Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 25 *Volume XXV*
Number 3 *Volume XXV Book 3*

Article 5

2015

Biometric Boom: How the Private Sector Commodifies Human Characteristics

Elizabeth M. Walker
Fordham University School of Law

Biometric Boom: How the Private Sector Commodifies Human Characteristics

Cover Page Footnote

The Author would like to thank Professor Shlomit Yanisky-Ravid for her invaluable wisdom and guidance throughout the development of this Note. The Author specially thanks her parents, Richard and Joy, for their unconditional love and support. The Author thanks her brother, James, for his encouragement to never stop learning.

Biometric Boom: How the Private Sector Commodifies Human Characteristics

Elizabeth M. Walker*

Biometric technology has become an increasingly common part of daily life. Although biometrics have been used for decades, recent advances and new uses have made the technology more prevalent, particularly in the private sector. This Note examines how widespread use of biometrics by the private sector is commodifying human characteristics. As the use of biometrics has become more extensive, it exacerbates and exposes individuals and industry to a number of risks and problems associated with biometrics. Despite public belief, biometric systems may be bypassed, hacked, or even fail. The more a characteristic is utilized, the less value it will hold for security purposes. Once compromised, a biometric cannot be replaced as would a password or other security device.

This Note argues that there are strong justifications for a legal structure that builds hurdles to slow the adoption of biometrics in the private sector. By examining the law and economics and personality theories of commodification, this Note identifies market failure and potential harm to personhood due to biometrics. The competing theories justify a reform to protect human characteristics from commodification. This Note presents a set of principles and tools based on defaults, disclosures, incentives, and taxation to discourage use of biometrics, buying time to strengthen the technology, educate the public, and establish legal safeguards for when the technology is compromised or fails.

---

* Editor-in-Chief, *Fordham Intellectual Property, Media & Entertainment Law Journal*, Volume XXVI; J.D. Candidate, 2016, Fordham University School of Law; B.S., 2005, Boston College. The Author would like to thank Professor Shlomit Yanisky-Ravid for her invaluable wisdom and guidance throughout the development of this Note. The Author specially thanks her parents, Richard and Joy, for their unconditional love and support. The Author thanks her brother, James, for his encouragement to never stop learning.

INTRODUCTION

On any given afternoon, a person shops at a grocery store, withdraws money from an ATM, and checks her smartphone a dozen times. Except she performs these tasks with a biometric: the grocery store implemented a system to pay with a fingerprint, the bank's ATM requires a fingerprint instead of a PIN, and a fingerprint unlocks the screen of her smartphone. These uses of fingerprints are enormously convenient, and perhaps the individual feels more secure because her accounts are protected by something that

is attached to her body. But how many other things did she touch that day? Probably door handles, coffee cups, light switches, tables, books, and countless other things. Does that mean she left her "password" or "key" on all these items? Suppose her bank notifies her that it suffered a data breach. How does she change her fingerprint?

Fingerprints are merely a type of biometric. The term biometrics is often used interchangeably to describe a characteristic or a method.[1] As a characteristic, biometrics means measurable physiological or behavioral characteristics of a person that may be used for recognition.[2] Measurable physiological characteristics include fingerprints, face, iris, retina, and hand geometry; examples of measurable behavioral characteristics are voice, keystroke, signature, and gait.[3] As a method, biometrics means the process of automated recognition based on a person's measurable characteristic.[4] Biometric systems essentially make the human body "machine-readable."[5]

Scholarly analysis of biometrics generally relates to government uses, such as national security and surveillance.[6] However, this

---

[1] *See* CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 31:1 (2013). This Note primarily uses "biometrics" to refer to human measurable characteristics and uses "biometric system" when discussing the recognition process.

[2] *See* NSTC SUBCOMM. ON BIOMETRICS, BIOMETRICS "FOUNDATION DOCUMENTS" 1 (2006), *available at* http://www.biometrics.gov/Documents/biofoundationdocs.pdf [hereinafter Foundation Documents].

[3] *See* Ishwar K. Sethi, *Biometrics: Overview and Applications*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 117, 117 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006). There is some debate as to whether DNA is a biometric because DNA recognition is not currently automated. *See* Foundation Documents, *supra* note 2, at 21.

[4] *See* Foundation Documents, *supra* note 2, at 1.

[5] *See* Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technology*, 00720/12/EN, WP 193, at 4 (Apr. 27, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf [hereinafter WP 193].

