With Great Technology Comes Great Responsibility: Why Smartphone Users' Biometric Data Needs to Be Protected

J. P. Raynal

Maurice A. Deane School of Law at Hofstra University

Follow this and additional works at: https://scholarlycommons.law.hofstra.edu/hlr

Part of the Law Commons

Recommended Citation


Available at: https://scholarlycommons.law.hofstra.edu/hlr/vol48/iss1/7
NOTE

WITH GREAT TECHNOLOGY COMES GREAT RESPONSIBILITY:
WHY SMARTPHONE USERS’ BIOMETRIC DATA NEEDS TO BE PROTECTED

I. INTRODUCTION

Imagine an individual going about a daily routine, only to find out later that the person’s face has been stolen without their consent.¹ This nightmare became all too real for Lindabeth Rivera of Illinois in the months leading up to March 2016.² Lindabeth was one of many victims of biometric identity theft, as approximately eleven photographs were taken of her by a “Google Droid” device and automatically uploaded to Google’s cloud-based storage service, Google Photos.³ It didn’t stop there: Google then created a unique face template by scanning Lindabeth’s facial and geometric features without first obtaining her consent.⁴ In Rivera v. Google, Inc., Lindabeth sued Google for violating Illinois’s Biometric Information Privacy Act (“BIPA”), which forbids the unauthorized collection and storing of a subject’s biometric data.⁵

Joseph Weiss joined Lindabeth in her suit against Google on the same grounds.⁶ Google took photographs directly from Joseph’s own smartphone device and used those photographs to unlawfully create a face scan of Joseph’s facial features.⁷ In both situations, the photos were immediately uploaded to Google Photos and scanned to create custom face-templates that map and record distinct facial measurements and contours.⁸

² Id.
³ Id.
⁴ Id.
⁵ 740 ILL. COMP. STAT. § 14/15(b) (2008); see Rivera, 238 F. Supp. 3d at 1090, 1093.
⁶ Rivera, 238 F. Supp. 3d at 1090-91.
⁷ Id. at 1091.
⁸ Id.
Google did not simply use the photographs to map the subjects’ facial features, but further used the illegal face-templates to recognize Lindabeth’s and Joseph’s age, location, gender, and race, among other things. In both cases, at the time of uploading and scanning, the devices were in the state of Illinois and carried Illinois IP addresses. The only difference between the two stories is that Joseph was a user of his own Google Droid smartphone and Google Photos, whereas Lindabeth had neither a Droid nor a Google Photos account.

In *Rivera v. Google, Inc.*, suit was brought in federal district court in Illinois by Lindabeth and Joseph, individually and on behalf of a class of people similarly situated. The plaintiffs argued that the face geometry templates created by Google are “biometric identifiers” and thus are protected under the BIPA. Their stories are just two examples of the privacy horrors facing today’s society as the use of biometrics grows across industries. These horrors constitute threats to citizens’ privacy and civil liberties as biometrics like facial recognition can easily be used to identify large amounts of people and can be used for indiscriminate surveillance of the general public.

The advancement of smartphone technology and the constant need to remain relevant has led to the prevalence of biometric and facial recognition technology in smartphones. What was once known as a “landline” telephone is slowly fading out of memory. Nowadays, smartphone devices continue to advance at breakneck speeds, further impacting the entire globe with seemingly no end in sight. Apple has indicated that facial recognition is not intended for children under thirteen years of age, due to the fact that their faces have not fully developed distinct facial features; as such, their use of facial recognition can lead to increased security risks. It is unclear, however, whether Apple

---

9. *Id.*
10. *Id.*
11. *Id.*
12. *Id.*
13. *Id.*
16. *See infra* Parts II–IV.
18. *Id.*
recognizes any security concerns about collecting and storing children’s biometric identifiers.  

Notably, the storage capacity of smartphones is what makes them so popular, and yet, so dangerous. Smartphone devices can “store and disseminate huge amounts of data, photos, financial records, emails, instant messages, notes and other information.” However, this data is secured by passcodes or biometric sensors, leaving many smartphone users viewing fingerprint identification as a secure means to protect biometric and other sensitive information stored on mobile devices.

Regardless of how impressive it is to have such great technological power in peoples’ hands, such “[t]echnological advances have turned our privacy jurisprudence on end.” Chief Justice John Roberts has opined that “some of the [C]ourt’s most challenging cases involve applying long-held rules created by the courts to quickly developing technology.” This new technology has given rise to the biometric system, a security system that recognizes the user registered to that particular smartphone. Once this information is in a database, “biometric authentication can then be used to either verify an individual’s identity, or to identify an unknown person.” What was once a concept of fiction, employed by the likes of James Bond and other high-tech spies on the big screen, has now become a reality.

While biometric technology is a recent phenomenon in smartphones, the use of biometric identification is nothing new to the federal government. In the final year of his presidency, President George W. Bush issued the Directive on Biometrics for Identification and Screening To Enhance National Security which established a framework to ensure that Federal executive departments and agencies . . . use mutually compatible methods and procedures in the

20. Id.
22. Id. at 126.
27. Id. at 641; see Erin M. Sales, Note, The “Biometric Revolution”: An Erosion of the Fifth Amendment Privilege to be Free from Self-Incrimination, 69 U. MIAMI L. REV. 193, 213-14 (2014).
29. Sales, supra note 27, at 214.
collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law.\textsuperscript{30}

Furthermore, government fingerprint identification has been used in the criminal context “since the early twentieth century.”\textsuperscript{31} Biometric identifiers, such as fingerprint scanning, became such a source of confidence among law enforcement agencies that its use and popularity quickly transitioned to the private sector.\textsuperscript{32}

The ease with which biometric scanners can be embedded into smartphones has led to “fingerprint-based authentication becoming more and more popular in a number of civilian and commercial applications such as, welfare disbursement, cellular phone access, and laptop computer log-in.”\textsuperscript{33} Further, the uniqueness of fingerprints adds to its popularity among smartphone users, as “all fingertips have unique ridge formation patterns.”\textsuperscript{34} Because an individual’s fingerprint is so unique and doesn’t change over time, fingerprint-scanning is a quick, easy, and noninvasive method of authenticating a smartphone user.\textsuperscript{35} However, fingerprint authentication has its drawbacks, as fingerprints can easily be lifted from surfaces with tape.\textsuperscript{36} Despite this, the biometric systems market continues to grow.\textsuperscript{37}

The value of the biometrics system market has been growing exponentially.\textsuperscript{38} In 2017, the biometrics system market was valued at “USD 13.89 billion ... and is expected to reach USD 41.80 billion by 2023, at a [Compound Annual Growth Rate] of 19.99% during the forecast period.”\textsuperscript{39} Among the multifactor authentication methods in

\textsuperscript{30} Id. at 214; see Directive on Biometrics for Identification and Screening to Enhance National Security, 1 PUB. PAPERS 757 (June 5, 2008) (acknowledging that many agencies were already collecting biometric information in their identification and screening processes, and that the harmonization of their collecting, storing, and sharing procedures would help identify “individuals who may do harm to Americans and the Nation”).

\textsuperscript{31} Sales, supra note 27, at 215.

\textsuperscript{32} Id.

\textsuperscript{33} Id. (quoting A. Jameer Basha et al., Efficient Multimodal Biometric Authentication Using Fast Fingerprint Verification and Enhanced Iris Features, 7 J. COMPUTER SCI. 698, 698 (2011)).

\textsuperscript{34} Sales, supra note 27, at 215.

\textsuperscript{35} Id.

\textsuperscript{36} Id.

\textsuperscript{37} Biometric System Market by Authentication Type (Single-Factor and Multifactor), Functionality Type (Contact, Non-Contact, and Combined), Component (Hardware and Software), Application, and Geography – Global Forecast to 2023, MARKETSANDMARKETS (July 2018), https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html.

\textsuperscript{38} Id.

\textsuperscript{39} Id. (explaining that the base year used for the biometrics system market study is 2017, and
biometrics systems, “pin [codes] with biometrics held the largest share in 2017. The systems based on both biometrics and PIN are cost-effective and use a secure method for authentication compared with other multifactor authentication systems.”40

Biometric technology has been around for years; “in the 1960s, scientists (both civilian and military) began to explore the technological ability to ‘identify, at a distance, specific individuals among the enemy ranks.’”41 Apple, however, brought biometric technology into users’ homes when it started using biometric technology in its devices in 2013.42 Apple’s announcement that the iPhone 5S “would include a fingerprint scanner to support its then-new Touch ID security protocol” changed the smartphone game.43 Fast-forward to April 2017 when Apple’s rival manufacturer, Samsung, released its flagship Galaxy S8 in the United States.44 The technology in the Galaxy S8 included facial and iris recognition technology, along with a fingerprint scanner, “something noticeably absent from the iPhone X,” which was released in the United States in November 2017.45

In late September 2018, Apple released a trio of iPhones, namely the iPhone XS, iPhone XS Max, and iPhone XR, all of which boast Apple’s latest A12 Bionic processor.46 Aside from 50% increased speed and a tremendous increase in storage capacity, the A12 Bionic processor’s neural engine is used for “running machine learning and artificial intelligence software used in everything from recognizing faces to understanding voice commands.”47

Most recently, according to a Techspot article, a full-screen fingerprint scanner patent submitted by Samsung was published in

the forecast period is 2018–2023).

