greatly because the hacker can use the biometric data to falsify travel or legal documents or even criminal records. A way to thwart hackers is to make the biometric system more secretive and create encryptions and transformation patterns for biometric data to make it more challenging for hackers to obtain the personal information. To keep a rotational system of changing the patterns every couple of months will also help make a hacker's job more challenging.

Society today aims to make the everyday life easier through numerous technological advances. This is what makes biometrics so enticing to many individuals. Its ease to give individuals access to their phones or buildings by just a scan of the face or the use of a fingerprint draws individuals to using it so often. However, what is overlooked by many is the fact that the biometric data that is collected is so personal and unique to the individual that any compromise of such data can have life-changing repercussions. An individual's identity can easily be stolen by hackers if the biometric system in which the personal information is stored is compromised. Some individuals may not even realize that their personal information has already been taken just by walking out in the public. Biometrics may seem like a great idea, but without the proper privacy and security protections, it can be a disastrous concept, especially if an individual's personal information has been taken without him or her even knowing. Ultimately, there is one

211. Negrón, *supra* note 9.

212. De Lillo, *supra* note 105, at 285.

213. *See generally* Alienor, *supra* note 156 (discussing how hackers are interested in biometrics because it is something that is new and progressing very quickly without additional securities being added to it).

question that all individuals should ask themselves: is my biometric data already in a database?