[6] *See, e.g.*, Lauren D. Adkins, *Biometrics: Weighing Convenience and National Security Against Your Privacy*, 13 MICH. TELECOMM. & TECH. L. REV. 541 (2007); Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407 (2012); Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475 (2013); Rudy Ng, *Catching Up To Our Biometric*

Note examines the rapidly expanding use of biometrics by the private sector. Does extensive use across industries accelerate the transformation of nonsalable attributes into market goods? For what purposes is it justified to use something so closely associated with oneself? This Note claims that widespread use of biometrics by the private sector is commodifying human characteristics and exacerbating other risks and problems associated with biometrics.

Biometrics are not new. For decades, law enforcement has used fingerprint analysis during criminal investigations.[7] However, in the last few decades, technology has helped to automate the process and allow more human characteristics to be utilized for recognition.[8] These technological advancements, coupled with growing concerns for terrorism and cybersecurity, are propelling the growth of biometric technology.[9] Biometrics offer a number of advantages over other security systems. The characteristics are well-suited as identifiers because they are unique to each individual.[10] Also, biometric identifiers are convenient; because humans carry the characteristic on their body at all times and it cannot be forgotten, biometrics eliminate the need to remember PINs and passwords or to carry identification documents.[11]

However, this Note demonstrates that the private sector's use of biometrics raises significant privacy and security concerns. Privacy is about power over information, determining who should access and use information.[12] Companies are beginning to collect

---

Future: Fourth Amendment Privacy Rights and Biometric Identification Technology, 28 HASTINGS COMM. & ENT. L.J. 425 (2006).

7 *See* Donohue, *supra* note 6, at 418–19; NANCY YUE LIU, BIO-PRIVACY: PRIVACY REGULATIONS AND THE CHALLENGE OF BIOMETRICS 4 (2012).

8 *See* Foundation Documents, *supra* note 2, at 7; LIU, *supra* note 7, at 10–11.

9 *See* LIU, *supra* note 7, at 3.

10 *See* Robyn Moo-Young, *"Eyeing" the Future: Surviving the Criticisms of Biometric Authentication*, 5 N.C. BANKING INST. 421, 422 (2001). It should be noted that biometrics are not truly universal as some individuals may not have a specific characteristic due to disease, birth defects, or other causes, which could lead to discrimination as biometric systems are more widely implemented. *See* LIU, *supra* note 7, at 68.

11 *See* Robin Feldman, *Considerations on the Emerging Implementation of Biometric Technology*, 25 HASTINGS COMM. & ENT. L.J. 653, 662 (2003); DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 201 (2011).

12 *See* Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 673 (2013).

biometrics in exchange for something else or without an individual's knowledge. Because biometrics are easily obtained, individuals are left powerless over the collection and use of their characteristics. Similarly, if an individual is left with a binary choice of whether to provide biometrics or forgo a product, the collector has all the power in the transaction.

Security, on the other hand, determines who can actually access and use information; it implements the privacy choices.[13] Biometrics are being used as a security measure; attributes are protecting other personal information. Most individuals believe that biometrics systems are accurate and secure. However, this Note demonstrates the alarming number of flaws in biometric systems, such as the countless ways in which biometrics can be hacked and compromised. Further, a significant risk with biometrics is that they are irreplaceable. Reliance is rapidly being placed on human attributes that cannot be changed. In a world where data breaches are common occurrences, individuals should be prepared to change passwords and other security measures frequently. The numerous risks associated with biometrics are accentuated as the technology becomes more prevalent.

This Note argues that widespread use, propelled by the private sector, causes more parties to be interested in biometrics. As more biometric systems are implemented, unique human characteristics become more commonplace, heightening concerns for irreplaceability and security. This Note demonstrates that competing theories of commodification justify reform to protect biometrics. The law and economics approach, which places all things in the free market, allows intervention when faced with an inefficient market. Extensive evidence demonstrates that the nature of privacy, biometrics, and human cognition result in market failure. A similar conclusion is reached when biometrics are analyzed under Margaret Radin's personality theory, where personal attributes are too personal to be monetized. Rather, the noncommodified version of biometrics fosters personhood and improves social interactions.

This Note concludes that there are strong justifications for a legal structure that builds hurdles to slow the adoption of biometrics

---

[13] *See id.* at 676–78.

in the private sector. Based on choice architecture, this Note presents a system of defaults, disclosures, and incentives to push the private sector, and individuals, away from utilizing biometrics. There is no way to prevent the use of biometrics altogether, but forcing companies and individuals to slow down will give society time to consider the risks, fortify security, and build safeguards for when the technology is compromised or fails. The proposed principles and set of tools are consistent with the self-regulation and limited government regulation traditions of the United States.