40. Id.


43. Id.

44. Id.


October 2018.\textsuperscript{48} The patent proposed an upgrade to already-existing smartphone biometric sensors, by describing “using a biometric scanner built into the display layer itself.”\textsuperscript{49} Currently, smartphones equipped with biometric sensors require users to touch a particular portion of the screen where the biometric sensor is located.\textsuperscript{50} Samsung’s new patent will allow a user to unlock their phone by placing their finger anywhere on the display screen.\textsuperscript{51} The full-screen scanner is intended to quicken the biometric authentication process by employing a separate, low-energy processor that, upon sensing a finger on the screen, brightens the display and quickly scans the fingerprint three times.\textsuperscript{52}

Much, if not all, of our lives are digitally stored on our smartphones and “it’s important to protect that information.”\textsuperscript{53} Just as fingerprint identification (“fingerprint “ID”) revolutionized the way consumers used their smartphones, face identification (“face ID”) enabled by Apple’s state-of-the-art TrueDepth camera system now allows consumers to unlock their phones with a simple glance.\textsuperscript{54} It doesn’t stop there: Face ID can be used to “authorize purchases from the iTunes Store, App Store, and Apple Books, and payments with Apple Pay.”\textsuperscript{55} Moreover, applications (“apps”) that allow fingerprint ID now also support face ID.\textsuperscript{56}

With biometric technology advancements unveiled with the release of each new smartphone, such as the storage abilities of Apple’s new A12 Bionic processor, users are increasingly able to store different types of biometric identifying information on their phones.\textsuperscript{57} However, “despite the popularity of biometrics and the unique issues they pose, there is no generally applicable federal law that regulates the private sector’s collection and use of biometric information in the United States.”\textsuperscript{58}

Biometric data protection is an issue that covers the entire globe, and some countries, including those that make up the European Union (“EU”),

\begin{enumerate}
\item Id.
\item Id.
\item Thubron, supra note 48.
\item Id.
\item Id.
\item Id.
\item Shankland, supra note 47.
\item Zimmerman, supra note 14, at 638.
\end{enumerate}
have already taken steps to expand the definition of privacy.\textsuperscript{59} In May 2018, the EU’s General Data Protection Regulation ("GDPR") became effective.\textsuperscript{60} Through the GDPR, the EU considers biometric data "a special category of personal data that calls for stricter rules on the processing of that data."\textsuperscript{61} As such, the GDPR aims to provide uniformity across the EU as well as further "safeguard individual citizens’ data rights in the increasingly technological world."\textsuperscript{62}

Biometric data is unique to the individual and it therefore needs to be regulated.\textsuperscript{63} This is especially true because the government is not the only entity that collects personal data: Thanks to the biometric identification systems preloaded onto their smartphones, private companies, such as Apple, Samsung, and Google, among others, also collect and store vast amounts of personal data, including biometric data.\textsuperscript{64} This Note focuses on biometric data because of its increased relevance in today’s society and because of the personal and permanent nature of the data.\textsuperscript{65} This Note explores the most progressive privacy legislation in the EU, the GDPR, current state biometric laws, such as Illinois’ BIPA, and argues for a preventative approach to biometric data privacy.\textsuperscript{66}

In Part II, this Note gives background information pertaining to the Fourth Amendment right to privacy, how the Fourth Amendment right to privacy applies to today’s technological society, and the EU’s response to biometric privacy issues.\textsuperscript{67} Part III explores the lack of biometric privacy law in the United States and how the lack of federal regulation of biometric data fails to protect the public from threats to privacy and civil liberties and leaves the future of privacy uncertain for consumers.\textsuperscript{68} Part III further addresses and compares current leading state biometric privacy laws.\textsuperscript{69} Part IV offers a solution to the aforementioned issue by proposing broad federal legislation and the creation of the Federal Biometric Data

---

\textsuperscript{60} Id.
\textsuperscript{61} Id.
\textsuperscript{62} Id. at 374-75.
\textsuperscript{63} See Zimmerman, supra note 14, at 641 (discussing unique characteristics of biometric identifying data and how biometric data is widely unregulated).
\textsuperscript{64} Id. at 641, 643.
\textsuperscript{65} See id. at 638 (discussing the concerns of unique biometric identifying data and discussing how biometric data is generally unregulated).
\textsuperscript{66} See infra Parts II–IV.
\textsuperscript{67} See infra Part II.
\textsuperscript{68} See infra Part III.
\textsuperscript{69} See infra Part III.
Agency, which would be responsible for regulating the collection, storage, and use of smartphone users' sensitive data.\textsuperscript{70}

II. BIOMETRIC DATA AND THE CONSTITUTIONAL RIGHT TO PRIVACY

The Fourth Amendment to the United States Constitution protects citizens of the United States from unreasonable searches and seizures.\textsuperscript{71} More specifically, the Fourth Amendment grants the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."\textsuperscript{72} The majority of Fourth Amendment privacy arguments are made in an effort to curtail the government's power and authority, as the Fourth Amendment was drafted with specific language:

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.\textsuperscript{73}

During the framing era itself, the drafters' primary concern was against "general warrants."\textsuperscript{74} In that time, it was thought that the Fourth Amendment "forbade warrants that were unparticularized as to the place or things to be searched for or that lacked specific factual grounds justifying the search."\textsuperscript{75}

Subpart A gives an overview of the right to privacy by discussing the Fourth Amendment as well as notable criminal and civil cases in which the judiciary was tasked with addressing the right to privacy in today's digitized society.\textsuperscript{76} Subpart B focuses on defining biometric data and exploring the relationship between biometrics, smartphones, and smartphone users.\textsuperscript{77} Subpart C analyzes how the EU has responded to privacy concerns resulting from biometric technology advances through the recent enactment of the GDPR.\textsuperscript{78}

\begin{thebibliography}{99}
\bibitem{70} See infra Part IV.
\bibitem{71} U.S. CONST. amend. IV.
\bibitem{73} U.S. CONST. amend. IV.
\bibitem{74} Thomas Y. Davies, Can You Handle The Truth? The Framers Preserved Common-Law Criminal Arrest and Search Rules In "Due Process Of Law"—"Fourth Amendment Reasonableness" Is Only a Modern, Destructive, Judicial Myth, 43 TEX. TECH. L. REV. 51, 55 (2010).
\bibitem{75} Id.
\bibitem{76} See infra Part II.A.
\bibitem{77} See infra Part II.B.
\bibitem{78} See infra Part II.C.
\end{thebibliography}
A. How the Fourth Amendment's Implied Right to Privacy Applies to Today's Society

Separately from security of one’s privacy against arbitrary intrusion by the government, the Fourth Amendment right to privacy extends to private industry and is equally as central in today’s society. In fact, they are “‘of the very essence of constitutional liberty’ the guaranty of which ‘is as important and as imperative as are the guarantees of the other fundamental rights of the individual citizen.” Many scholars have studied the Fourth Amendment’s privacy language with respect to criminal procedure. However, technological advancements and growing privacy concerns require interpreting the Fourth Amendment through a more technological lens.

Some scholars have opined that the world is headed towards a society where privacy is nonexistent and where the Fourth Amendment’s reasonable expectation of privacy will be no more. To illustrate this, the United States government has already developed and begun to implement the Biometric Optical Surveillance System ("BOSS"). Through the BOSS, the federal government has the capability of “identifying individuals from distances of up to 100 meters.”

With 292.8 million U.S. cellphone users in 2010, it is no surprise that society has become “phone-centric.” With such a high number of cellphone users in 2010, it is likely that the majority of people walking around on the streets today have some sort of cellphone in their possession, making it easier for “Big Data” to collect and store their information, and, ultimately, to identify them. This is especially relevant since, as today’s society has become increasingly digitized, cellphones are no longer used to solely make telephone calls. In addition to the classic telephone call, cellphones have become a “multi-functional tool” that is essentially a “pocket super-computer.”

While there is no current federal legislation regulating citizens’ biometric data—a topic that will be discussed more fully later in this

79. Ohm, supra note 72, at 1311.
81. Ohm, supra note 72, at 1311.
82. Id. at 1311-12.
83. Id. at 1320.
84. Friedland, supra note 17, at 125.
85. Id.
86. Id. at 125-26.
87. Id. at 127.
88. Id. at 126.
89. Id.
Note—it does not mean that the privacy issue has not made its way through the United States judicial system. The notable 1967 Supreme Court decision in *Katz v. United States* created the judicial framework for the reasonable expectation of privacy test that is used in deciding whether an individual’s reasonable expectation of privacy has been violated. This test is criticized, however, because the test “rests on the assumption that [the] hypothetical reasonable person has a well-developed and stable [sense] of privacy expectations,” which ever-changing technology disrupts.

Nowadays, the issue of cellphone functionality and privacy has been the subject of Supreme Court decisions. The Court addressed the issue of Fourth Amendment privacy as related to warrantless cellphone searches in *Riley v. California*, as consolidated with *United States v. Wurie*. Of particular significance in cellphone privacy cases is the fact that cellphones now have Internet access, live turn-by-turn Global Positioning System (“GPS”) navigation systems, calendars, and much more. Such highly-advanced technology is an issue that Supreme Court Justices have to struggle with.