Part I explains how biometric technology operates and how the private sector is using biometrics. The discussion assesses the security vulnerabilities and serious risks of using biometrics. Part II explores competing theoretical views of commodification and concludes that due to the nature of biometrics and problems with privacy, intervention and reform are needed to govern biometrics. Part III describes available legal tools that may be applied to biometrics. The discussion suggests that current legal structures are inadequate to govern biometrics in the United States, but that a hybrid solution may be more effective. Part IV proposes a set of principles to guide collection, use, and storage of biometrics by the private sector. The proposal attempts to establish hurdles to slow the adoption and discourage private entities and individuals from utilizing biometrics.

I. BIOMETRICS OVERVIEW

This Part provides an overview of biometric technology. First, there is an explanation of how the technology operates and its vulnerabilities. This Part also reviews the private sector's growing list of diverse biometric implementations. Finally, there is a discussion of how the private sector's rapid adoption is spurring the commodification of biometrics, which in turn is aggravating other problems associated with the technology.

A. System Operation & Vulnerabilities

Biometric systems are pattern recognition systems most often used to verify or identify an individual.[14] The first phase of the process is enrollment where an individual's biometric characteristic is captured by a sensor device.[15] The device extracts key features from the characteristic and produces a mathematical model called a template.[16] The system predetermines which features it will extract and use for matching, and the templates only encode those extracted features.[17]

The second phase is either verification or identification.[18] An individual presents her characteristic to the device and the system conducts a search to match the presented characteristic against existing templates.[19] Matching results are based on statistical certainty that the presented characteristic and existing template are from the same person.[20] Verification, or "one-to-one" matching, is used to confirm an individual; the system matches the presented characteristic against the individual's claimed identity.[21] Identification, or "one-to-many" matching, is used to recognize an individual; the system searches a database of stored templates to match the presented characteristic.[22] The identification process depends on a database of stored templates; however, verification may match templates stored in a database or stored locally in a token or identification card.[23]

The benefit of biometric systems is that they are more secure than other security measures currently available. Biometrics produce significantly longer data streams than any password a human

---

14 *See* Sethi, *supra* note 3, at 119; Stephen Hoffman, *Biometrics, Retinal Scanning, and the Right to Privacy in the 21st Century*, 22 SYRACUSE SCI. & TECH. L. REP. 38, 46 (2010).

15 *See* LIU, *supra* note 7, at 32.

16 *See id.*

17 *See id.* at 119–20.

18 *See* Sethi, *supra* note 3, at 120.

19 *See id.* at 120–21.

20 *See* LIU, *supra* note 7, at 33.

21 *See* Sethi, *supra* note 3, at 118.

22 *See id.*

23 *See* LIU, *supra* note 7, at 32.

could recall.[24] Long passwords are more secure against attacks than shorter passwords.[25] However, just because the technology is more secure by comparison does not mean that it is secure in and of itself. The technology actually has a number of troubling vulnerabilities.[26] One point of attack is faking—also called "spoofing"—the characteristic.[27] Studies have shown that biometric systems can be bypassed with fake fingerprints and high resolution images of eyes and faces.[28] Another potential breach is through modifying the template, which is based on a discrete number of features.[29] Someone looking to bypass the system would only need to know the features the system uses and would not have to replicate the exact characteristic.[30] Finally, because a characteristic is saved as data, a template may be decoded leaving biometric systems vulnerable to hacking just like other password-based systems.[31]

A related concern is the ongoing cybersecurity arms race.[32] Even as security measures become more advanced, hackers continue to find flaws, causing security to be repaired and further strengthened.[33] This constant back-and-forth game means that hackers are usually ahead of security experts.[34] Technology will always be

---

[24] *See* Nalini K. Ratha et al., *An Analysis of Minutiae Matching Strength*, *in* AUDIO- AND VIDEO-BASED BIOMETRIC PERSON AUTHENTICATION: THIRD INTERNATIONAL CONFERENCE, AVBPA 2001 HALMSTAD, SWEDEN, JUNE 2001 PROCEEDINGS 225 (Springer 2001), *available at* http://www.cse.msu.edu/~rossarun/BiometricsTextBook/Papers/Security/Ratha_MinaMatchingStrength_AVBPA01.pdf.

[25] *See id.*

[26] For a longer discussion on biometric system security and vulnerability, see Anil K. Jain & Ajay Kumar, *Biometric Recognition: An Overview*, *in* SECOND GENERATION BIOMETRICS: THE ETHICAL, LEGAL AND SOCIAL CONTEXT 49, 60–65 (Emilio Mordini & Dimitros Tzovaras eds., 2012); Gang Wei & Dongge Li, *Biometrics: Applications, Challenges and the Future*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 135, 142–45 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006).

[27] *See* Jain & Kumar, *supra* note 26, at 60–61.

[28] *See* SOLOVE, *supra* note 11, at 202; Sethi, *supra* note 3, at 131–32.

[29] *See* Jain & Kumar, *supra* note 26, at 61.

[30] *See id.*

[31] *See* DATA BREACH AND ENCRYPTION HANDBOOK 204 (Lucy L. Thomson ed., 2011).

[32] *See* Harry Bruinius, *Feds Hacked: Is Cybersecurity a Bigger Threat Than Terrorism?*, CHRISTIAN SCI. MONITOR (Nov. 10, 2014), http://www.csmonitor.com/USA/2014/1110/Feds-hacked-Is-cybersecurity-a-bigger-threat-than-terrorism-video.

[33] *See id.*

[34] *See id.*

vulnerable to sophisticated hackers.[35] Even if biometrics are currently more secure than other security measures, that does not mean that they will always be more secure.

There is also a common misconception that biometric systems are precise. Rather, it is actually impossible for a biometric system to be 100% accurate.[36] The results are based on statistical certainty and—by the nature of the technology—the system must accept false positives and false negatives.[37]

These flaws are significant. The movement towards biometrics is based on the belief that the systems are secure and accurate, two arguments easily refuted. As the following section demonstrates, biometrics are being rapidly adopted for a variety of uses. However, in light of the technological vulnerabilities, it seems foolish that the technology is being relied upon so heavily.

B. Expanding Uses

The government was an early adopter of biometric technology, and its predominant use of the technology is for security purposes. The Department of Homeland Security uses fingerprint scanning and facial-recognition technology to record the identities of visitors to the United States.[38] Similarly, many states require fingerprint scanning to confirm an individual's identity before distributing welfare or unemployment benefits.[39] Some public schools have even begun allowing children to pay for lunch using their finger- or handprint.[40]

However, the private sector has also begun implementing biometric systems. Without any restrictions on what can be collected or how it may be used, industry is rapidly expanding the prevalence of biometric systems. Security is the most common purpose for which the private sector uses biometrics. Examples include Ap-

---

35 *See id.*

36 *See* Hu, *supra* note 6, at 1535.

37 *See id.*; LIU, *supra* note 7, at 33.

38 *See* FISHMAN & MCKENNA, *supra* note 1, § 31:38.

39 *See id.* § 31:43.

40 *See School Cafeterias Trading Lunch Money For Fingerprint Scans*, CBS CHI. (July 2, 2014, 12:49 PM), http://chicago.cbslocal.com/2014/07/02/school-cafeterias-trading-lunch-money-for-fingerprint-scans/.

ple's Touch ID, which allows users to unlock their phones and tablets with a fingerprint;[41] amusement parks, including Disney World, require patrons to scan their fingerprints to use passes;[42] some ATMs are equipped with fingerprint scanners;[43] MasterCard announced a fingerprint-enabled credit card;[44] and some hospitals are scanning patient hands in order to retrieve the correct medical records.[45] Recently, banks have begun storing and processing voice samples of customers calling about their accounts to create a "voiceprint."[46] The bank will use the voiceprint to verify the customer's identity and prevent fraudsters from gaining access to an account over the telephone.[47]

Companies are also beginning to explore other purposes for biometric technology. A recent trend in biometric use is to provide a value-add service based on individuals' characteristics. Facebook launched a feature that "tagged" individuals in uploaded images.[48] The site collected and stored biometric information from millions of users and utilized facial recognition technology to automatically identify the individuals.[49] Another example of a value-add use of biometrics is Google Audio History.[50] This opt-in service retains recordings of voice searches or commands so the company can learn the sound of an individual's voice and provide better results when speech recognition products are used.[51]

---

41 *See Use Touch ID on iPhone and iPad*, APPLE, http://support.apple.com/en-us/HT5883 (last modified Mar. 3, 2015).

42 *SEE FINGER SCANNING AT THEME PARKS*, MY FOX ORLANDO (MAY 9, 2012, 11:58 PM), http://www.myfoxorlando.com/story/18248551/finger-scanning-at-theme-parks.