In November 2011, the Supreme Court notably heard arguments regarding the scope of the Fourth Amendment’s right to privacy in *United States v. Jones*. Antoine Jones, a Washington, D.C. nightclub owner,

---

90. See McKenna, supra note 24, at 1071-72 (discussing notable United States Supreme Court privacy decisions).
92. Id. at 360-61 (Harlan, J., concurring) (noting that to determine one’s reasonable expectation of privacy, courts must first consider the subjective prong, which requires that an individual “exhibits an actual (subjective) expectation of privacy,” and then evaluate the objective prong, which determines whether that “expectation [is] one that society is prepared to recognize as ‘reasonable’”).
93. McKenna, supra note 24, at 1071.
94. Friedland, supra note 17, at 122-23.
95. 573 U.S. 373 (2014).
96. Friedland, supra note 17, at 122-23.
97. Id. at 126.
98. de Vogue, supra note 25. In *Carpenter v. United States*, the Supreme Court discussed the application of the Stored Communications Act (“SCA”) on suspects' cell phone data obtained by the FBI. 138 S. Ct. 2206, 2221 (2018). In 2011, four men were arrested in connection with a series of armed robberies. Id. at 2212. Defendant Timothy Carpenter moved to suppress the government’s cell-site location evidence on Fourth Amendment grounds, arguing that a warrant was required in order to obtain the records. Id. Carpenter’s motion was denied by the District Court and the Sixth Circuit affirmed. Id. at 2213. The Supreme Court reversed, holding: (1) an individual maintains a legitimate expectation of privacy, for Fourth Amendment purposes, in the record of his physical movements as captured through cell-site location information (“CSLI”); (2) seven days of historical CSLI obtained from defendant’s wireless carrier, pursuant to an order issued under the SCA, was the product of a “search”; (3) the Government’s access to 127 days of historical CSLI invaded defendant’s reasonable expectation of privacy; and (4) the Government must generally obtain a search warrant supported by probable cause before acquiring CSLI from a wireless carrier. Id. at 2217, 2219, 2221, 2223.
99. 565 U.S. 400, 403-04 (2012) (holding that the attachment of a GPS tracking device to a
was suspected of narcotics trafficking and was placed under FBI and D.C. Metropolitan Police task force surveillance. Various investigative techniques were used, including visual surveillance and phone wiretaps. The United States District Court for the District of Columbia granted a warrant to place a GPS tracking device on the Jeep Grand Cherokee registered to Jones’s wife, as long as the device was installed within ten days from the warrant date, and while the vehicle was located in D.C.

The GPS tracker was placed on Jones’s vehicle, located in Maryland, on the eleventh day after the warrant was issued. For the following twenty-eight days, the Government tracked Jones’s vehicle, amassing over 2000 pages of data on Jones, and ultimately leading to a multiple-count indictment charging Jones and several alleged co-conspirators with conspiracy to distribute and possession with intent to distribute, inter alia, five kilograms of cocaine. A jury returned a guilty verdict and the District Court sentenced Jones to life imprisonment.

The Supreme Court granted certiorari to review the issue of "whether the attachment of a [GPS] tracking device to an individual’s vehicle, and subsequent use of that device to monitor the vehicle’s movements on public streets, constitutes a search and seizure under the Fourth Amendment." Justice Antonin Scalia delivered the opinion of the Court, holding that the Government’s installation of a GPS device on a target’s vehicle and its use of the device to monitor the vehicle’s movements constituted a “search” under the meaning of the Fourth Amendment.

In his opinion, Justice Scalia employed a textualist approach in analyzing the relevant language of the Fourth Amendment:

The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to “the right of

---

100. Id. at 402.
101. Id.
102. Id. at 402-03.
103. Id. at 403.
104. Id.
105. Id. at 404.
106. Id.
107. Id. at 402.
108. Id. at 404.
the people to be secure against unreasonable searches and seizures”; the phrase “in their persons, houses, papers, and effects” would have been superfluous. Consistent with this understanding, our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century.\textsuperscript{109}

Scalia stressed that the “Government physically occupied private property for the purpose of obtaining information . . . [the Court has] no doubt that such a physical intrusion would have been considered a ‘search’ within the meaning of the Fourth Amendment.”\textsuperscript{110}

The Court deviated from the historical property-based approach and cited its earlier decision in \textit{Katz v. United States}.\textsuperscript{111} In \textit{Katz}, the Court held that “the Fourth Amendment protects people, not places.”\textsuperscript{112} The Court’s decisions in \textit{Jones} and \textit{Riley v. California} show an effort to protect individuals from the government, effectively updating the Constitution by applying privacy rights to individuals in the realm of data privacy.\textsuperscript{113} The ever-changing application of the language of the Fourth Amendment as it encompasses data privacy rights warrants repeating the words of Chief Justice Roberts, as he recognized the difficulty in keeping up with ever-increasing technological advances: “[S]ome of the [C]ourt’s most challenging cases involve applying long-held rules created by the courts to quickly developing technology.”\textsuperscript{114}

\textbf{B. Biometric Data and Smartphones}

Today, it is just about impossible to own a smartphone that is not equipped with some form of biometric identifying capability.\textsuperscript{115} “Biometrics” is defined as “the measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity.”\textsuperscript{116} Biometric characteristics can be divided into two categories:

\begin{itemize}
  \item \textsuperscript{109} \textit{Id.} at 405.
  \item \textsuperscript{110} \textit{Id.} at 404-05.
  \item \textsuperscript{111} \textit{Id.} at 405-06.
  \item \textsuperscript{112} \textit{Katz} v. \textit{United States}, 389 U.S. 347, 351 (1967).
  \item \textsuperscript{113} \textit{Jones}, 565 U.S. at 422 (Alito, J., concurring). In \textit{Riley v. California}, the Supreme Court ruled that: “(1) the interest in protecting police officers’ safety did not justify dispensing with warrant requirement for searches of cell phone data; and (2) the interest in preventing destruction of evidence did not justify dispensing with warrant requirement for searches of cell phone data.” 134 S. Ct. 2473, 2486 (2014). In this case, the Court sought to protect the individual’s right to cell-phone data privacy from unwarranted intrusion by the Government.” \textit{Id.}
  \item \textsuperscript{114} de Vogue, \textit{ supra} note 25.
  \item \textsuperscript{115} Zimmerman, \textit{ supra} note 14, at 637.
  \item \textsuperscript{116} \textit{Biometrics}, \textsc{Merriam-Webster}, https://www.merriamwebster.com/dictionary/biometrics (last visited Nov. 18, 2018).
\end{itemize}
physiological, which concerns an individual’s body composition, and behavioral, which concerns an individual’s behavioral patterns such as gait and voice. The most common examples of physiological biometric identifiers being implemented in smartphones are facial recognition, fingerprint scanning, hand geometry scanning, iris and retinal scanning, and even vein scanning.

According to IHS Inc., a global source of information and analytics, the number of smartphones with embedded fingerprint sensors “is projected to grow from 499 million in 2015 to 1.6 billion in 2020.” Smartphone companies such as Apple, Samsung, and Huawei have not stopped at fingerprint sensors, as automated facial recognition, hand gesture recognition, iris scanners, hand-vein scanners, and heart rhythm monitors “are all vying to be ‘the next big thing.’”

In essence, smartphone biometric technology requires a scanning device to record biometric authentication factors, software to convert the scanned information into a digital format—which then compares the recently-scanned data with stored data—and lastly, a database to securely store biometric data. Biometrics does not only apply to the specific individual’s identifying information; rather, biometrics is also a process of recognizing an individual based on a “measurable physiological or behavioral characteristic.”

Apple’s more recent smartphones with Face ID, for example, employ some of the most highly sophisticated technology ever created:

The TrueDepth camera captures accurate face data by projecting and analyzing over 30,000 invisible dots to create a depth map of [a user’s] face and also captures an infrared image of [the person’s] face. A portion of the neural engine of the A11, A12 Bionic, and A12X Bionic Chip—protected within the Secure Enclave—transforms the depth map and infrared image into a mathematical representation and compares that representation to the enrolled facial data. Face ID automatically adapts

121. Rouse, supra note 118.
to changes in [] appearance, such as wearing cosmetic makeup or growing facial hair. If there is a more significant change in [] appearance, like shaving a full beard, Face ID confirms [the] identity by using [the user’s] passcode before it updates [] face data. Face ID is designed to work with hats, scarves, glasses, contact lenses, and many sunglasses. Furthermore, it’s designed to work indoors, outdoors, and even in total darkness.123

The sophistication, albeit impressive, has required companies like Apple to take increased steps to safeguard users’ biometric data.124 Face ID data—including the stored mathematical representations of users’ faces—is “encrypted and protected with a key available only to the Secure Enclave.”125

The so-called Secure Enclave creates an added layer of security for private keys.126 The Secure Enclave “is a hardware-based key manager that’s isolated from the main processor.”127 When a key is stored in the Secure Enclave, the user never actually handles the key, “making it difficult for the key to become compromised.”128 While the Secure Enclave’s security measures are a significant step in protecting users’ sensitive data, breaches are still an all-too-real worry for consumers and businesses alike.129

The widespread problem with millions of people using fingerprint scanners and other biometric identifiers is that privacy and data security risks grow as the use of biometric identifiers rises in popularity.130 As data breaches have become increasingly common, the security of smartphone users’ private and sensitive information has risen to the forefront of consumers’ minds as they look to keep up with important technological advancements.131 For example, subsequent to Apple’s highly-anticipated iPhone X release, “it took researchers just two weeks to bypass Apple’s Face ID facial recognition using a 3D-printed mask; Face ID can also be

123. Apple, supra note 53.
124. Id.
125. Id.
127. Id.
128. Id.
129. Zimmerman, supra note 14, at 637-38; see also Joseph Cox, Are Data Breaches Becoming More Common?, VICe: MOTHERBOARD (July 28, 2016, 12:58 PM), https://motherboard.vice.com/en_us/article/data-breaches-vigilante-pw (discussing listings of hacks on Vigilante.pw, which showed that “data breaches have become more frequent over the past few years.”).
130. Zimmerman, supra note 14, at 661.
131. Id. at 656; see also Cox, supra note 129.
defeated by individuals related to the authenticated user, including children or siblings."\textsuperscript{132}

\subsection*{C. The General Data Protection Regulation}

The EU realized the increasing dangers of biometric data recognition technology in the twenty-first century and implemented the GDPR in May 2018.\textsuperscript{133} The GDPR replaced the Data Protection Directive of 1995 ("DPD"), becoming "the leading legislation regarding data protection in the EU."\textsuperscript{134} The passing of the DPD was the first time that individuals received a right to protection of their personal information.\textsuperscript{135} The broad and generalized language of the DPD raised the need for increased data security and provided for a good foundation upon which the GDPR was created:

Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected.\textsuperscript{136}

Technological advances, such as advancements in smartphone capabilities, required revisiting and revising the DPD.\textsuperscript{137} This led to the 2012 proposal in which the EU sought a "more comprehensive Data Protection Regulation," indicating that "rapid technological developments have brought new challenges for the protection of personal data."\textsuperscript{138}

One of the factors that makes the GDPR a step in the right direction is the fact that it "harmonises [sic] data protection law across all member states, making it identical."\textsuperscript{139} In an effort to increase transparency

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{132} Rouse, supra note 118.
\item \textsuperscript{133} Monajemi, supra note 59, at 376-77.
\item \textsuperscript{134} Id. at 376.
\item \textsuperscript{135} Id. at 377; see also Council Directive 95/46, Data Protection Directive of 1995, 1995 O.J. (L 281) 31, 31 (EC) [hereinafter DPD].
\item \textsuperscript{136} DPD, supra note 135, at 35-36.
\item \textsuperscript{137} Monajemi, supra note 59, at 377.
\item \textsuperscript{138} Id. (quoting Commission Regulation 2016/679, 2016 O.J. (L 119) 1, 2 [hereinafter GDPR]).
\end{itemize}
\end{footnotesize}
between consumers and data-collecting organizations, the GDPR "makes it easier for people to discover what information organisations [sic] have on them" as well as what the organizations use the data for.\textsuperscript{140} A notable facet of the GDPR, giving it some teeth, is the introduction of larger penalties for organizations that do not comply with the regulations.\textsuperscript{141}

A key component of the GDPR is the "right to be forgotten."\textsuperscript{142} As Thomas McMullan and Joe Curtis explain, the GDPR gives consumers the power to control their private information:

[People] can have their data deleted at any time if it's not relevant anymore - i.e. the company storing it no longer needs it for the purpose they collected it for. If the data was collected under the consent model, a citizen can withdraw this consent whenever they like. They might do so because they object to how an organisation [sic] is processing their information, or simply don't want it collected anymore.\textsuperscript{143}

Under the GDPR, in order for EU citizens to communicate that they would like their personal data deleted, they must contact the "data controller," a person or entity that is the principal party that "determines the purposes and means of the processing of personal data."\textsuperscript{144} The GDPR simplifies data protection by essentially creating two categories of "people" responsible for collecting consumers' data, and then processing such data.\textsuperscript{145}

The two categories created by the GDPR are data controllers and data processors.\textsuperscript{146} The GDPR's definition of a data controller is "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."\textsuperscript{147} Data processors are defined as a "natural or legal person, public authority, agency, or other body which processes personal data on behalf of a data controller."\textsuperscript{148} Data controllers and data processors work together.\textsuperscript{149} However, the controllers bear the burden of proving the data subjects consented to the processing of their personal data for specified purposes.\textsuperscript{150} The GDPR simplifies and unifies data privacy

\textsuperscript{140} Id.
\textsuperscript{141} Id.
\textsuperscript{142} Id.
\textsuperscript{143} Id.
\textsuperscript{144} See GDPR, supra note 138, at art. 4(7); Monajemi, supra note 59, at 378.
\textsuperscript{145} Monajemi, supra note 59, at 378.
\textsuperscript{146} See GDPR, supra note 138, at art. 1(13).
\textsuperscript{147} Id. at art. 4(7).
\textsuperscript{148} See id. at art. 4(8); see also Monajemi, supra note 59, at 378.
\textsuperscript{149} See GDPR, supra note 138, at art. 4(8).
\textsuperscript{150} Id. at art. 7(1).
security by having one point of contact—the data controller—for people to “complain and reach out to.”

Article 7 of the GDPR governs the conditions for consent required before any subject’s personal data can be collected and processed. The consent provision of the GDPR further protects individuals because it stresses that consent shall not provide a legal basis for the processing of a person’s private data. The consent clause works synergistically with Article 32, which further establishes security measures for the actual processing of a subject’s sensitive information. Article 32 charges data controllers and data processors with taking measures to protect personal data against “accidental or unlawful destruction, loss, alteration, unauthorised [sic] disclosure of, or access to personal data transmitted, stored or otherwise processed.”

The GDPR considers a person’s sensitive personal data as a “‘special category of personal data . . .’ and by definition require more protection than [regular] personal data.” Among the types of personal data considered to be a special category is biometric data. As Michael Monajemi explains in his article, “[o]ne of the most revolutionary aspects of the GDPR is the fact that it regulates biometric data as a separate entity rather than trying to include it in an existing privacy scheme that does not take into account biometric data sensitivity.” The GDPR defines biometric data as “personal data resulting from specific technical processing relating to the physical, physiological or behavioural [sic] characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.”

The GDPR realizes that technology is ever-advancing and that biometric data will continue to evolve; therefore, the GDPR broadly defines biometric data. Monajemi explains that the GDPR is “in a good position to apply to many different types of biometric data that will arise through the development of technology.” The GDPR requires data controllers to “conduct Privacy Impact Assessments (PIA) for many

151. Monajemi, supra note 59, at 379.
152. See GDPR, supra note 138, at art. 7(1).
153. Id. at 8.
154. Id. at art. 32(1)-(4).
155. Id. at art. 32(2).
156. Monajemi, supra note 59, at art. 382 (citing GDPR, supra note 138, at art. I(10)).
157. Id. at 382.
158. Id.
159. GDPR, supra note 138, at art. 4(14).
160. Monajemi, supra note 59, at 382-83.
161. Id. at 383.
forms of biometric data processing."\textsuperscript{162} Impact assessments are used when a type of data processing is likely to result in a "high risk to the rights and freedoms of natural persons."\textsuperscript{163}

To protect the rights and freedoms of natural persons, Article 35 addresses three particular instances when controllers would need to run impact assessments:

A data protection impact assessment . . . shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.\textsuperscript{164}

The rationale behind requiring data controllers to conduct impact assessments in these particular instances is to determine whether automated profiling and large-scale processing, if approved, will adversely affect the rights and freedoms of data subjects.\textsuperscript{165} In addition, the GDPR allows data controllers to consult with the data subjects when appropriate.\textsuperscript{166}

By enacting the GDPR, the EU recognized the privacy risks to the fundamental rights and freedoms of the public associated with the collection and storage of biometric information.\textsuperscript{167} The GDPR recognizes that the protection of natural persons "in relation to the processing of personal data is a fundamental right."\textsuperscript{168} Notably, the GDPR is intended to "contribute to the accomplishment of an area of freedom, security and

\textsuperscript{162} Id.

\textsuperscript{163} See GDPR, supra note 138, at art. 35(1) (stating that "[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.").

\textsuperscript{164} Id. at art. 35(3).

\textsuperscript{165} Id. at art. 35(7).

\textsuperscript{166} See id. at art. 35(9) (indicating that "[w]here appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.").

\textsuperscript{167} Id. at art. 1(51).