43 *See* FISHMAN & MCKENNA, *supra* note 1, § 31:46.

44 *See* Darrell Etherington, *MasterCard Will Borrow a Touch ID Trick for Fingerprint Scanning Credit Card*, TECHCRUNCH (Oct. 17, 2014), http://techcrunch.com/2014/10/17/mastercard-will-borrow-a-touch-id-trick-for-fingerprint-scanning-credit-card/.

45 *See* Eliene Augenbraun, *How Biometric Palm Scans Help Keep Hospitals Secure*, CBS NEWS (Oct. 27, 2014, 5:00 AM), http://www.cbsnews.com/news/patientsecure-biometric-palm-scan-system-hospital-security/.

46 *See* Raphael Satter, *Banks Harvest Callers' Voiceprints to Fight Fraud*, USA TODAY (Oct. 13, 2014, 3:20 PM), http://www.usatoday.com/story/money/business/2014/10/13/voiceprints-harveted/17207381/.

47 *See id.*

48 *See* FISHMAN & MCKENNA, *supra* note 1, § 31:45.

49 *See id.*

50 *See Google Voice & Audio History*, GOOGLE, https://support.google.com/websearch/answer/6030020 (last visited Mar. 9, 2015).

51 *See id.*

Finally, the private sector is also using biometrics for advertising. Digital billboards can use facial recognition to identify a viewer's gender, age, and ethnicity.[52] For example, an advertising campaign in London only displayed advertisements to women who looked at the billboard.[53] The ability to use biometrics for advertising is an emerging field, with some companies exploring how they can use social media photographs to identify an individual in the real world.[54]

Use of biometrics has become much more expansive in recent months, and it is likely that the private sector will devise further uses for biometrics. Such pervasive and widespread uses reduce the effectiveness of human attributes for security purposes, exposing the data to more system vulnerabilities. It also degrades the value of the characteristics as security identifiers. Suddenly the private sector values fingerprints, eyes, voices, and faces more significantly than the individuals do.

C. Commodification and Other Risks

Biometrics share many similarities with personal information, and the problems plaguing information privacy and security are also relevant concerns for biometrics. Personal information has been commodified; it is now a type of good that can be exchanged for something else.[55] Two factors that significantly contributed to the commodification of personal information were technology and the private sector. Technology changed the way information is collected, used, and stored. Personal information, which was once difficult to acquire and process, has been made significantly easier to access by advances in technology. The ease of information flow was

---

[52] *See* Michael Fitzpatrick, *Advertising Billboards Use Facial Recognition to Target Shoppers*, GUARDIAN (Sept. 27, 2010, 2:00 AM), http://www.theguardian.com/media/pda/2010/sep/27/advertising-billboards-facial-recognition-japan.

[53] *See* Erica Ho, *Face-Recognizing Billboard Shows Ad to Women Only*, TIME (Feb. 23, 2012), http://newsfeed.time.com/2012/02/23/face-recognizing-billboard-shows-ad-to-women-only/.

[54] *See* Chris Strohm, *Facial Recognition on Facebook to IPhone Awaits U.S. Code*, BLOOMBERG (Dec. 16, 2013, 12:00 AM), http://www.bloomberg.com/news/2013-12-16/facial-recognition-on-facebook-to-iphone-awaits-u-s-code.html (discussing Redpepper facial recognition application).

[55] *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2069 (2004).

exacerbated by the private sector sharing and aggregating information.

An example of this downward spiral is the Social Security number. Social Security numbers were never intended as a general use identifier.[56] However, because everyone has one, the government and the private sector have adopted it as an identifier.[57] As more institutions adopted the number, it became less effective as a password.[58] Technology sped up dispersal of the numbers.[59] Today, the Social Security number is considered the most valuable piece of information to a criminal because it is a "skeleton key" for all accounts.[60]

Given how the private sector and technology spurred the commodification of social security numbers, extensive industry use of biometrics also commodifies human characteristics. Despite using biometrics for years, technology has automated the process and allowed for the storage and processing of more characteristics than were possible before. Recent private sector uses show how these characteristics are being collected and used at an alarming rate.[61] As is occurring with personal information, companies are collecting biometrics in exchange for goods and services, or even without the knowledge of the individuals. This leaves individuals without the power to choose how to control their own biometrics. The private sector's behavior is propelling the widespread use of biometrics, which reduces their effectiveness for security. Further, commodification exacerbates existing problems and risks associated with biometrics.