\textsuperscript{168} Id. at art. 8(1) (stating that "Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.").
justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons."^{169} In the United States, the notion of freedom and security of the "privacies of life" emanates from the fundamental right to privacy worthy of the protection for which the Founders fought.\textsuperscript{170} However, there is no existing federal legislation protecting the public’s biometric privacy rights.\textsuperscript{171} This issue is discussed in further detail in Part III of this Note.\textsuperscript{172}

III. THE LACK OF BIOMETRIC PRIVACY LAW IN THE UNITED STATES ENDANGERS THE EVER-GROWING AMOUNT OF SMARTPHONE USERS

The United States government, as well as private companies, use biometric data for different reasons.\textsuperscript{173} The use of biometric data to identify the public, whether for governmental or smartphone-access purposes, raises legal privacy concerns; namely the lack of federal regulation on the matter.\textsuperscript{174} Subpart A examines the legal issue caused by the lack of broad federal regulation allowing private companies to remain unchecked in how they collect, store, and protect sensitive biometric information.\textsuperscript{175} Subpart B analyzes the leading current state biometric privacy laws to identify how certain states protect consumers’ biometric privacy.\textsuperscript{176}

A. Lack of Broad Federal Regulation Allows Companies to Use Customers’ Information Leaving Customers with No Recourse

In 2017, the United States Department of Homeland Security implemented a program called the Travelers Verification Service ("TVS").\textsuperscript{177} The TVS streamlines the boarding process of international flights.\textsuperscript{178} The key to the TVS is travelers’ faces.\textsuperscript{179} Passengers simply “step up to the gate, get their photo taken and proceed onto the plane.

\textsuperscript{169} Id. at art. I(2).
\textsuperscript{170} See Riley v. California, 134 S. Ct. 2473, 2494-95 (2014).
\textsuperscript{171} Nakar & Greenbaum, supra note 41, at 106.
\textsuperscript{172} See infra Part III.
\textsuperscript{173} Sales, supra note 27, at 219.
\textsuperscript{174} Zimmerman, supra note 14, at 663 (discussing the current lack of regulation in the United States to protect consumers).
\textsuperscript{175} See infra Part III.A.
\textsuperscript{176} See infra Part III.B.
\textsuperscript{178} Id.
\textsuperscript{179} Id.
Thanks to facial recognition technology, [a passenger’s] face becomes their boarding pass.\textsuperscript{180} Similarly, with biometric technology in smartphones, the TVS technology is convenient, yet unregulated and dangerous.\textsuperscript{181}

One notable issue with the implementation of the TVS is that it applies to American citizens as well as other international travelers.\textsuperscript{182} According to reports, few companies participating in the TVS “give explicit guarantees that passengers’ facial recognition data will be protected.”\textsuperscript{183} Additionally, federal officials “have placed no limits on how participating companies—mostly airlines but also cruise lines—can use that data or store it, opening up travelers’ most personal information to potential misuse and abuse such as being sold or used to track passengers’ whereabouts.”\textsuperscript{184}

American travelers are at a significant risk of identity theft through the use of biometric identification, regardless of whether the information is obtained through the TVS or through their smartphones:

The data the airlines collect is used to verify the identity of passengers leaving the country, an attempt by the [D]epartment [of Homeland Security] to better track foreigners who overstay their visas. After passengers’ faces are scanned at the gate, the scan is sent to Customs and Border Protection and linked with other personally identifying data, such as date of birth and passport and flight information. For its part, Customs and Border Protection has said it will retain facial scans of American citizens for no longer than 14 days. But the agency has said it cannot control how the companies use the data.\textsuperscript{185}

Customs and Border Protection has a duty to protect Americans’ data.\textsuperscript{186} In objecting to the use of facial recognition biometrics, the American Civil Liberties Union mentioned that “from a privacy perspective, it is the most dangerous biometric identifier because it has great potential for expansion and misuse.”\textsuperscript{187} The implementation of the

\textsuperscript{180} Id.
\textsuperscript{181} Id.; see also Nolan Rappaport, \textit{Will Trump’s Biometric Entry-Exit Be as Controversial as His Travel Ban?}, \textit{The Hill} (Sept. 2, 2018, 11:30 AM), https://thehill.com/opinion/immigration/404625-will-trumps-biometric-entry-exit-system-be-as-controversial-as-his-travel (“Unlike the travel ban, which just applied to aliens seeking admission to the United States, Trump’s biometric entry-exit tracking system will apply also to American citizens. The facial recognition technology that the system uses to identify travelers leaving the country will be used to identify American citizens too, unless they request an alternative means of verifying their identities.”).
\textsuperscript{182} Rappaport, \textit{supra} note 181.
\textsuperscript{183} Edmondson, \textit{supra} note 177.
\textsuperscript{184} Id.
\textsuperscript{185} Id.
\textsuperscript{186} Id.
\textsuperscript{187} Rappaport, \textit{supra} note 181.
TVS provides further support for the notion that the collection, storage, and use of biometric identifiers is dangerous for the American public and has led to a rise in class-action lawsuits in some states.\(^{188}\)

While it is reassuring to know that biometric data privacy has made its way to the judiciary, aside from the Health Insurance Portability and Accountability Act—which specifically removed biometric identifiers from protected health information—there is still no federal legislation to regulate the capture, storage, or use of such sensitive information.\(^{189}\) For a country as technologically advanced as the United States, and as a world-leading country in business, the federal government has failed to “protect consumers from the collection of biometric data, despite requests from industry leaders for guidelines to protect individuals from the collection of their biometric data without their consent.”\(^{190}\)

Privacy laws do exist, however, and the majority of existing data privacy laws follow the Organization for Economic Co-operation and Development (“OECD”) model.\(^{191}\) The OECD, a group of thirty member-countries including the United States, created a model for countries to follow using the same basic principles:

\[ (1) \] *Collection limitation principle.* Data should be collected by “lawful and fair means,” with the knowledge and consent of the consumer. \[ (2) \] *Data quality principle.* Collected data should be relevant to the purposes of the data use, and the need for the data should be accurate, complete, and current. \[ (3) \] *Purpose specification principle.* Consumers should be given timely notice of the purpose of the data collection. \[ (4) \] *Use limitation principle.* The collected data should not be disclosed or made available to other companies unless there is consent given by the consumer or authorized by law. \[ (5) \] *Security safeguards principle.* The collected data “should be protected by reasonable security safeguards against such risks as loss or unauthori[z]ed access, destruction, use, modification or disclosure of data.” \[ (6) \] *Openness principle.* Companies should make information available to the consumer about the consumer’s collected data. \[ (7) \] *Individual participation principle.* Consumers should be able to challenge incorrect data about them and should have a right to inquire about the data collection. \[ (8) \] *Accountability principle.* A data controller should be accountable for


\(^{189}\) Zimmerman, *supra* note 14, at 645.

\(^{190}\) Id. at 643-44.

complying with all the previous principles by having appropriate safeguards in place, coupled with a notification system.\textsuperscript{192}

The concern, however, is that although some bills have been introduced, Congress still has not enacted any laws specifically geared towards protecting the privacy of Americans' biometric data.\textsuperscript{193}

In \textit{Lujan v. Defenders of Wildlife},\textsuperscript{194} the Supreme Court established a three-part test that a plaintiff must meet in order to constitutionally bring a cause of action in court: "(1) there must exist an invasion of a legally protected interest which is 'concrete and particularized'; (2) the invasion of that legally protected interest must be 'actual or imminent, not "conjectural" or "hypothetical"'; and (3) judicial redress must be 'likely' and not simply 'speculative.'"\textsuperscript{195} A critical requirement of this test is that a \textit{legally protected interest} must exist, thereby establishing the need for a protective statute.\textsuperscript{196} It follows that the best way for a consumer to seek recourse for an invasion of data privacy or data breach is to claim a statutory violation because a statutory violation constitutes an invasion of a legally protected interest.\textsuperscript{197}

In 1986, the Electronic Communications Privacy Act ("ECPA") added "electronic communications"\textsuperscript{198} to the definition of "wire communication" as defined in Title III of the Omnibus Crime Control and Safe Streets Act ("OCCSSA")—allowing a plaintiff to recover if an electronic communication is intercepted or disclosed in violation of the statute.\textsuperscript{199} Title III was intended by Congress to safeguard the privacy of wire and oral communications.\textsuperscript{200} By enacting the ECPA, Congress amended Title III and effectively created an umbrella definition of electronic communication, covering many types of electronic and internet-based communications.\textsuperscript{201} In addition to the ECPA, the Stored Communications Act ("SCA") also regulates the storage and use of electronic-based communications.\textsuperscript{202}

\footnotesize
193. Jones, supra note 191, at 130.
196. Id.
197. Id.
198. 18 U.S.C. § 2510 (2012); see also McKenna, supra note 24, at 1047-49.
199. See 18 U.S.C. § 2520 (2012); see also McKenna, supra note 24, at 1048.
200. McKenna, supra note 24, at 1047.
201. Id. at 1048.
202. See 18 U.S.C. §§ 2703(a),(d) (2012) (stating the requirements for a warrant or court order to obtain access to stored communications); see also McKenna, supra note 24, at 1049.
While privacy schemes have already been in place, these laws attempt to protect the privacy of communications by constraining the reach of the government and by limiting what data private actors may share with the government. However, these laws do not protect the unique characteristics of biometric data from collection and storage by private actors. The private industry is just as much to blame for putting consumers’ biometric privacy at risk. As Anne McKenna articulates:

Many people unknowingly supply data when a software app gathers it surreptitiously, or they supply information through the Internet or their smartphone for convenience. In the latter case, they do so because their choice is either give information or be precluded from the use of a helpful or popular application. Convenience often outweighs thoughts of privacy, yet when the information given is used for a purpose different from that of the application for which it was provided, the consumer has been wronged.

An example, as illustrated by McKenna, is the pairing of "a consumer’s likes and other personal information with face recognition technology, [thereby allowing] a previously anonymous person [to] be identified and then targeted with specific marketing” tailored to the individual.

Companies that collect and store vast amounts of personal data are increasingly subject to security breaches. One example of the devastating effect of security breaches is the 2014 data breach of the governmental databases at the United States Office of Personnel Management. As a result of the security breach, more than twenty-two million people had sensitive information stolen by hackers. According to those U.S. officials close to the matter, “the breach ranks among the

203. See 18 U.S.C. §§ 2703(c)(1)–(2) (2012); McKenna, supra note 24, at 1049.
204.  McKenna, supra note 24, at 1049.
205.  Id. at 1075 (discussing some of the ways that private industry places consumers’ personal data at risk).
206.  Id.; see also Nicole Perlroth & Nick Bilton, Mobile Apps Take Data Without Permission, N.Y. TIMES: BITS BLOG (Feb. 15, 2012, 9:05 AM), http://bits.blogs.nytimes.com/2012/02/is/google-and-mobile-apps-take-data-books-withoutpermission? r=0 (noting that “companies that make many of the most popular smartphone apps for Apple and Android devices—Twitter, Foursquare and Instagram among them—routinely gather the information in personal address books on the phone and in some cases store it on their own computers.”). The article further notes that “findings shed more light on how technology companies sift through people’s personal and private information without their knowledge.” Perlroth & Bilton, supra.
207.  McKenna, supra note 24, at 1075-76.
208.  Zimmerman, supra note 14, at 656.
209.  Id. at 656-57; see also Tom Iacuzio, Accessing Safety in the Age of Biometrics, EMBRY-RIDDLE NEWSROOM (Oct. 11, 2016, 5:01 PM), http://news.erau.edu/headlines/accessing-safety-in-the-age-of-biometrics.
210.  Iacuzio, supra note 209.
most damaging cyber heists in history primarily due to the detail in the files, some of which included fingerprints."211

On September 7, 2017, one of the most damaging data breaches occurred when consumer-credit-reporting agency Equifax reported a security breach.212 The breach took place from mid-May 2017 through July 2017 and affected 145 million users.213 Although not the largest in cyber history, the damage caused by the Equifax breach is particularly noteworthy due to the sensitive nature of the compromised data.214 Hackers accessed "a treasure trove of names, Social Security numbers, birth dates, street addresses and, in some instances, driver's license numbers."215 With this type of personal information, "miscreants can pose as [individuals] to set up credit cards, mortgages, [and] loans" thereby highlighting the very real horrors of security breaches and the vital need for uniform data security.216

In the case of the Equifax breach, the compromised information was not necessarily biometric information, however poached biometric information "poses unique problems for consumers."217 Credit and debit cards, driver’s licenses, Social Security numbers, and passwords can all be replaced, however, compromised biometric information, by its nature, cannot be replaced.218 As Marc Goodman explains, biometric details that have been collected and stored "undoubtedly will" become hacked and "remediation of the problem will prove much more difficult, if not impossible."219

Facebook, for example, admitted to collecting, storing, and using the biometric information of millions and millions of users around the world through Facebook’s facial recognition software.220 Facebook has become the world’s largest social networking website,221 and the sheer volume of

211. Id.
213. Id.
214. Id.
215. Id.
216. Id.
218. Id. at 658; see also Marc Goodman, You Can't Replace Your Fingerprint, SLATE (Feb. 24, 2015, 10:05 AM), https://slate.com/technology/2015/02/future-crimes-excerpt-how-hackers-can-steal-fingerprints-and-more.html (discussing the dangers of biometric authentication).
220. McKenna, supra note 24, at 1068.
Facebook users worldwide indicates how much sensitive data is at risk.\(^{222}\) Aside from hacking into databases, cyber criminals can acquire sensitive biometric data through their ability to fool biometric technology.\(^{223}\)

Marc Goodman asserts that the future of identity theft involves stealing and compromising biometrics by discussing the work of Tsutomu Matsumoto, a security researcher at Yokohama National University:

[Tsutomu Matsumoto] has devised a method allowing him to "take a photograph of a latent fingerprint (on a wineglass, for example)" and recreate it in molded gelatin. The technique is good enough to fool biometric scanners 80 percent of the time. Hackers have also used everyday child’s Play-Doh to create fingerprint molds good enough to fool 90 percent of fingerprint readers.\(^{224}\)

Matsumoto’s fingerprint research experiment is only one example showing how easily biometric authentication can be fooled.\(^{225}\)

A problem with biometric authentication is “the fact that biometric information is inherently not a secret.”\(^{226}\) The dangers do not lie with fingerprints alone, as the prominence of facial recognition technology has led to other security risks:

Just as fingerprint sensors can be hacked, so too can face-printing systems increasingly be used to unlock your phone or computer or to gain access to your office. All it takes to defeat some systems, such as those on Lenovo laptops or smartphone password apps such as FastAccess Anywhere, is to hold up a photograph of the person you wish to impersonate. This very technique has also worked with iris scanning, allowing hackers to reverse engineer the biometric information stored in a secure database and use it to print a photographic iris good enough to fool most commercial eye scanners.\(^{227}\)

In response to the growing privacy risks associated with biometric technology, several states have enacted statutes governing biometric data protection and are attempting to provide recourse to victims.\(^{228}\)

---

\(^{222}\) McKenna, supra note 24, at 1068; see also Aguado, supra note 221, at 195-96.

\(^{223}\) Goodman, supra note 218.

\(^{224}\) Id.

\(^{225}\) Id (discussing the problems with hacking facial recognition technology).

\(^{226}\) Zimmerman, supra note 14, at 658.

\(^{227}\) Goodman, supra note 218.

\(^{228}\) Zimmerman, supra note 14, at 648.
B. State Biometric Privacy Laws

In the absence of broad federal regulation, some states have taken steps to protect smartphone consumers’ biometric data. For example, states such as Iowa, Nebraska, Wisconsin, and North Carolina “have recognized the need to regulate the collection of biometric information.” Two states, Illinois and Texas, have taken a step further by following the OECD model to discern between the intimate nature of biometric information and regular personal information. Illinois’s BIPA defines biometric identifier as “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry” and does not include “biological materials regulated under the Genetic Information Privacy Act.” The BIPA additionally defines biometric information as “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.”

Illinois’s BIPA was the initial state statute governing the privacy of biometric data. Enacted in 2008, the BIPA was passed “in response to the growing use of biometrics and the potential for identity theft if biometric data is compromised.” The BIPA contains six key requirements for any private entity in possession of or collecting biometric data:

(i) Develop a written policy, available to the public, establishing a retention schedule and guidelines for destruction;
(ii) Destroy biometric data when the initial purpose for obtaining/collecting such data has been fulfilled, or within three years of the person’s last interaction with the entity, whichever is sooner;
(iii) Biometric data cannot be collected or otherwise obtained without prior written consent based on a disclosure to an individual that biometric data is being collected and the length of time for which the data is collected;
(iv) Biometric data cannot be sold;
(v) Biometric data cannot be disclosed unless (a) consent is obtained, (b)

229. Id.
231. Id.
232. 740 ILL. COMP. STAT. § 14/10 (2010).
233. Id.
235. See 740 ILL. COMP. STAT. § 14/5 (2010) (describing the legislative findings and intent for enacting the Illinois biometric privacy law); Lessack, supra note 234.
Disclosure is necessary to complete a financial transaction requested or authorized by the subject, (c) disclosure is required by law or (d) disclosure is required by subpoena; and (vi) Biometric data must be stored using a reasonable standard of care for the entity’s industry and in a manner that is the same or exceeds the standards used to protect other confidential information.  

As the first state to enact a biometric data privacy statute, the Illinois legislature acknowledged that “[t]he full ramifications of biometric technology are not fully known.”

Texas’s biometric statute, found in the Texas Business and Commerce Code, similarly defines biometric identifier as “a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.” The statute, enacted in 2009, called the “Capture or Use of Biometric Identifier” (“CUBI”), requires private entities to give notice and obtain an individual’s consent prior to collecting their biometric information. The Texas legislature specified limitations on biometric information that is captured and possessed for commercial purposes.

The CUBI, enacted a year after the BIPA, shares many similarities with the Illinois statute, however, the CUBI only regulates biometric identifiers that are used for a “commercial purpose.” The BIPA contains no such limitations and therefore has a broader scope. While the BIPA contains six key requirements, the CUBI states four requirements for collecting biometric data. Under the CUBI:

(c) A person who possesses a biometric identifier of an individual that is captured for a commercial purpose:
(1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless:
(A) the individual consents to the disclosure for identification purposes in the event of the individual’s disappearance or death;
(B) the disclosure completes a financial transaction that the individual requested or authorized;
(C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or

---

236. 740 ILL. COMP. STAT. § 14/15 (2010); Paul Werner, Six Things You Need to Know Before Collecting Biometric Information, SHEPPARDMULLIN (June 2, 2016), https://www.eyeonprivacy.com/2016/06/six-things-you-need-to-know-before-collecting-biometric-information (discussing the enactment and impact of current state biometric privacy laws).
237. § 14/5(f).
238. TEX. BUS. & COM. CODE ANN. § 503.001(a) (West 2009).
239. § 503.001(a); Lessack, supra note 234.
240. § 503.001(b).
241. Lessack, supra note 234.
242. Werner, supra note 236.
243. Id.
(D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant. 244

Both the BIPA and the CUBI have a consent requirement necessary to collect an individual’s biometric information; however, unlike the BIPA, the CUBI does not require the consent to be in writing. 245

Under both the BIPA and the CUBI, private entities can disclose an individual’s biometric information to a third party 246 “only if (1) the individual consents; (2) the disclosure completes a financial transaction the individual requested or authorized; (3) the disclosure is required by law; or (4) the disclosure is made in response to a warrant or subpoena.” 247

The statutory penalties for noncompliance are where the BIPA and the CUBI largely differ. 248 The “cost of not complying with the BIPA can be high,” 249 as the BIPA creates a private right of action for biometric data privacy violations. 250

Pursuant to the BIPA, a prevailing party may recover: (1) up to $1000 against a private entity for a violation of BIPA sounding in negligence; (2) up to $5000 against a private entity that intentionally or recklessly violates a provision of the BIPA; (3) reasonable attorneys’ fees and costs, including expert witness fees and other litigation expenses; and (4) other relief, including an injunction, as the State or federal court may deem appropriate. 251 The private right of action created in the BIPA sets it apart from similar laws. 252 Because the BIPA allows an aggrieved party to recover liquidated or statutory damages, victims like Lindabeth Rivera and Joseph Weiss have a suitable path to recovery. 253

The CUBI, on the other hand, does not create a private right of action. 244 Instead, the attorney general may bring an action to recover a civil penalty. 255 A person who violates the CUBI “is subject to a civil penalty of not more than $25,000 for each violation.” 256 Regardless of the method of action, the penalties under the BIPA and the CUBI per violation

244. § 503.001(c); Werner, supra note 236.
245. § 503.001(b); Lessack, supra note 234.
246. 740 ILL. COMP. STAT. §§ 14/15(d)(1)–(4) (2010); §§ 503.001(c)(1)(A)–(D).
249. Lessack, supra note 234.
250. 740 ILL. COMP. STAT. § 14/20 (2010); Zimmerman, supra note 14, at 649; Lessack, supra note 234; Werner, supra note 236.
251. § 14/20.
253. Id.; see supra Part I.
254. TEX. BUS. & COM. CODE ANN. § 503.001(d) (West 2009).
255. § 503.001(d).
256. Id.
can easily rise into the millions. Possible recoveries of liquidated damages ranging from $1000 to $5000 per violation, depending on the level of intent or recklessness, have made the BIPA a popular tool over the last year for consumer class action attorneys. In 2016, more than a half dozen class action lawsuits have been filed under the BIPA. Google, Shutterfly and a handful of social media companies have each been sued over the alleged use of facial geometry recognition software used for photo tagging. Palm Beach Tan and LA Tan were each sued over the alleged use of fingerprint data to act as a membership card, and Smarte Carte was sued over the alleged use of fingerprint security technology to lock and unlock lockers. Daycare company Crème de la Crème was sued recently over the alleged use of fingerprint technology to ensure the secure pickup of children.

Because of the BIPA, many industry-leading tech companies, such as Google, have been sued for the use of biometric facial recognition technology, in an effort to “reign[] in the use of” facial recognition technology. The BIPA is considered a heavy-hitting statute, as section 15(c) indicates: “No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person’s or a customer’s biometric identifier or biometric information.” The BIPA’s private right of action under section 20 specifies that: “Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party.” The statutory language allows any person aggrieved by a violation of the BIPA to bring an action in state or federal court.

In 2017, the State of Washington enacted a law governing biometric privacy. As the BIPA and the CUBI differ between themselves, the Washington statute also differs in its statutory definition of biometric information collection and in regards to civil penalties for biometric

257. Zimmerman, supra note 14, at 651.
259. Werner, supra note 236.
260. See Nakar & Greenbaum, supra note 41, at 91-92 (discussing that many companies, such as “Facebook, Shutterfly, Snapchat, and Google have each been sued over their implementation of FRT, particularly in Illinois under the BIPA”).
261. § 14/15(c) (2010).
262. § 14/20.
263. Id.
264. Lessack, supra note 234.
privacy violations. As such, there is a growing need for uniformity as states are increasingly adopting their own standards concerning the use and disclosure of biometric information. With differing state biometric privacy laws, companies that collect, store, and/or use biometric information will need a clear and uniform set of guidelines to follow when implementing biometric identification programs.

Most recently, on June 28, 2018, California Governor Jerry Brown signed a bill into law, effectively creating the California Consumer Privacy Act of 2018 ("CCPA"). The CCPA became "the strictest consumer data protection law in the country." The CCPA is relevant and appropriate, as it employs parts of the European GDPR:

[T]he CCPA gives consumers access to their data, the right to have their personal data deleted and the ability to opt out of having their data sold. The CCPA also goes further than any existing law in the United States. At the federal and state level, the U.S. has various data protection and privacy laws focused on specific financial, health and student information. However, these laws largely leave the bulk of the data economy—everything from data brokers to social media—beyond reproach.

The CCPA has statutory damages set at "$100 to $750 per person, per breach, or actual damages, whichever is greater . . . damages are higher for a civil suit brought by the attorney general." The CCPA is a large step in bringing accountability to the data economy.

IV. FEDERAL BIOMETRIC DATA AGENCY: REGULATING THE COLLECTION, STORAGE, AND USE OF SMARTPHONE USERS' SENSITIVE DATA

A solution to the legal issue explained above is twofold: first, a proposed broad federal legislation that regulates—similarly to the BIPA,
the CUBI, the CCPA, and the GDPR—the collection, storage, and use of smartphone users' sensitive biometric data; and second, the creation of the Federal Biometric Data Agency ("FBDA") tasked with the enforcement of the proposed biometric legislation.\textsuperscript{273} Having discussed the most progressive biometric data privacy legislation to date among the states and the EU, this Note proposes a preventative and uniform approach to the legal problem of biometric data privacy regulation.\textsuperscript{274} Below, Subpart A gives an overview of notable United States legislative responses to certain historical crises.\textsuperscript{275} Subpart B extends the federal agency creation concept by proposing the application of the said concept to the creation of the FBDA.\textsuperscript{276} Subpart B further proposes the application of parts of leading biometric data privacy laws to create a uniform federal biometric data privacy law in the United States.\textsuperscript{277}

**A. Creating Federal Agencies in Response to Crises**

In October 1929, when the stock market crashed, Congress held hearings to identify problems and solutions to the lack of public confidence in U.S. markets.\textsuperscript{278} The congressional intervention during the peak of the Great Depression resulted in the passage of the Securities Act of 1933 and the Securities Exchange Act of 1934 ("SEA"), which created the Securities and Exchange Commission ("SEC").\textsuperscript{279} The Securities Act of 1933 and the SEA were designed to restore investor confidence in the stock market:

[B]y providing investors and the markets with more reliable information and clear rules of honest dealing. The main purposes of these laws can be reduced to two common-sense notions: [(1)] Companies publicly offering securities for investment dollars must tell the public the truth about their businesses, the securities they are selling, and the risks involved in investing. [(2)] People who sell and trade securities — brokers, dealers, and exchanges — must treat investors fairly and honestly, putting investors' interests first. Monitoring the securities industry requires a highly coordinated effort. Congress established the

\textsuperscript{273} See Zimmerman, supra note 14, at 644, 664 (noting that there is no uniform federal law regulating the collection, storage, use, and trading of biometric information, and that "[p]rotection for consumers' biometric information will only be as strong as the laws or regulations that are put in place to govern the private industry's collection and storage of this sensitive information.").

\textsuperscript{274} See supra Part II.C; infra Part IV.A-B.

\textsuperscript{275} See infra Part IV.A.

\textsuperscript{276} See infra Part IV.B.

\textsuperscript{277} See infra Part IV.B.

\textsuperscript{278} The Role of the SEC, INVESTOR, https://www.investor.gov/introduction-investing/basics/role-sec (last visited Nov. 18, 2019).

\textsuperscript{279} Id.
Securities and Exchange Commission in 1934 to enforce the newly-passed securities laws, to promote stability in the markets and, most importantly, to protect investors. The SEC’s mission is “to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation.”

More recently, in response to the financial crisis of 2008, the Obama Administration enacted the Dodd-Frank Wall Street Reform and Consumer Protection Act (hereinafter “Dodd-Frank Act”) in 2010. Importantly, the Dodd-Frank Act created a federal agency, the Consumer Financial Protection Bureau (“CFPB”). The CFPB is a regulatory agency that oversees financial products and services to consumers. One could argue that creating federal agencies is costly, as the federal government is currently operating at a deficit; however, as growing pressures rise, the cost to individuals whose biometric information is compromised can be just as steep of a price.

B. Proposed Response to the Biometric Data Privacy Crisis

Similar to the advent of the SEC and the CFPB, in response to growing technology affecting the personal data of millions of individuals,

---

281. Id.
282. Will Kenton, Dodd-Frank Wall Street Reform and Consumer Protection Act, INVESTOPEDIA, https://www.investopedia.com/terms/d/dodd-frank-financial-regulatory-reform-bill.asp (last updated May 10, 2019) (noting that one of the ways the Dodd-Frank Act heavily regulates the United States financial system is by “monitoring the financial stability of major financial firms whose failure could have a serious negative impact on the U.S. economy (companies deemed ‘too big to fail’”).
283. Id.
284. Id. The CFPB helps consumer finance markets work more efficiently by providing and enforcing rules:
The [CFPB], established under Dodd-Frank, was given the job of preventing predatory mortgage lending (reflecting the widespread sentiment that the subprime mortgage market was the underlying cause of the 2008 catastrophe) and make it easier for consumers to understand the terms of a mortgage before agreeing to them. It deters mortgage brokers from earning higher commissions for closing loans with higher fees and/or higher interest rates and requires that mortgage originators not steer potential borrowers to the loan that will result in the highest payment for the originator. The [Dodd-Frank Act] was intended to prevent another financial crisis like the one in 2008.
Id.
the EU responded by enacting the GDPR.\textsuperscript{286} In light of the biometric data privacy crisis throughout the EU, the GDPR offers a "strong and more coherent data protection framework in the Union, backed by strong enforcement."\textsuperscript{287} The GDPR works well in the EU, in part, because of the increased penalties associated with non-compliance.\textsuperscript{288} Fines can be heavy for companies that fail to follow certain GDPR regulations, as the GDPR allows for supervisory authorities:

Supervisor authorities have investigative powers and can issue warnings for non-compliance, perform audits, and need companies to meet deadlines. The supervising authorities watch the data controllers and processors to make sure that they met the demands of the GDPR. If a supervising authority finds that an organization has been in violation, then they have the power to put sanctions on companies that have failed to follow with the Regulation. Instead of being fined a specific number, the GDPR will base sanctions on the affected company’s revenue. If companies do not follow with certain GDPR regulations, then the fines that are imposed may be up to 4\% of the annual income for a corporation.\textsuperscript{289}

Consequently, and due to the extraterritorial reach of the GDPR, American companies who wish to do business in the EU must be aware of GDPR regulations if they wish to remain compliant.\textsuperscript{290}

As the GDPR was enacted to provide uniform biometric data protection across the EU, it is imperative that the United States follow suit to protect biometric data with a uniform regulatory scheme.\textsuperscript{291} Already, the "Internet Association and other industry leaders prefer a federal law to a patchwork of state rules."\textsuperscript{292} This can be accomplished through federal legislation modeled after the leading privacy regulations discussed in this Note such as the GDPR, the BIPA, the CUBI, and the CCPA.\textsuperscript{293}

Just as the GDPR allows for supervisory authorities with investigative powers to audit and ensure compliance, the FBDA would have similar authority to the supervisory authorities in the EU, much like the SEC and CFPB’s authority over financial matters here in the United

\begin{footnotesize}
\begin{itemize}
    \item \textsuperscript{286} See supra Part II.C.
    \item \textsuperscript{287} See GDPR, supra note 138, at art. 1(7).
    \item \textsuperscript{288} Id. at art. 58(2)(a)–(j); see also Monajemi, supra note 59, at 393.
    \item \textsuperscript{289} Monajemi, supra note 59, at 393. See generally GDPR, supra note 138, at art. 58 (listing the investigative, corrective, authorization, and advisory powers of the supervisory authorities, including the power to issue opinions and draft codes, and order the erasure and recertification of personal data).
    \item \textsuperscript{290} Monajemi, supra note 59, at 390.
    \item \textsuperscript{291} See Zimmerman, supra note 14, at 644.
    \item \textsuperscript{292} Tashea, supra note 268.
    \item \textsuperscript{293} See supra Parts II.C, III.B.
\end{itemize}
\end{footnotesize}
A notable difference between the FBDA and the GDPR is that the FBDA would have sole authority to regulate, audit, and ensure biometric data privacy compliance, as opposed to multiple supervisory authorities. As previously discussed, existing privacy laws in states like Illinois, Texas, and California have already made an impact on biometric privacy rights.

The proposed federal biometric data privacy scheme would highlight effective language from the current models, for example, the BIPA and the CCPA create a private right of action for victims of biometric data privacy violations. Following the BIPA’s threat of liquidated and statutory damages of up to $5000 per violation, and civil penalties of up to $25,000 under CUBI, a federal penalty of up to $10,000 per violation, applied on a national level, would place companies under the threat of heavy uniform penalties, thereby incentivizing compliance with federal biometric data privacy law.

Federal biometric data privacy legislation modeled after current state laws would center around biometric identifiers, including retina and iris scans, fingerprints, voiceprints, hand geometry, and face geometry. Furthermore, the federal legislation needs a broad application, not one that is limited to biometric information solely used for commercial purposes such as the Texas CUBI. A critical component of federal biometric data privacy laws is the requirement of informed consent prior to any disclosure of an individual’s biometric information. Lastly, like the BIPA, the CUBI, the CCPA, and the GDPR, the proposed federal legislation would require companies to permanently destroy biometric information either: (1) at the request of the individual; (2) once the individual terminates interaction with the company; or (3) within a reasonable period of time after the information was initially collected.

Much like with other federal agencies, such as the SEC, crucial to the effectiveness of federal biometric data privacy law is its enforcement. Each year “the SEC brings hundreds of civil enforcement actions against individuals and companies for violation of the securities laws.293
The federal biometric data privacy legislation would create the FBDA and its responsibilities—such as the interpretation and enforcement of federal biometric data privacy laws—would parallel the SEC’s responsibilities of interpreting and enforcing federal securities laws.305

Ultimately, the FBDA operating similarly to the SEC, would ensure: (1) the creation of new rules and the amending of existing rules; (2) inspection of companies’ biometric information programs; (3) that companies cannot profit from individuals’ biometric information; and (4) coordination of U.S. biometric data regulation with federal, state, and foreign authorities.306 The FBDA’s enforcement power paired with a national biometric privacy framework that preempts state laws and provides recourse for aggrieved individuals, much like the BIPA’s liquidated and statutory damages clause and the CCPA’s damages clause, would force companies to act in the interest of the individuals.307 This Note ultimately proposes a federal biometric data protection law that, at its very core, like the CCPA and the GDPR, gives “consumers access to their data, the right to have their personal data deleted and the ability to opt out of having their data sold.”308

V. CONCLUSION

It is certainly awe-inspiring to look back to times as recent as the last turn of the century and admire how far technology has come.309 In turn, it has become difficult to imagine a world without smartphones, and subsequently, a world without the problems caused by such advanced technology.310

There is undoubtedly a need for broad federal legislation and for the proposition of model legislation.311 As stated above, the proposed creation of the FBDA and uniform federal legislation modeled after the GDPR, the BIPA, the CUBI, and the CCPA would ensure that everyday people like Lindabeth Rivera and Joseph Weiss have the necessary recourse, should their biometric information become compromised.312
The enactment of the GDPR in the EU has increasingly put pressure on the United States to keep up with data privacy initiatives. History has shown that Congress has resorted to creating agencies, and while it may be costly, Congress did it in 2010. Broad federal legislation and the creation of the FBDA will keep the United States up to date with advancements in biometric technology, and it will lead the country in the right direction by protecting the biometric information of its citizens through pressuring companies to reassess their data protection operations and comply with federal law.

JP Raynal*

313. Tashea, supra note 268 (quoting California Democratic Assemblyman and co-author of the California Consumer Privacy Act of 2018, Ed Chau: “Europe is already ahead of us, as we’ve seen with GDPR”).

314. See supra Part IV.A.

315. See supra Parts III–IV.

* J.D. Candidate, Business Law Honors Concentration, 2020, Maurice A. Deane School of Law at Hofstra University; B.A. in History, Minor in Political Science, 2015, Fordham University. First, I would like to thank my parents and family for being supportive and for making all of this possible. Second, I would like to thank my Ancona family in New York for supporting me with delicious homemade Italian food, never-ending humor, and moral support. Third, I would like to thank the entire membership of the Hofstra Law Review, especially the Volume 48 Managing Editors, Amy ElSayed, Sabrina Salama, and Madelyn Nicolini. This publication would not be possible without their leadership and hard work, as well as the dedication and effort provided by the remaining editors and staff members who contributed to the publication process. I would also like to extend a special thank you to Lindsay Wasserman, Nina Patel, and Aaron Shubert, the Articles Editor, Research Editor, and Notes Editor, respectively, for their extensive contributions to the entire editing process. I would like to thank Professor J. Scott Colesanti, my faculty advisor, for his support and guidance throughout the note-writing process. Lastly, I thank my friends and my girlfriend for supporting me and for always pushing me to be my best.