While some problems are the result of information privacy generally, biometrics also carry their own unique set of risks. The most significant risk with using biometrics is that the characteristics are

---

[56] *See* Carolyn Puckett, *The Story of the Social Security Number*, 69(2) SOC. SECURITY BULL., 55, 67, (2009) *available at* http://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.pdf.

[57] *See id.*

[58] *See* Jonathan J. Darrow & Stephen D. Lichtenstein, *"Do You Really Need My Social Security Number?" Data Collection Practices in the Digital Age*, 10 N.C. J.L. & TECH. 1, 4 (2008).

[59] *See id.* at 5.

[60] *See id.* at 4, 10.

[61] *See supra* notes 41–54 and accompanying text.

irreplaceable.[62] Currently, if a database is hacked, an individual can change her password or request a new credit card. However, if the system uses biometric verification for its security and the database is compromised, she cannot change or replace her fingerprint, eye, face, or other characteristics.[63] Another concern is that biometrics cannot be stored anonymously because they are, by their nature, identifying information.[64] The ability to link a person to data is a critical privacy issue and central to existing privacy regulations.[65] Finally, unlike passwords which must remain secret to be effective, many biometrics are publicly accessible and can be captured without an individual knowing. Individuals leave their fingerprints on countless items every day, and their faces and voices are shared with those around them. The availability of the characteristics minimizes their effectiveness for security.[66]

Another risk associated with biometrics is that there is no adequate legal structure to govern the technology. As use of biometrics expands, proponents of the technology praise it as reliable and foolproof.[67] However, they are focused on the benefits without considering the consequences that will result when the technology fails.[68] Privacy scholar Daniel Solove calls this the "Titanic Phenomenon."[69] Builders of the Titanic were so confident of its unsin-

---

62 *See* SOLOVE, *supra* note 11, at 202.

63 That is not to say it is impossible with advancements in transplant science. However, if these types of transplants were to become possible, it seems an extreme measure to take when a biometric system is compromised. Further, the ability to replace characteristics dilutes the argument that biometrics are more secure than passwords.

64 *See* Article 29 Data Protection Working Party, *Working Document on Biometrics*, 12168/02/EN, WP 80, at 5 (Aug. 1, 2003), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf.

65 *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and A New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1816 (2011).

66 *See* Sethi, *supra* note 3, at 127–28 (describing covert collection of biometrics, including facial recognition).

67 *See, e.g.*, Hu, *supra* note 6, at 1477–78; *Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the S. Comm. on the Judiciary*, 107th Cong. 2 (2001) (statement of Sen. Dianne Feinstein, Chairperson of Subcomm. on Technology, Terrorism, and Government Information) ("Biometric identifiers are the most secure and convenient way to authenticate and identify people because they cannot be borrowed, stolen, forgotten or forged.").

68 *See* SOLOVE, *supra* note 11, at 199.

69 *See id.*

kability that they did not have enough lifeboats when the ship sank.[70] Solove believes the same is true of biometrics: proponents view the technology as infallible, but biometric systems will fail and, when they do, there will not be adequate safeguards.[71] Perhaps the risk of biometrics failing was less significant a year or more ago, or that fewer individuals and institutions would be affected if a biometric system did fail. However, the private sector's increased use of biometrics has reached a critical point. If there once was time to develop the technology and educate the public, the rapid implementation of biometric systems has taken all that time away. Instead, a flawed technology is being implemented and the public has misconceptions of its reliability. The reach of biometrics now ensures that should a system fail, or should an individual's characteristic be compromised, the effects will be extensive and disastrous. Solove does not propose preventing the use of biometrics completely, merely that society prepare itself and build proper legal protections.[72] One way to accomplish this is to consider the private sector's commodification and explore whether there is any way to justify intervention.

II. JUSTIFYING INTERVENTION: COMPETING THEORIES OF COMMODIFICATION

As discussed in the previous section, commodification aggravates risks associated with biometrics. This Part examines competing commodification theories and concludes that intervention in the emerging biometric market is justified. The first critique considers economic theory, which supports unrestricted transfers of biometrics, and points to market failure as an argument against trading biometrics. The second critique examines the personality theory, which opposes commodified biometrics because they harm personhood, and suggests the concept of "market-inalienable" where only monetized versions of biometrics are forbidden.

---

70 *See id.*

71 *See id.* at 201–02.

72 *See id.* at 203.

A. Biometrics as Market Transactions

Economics is concerned with efficiency. The basic definition of efficiency is Pareto efficiency, which exists in a voluntary market transaction where both parties benefit from the transaction.[73] Law and economics scholars have applied economic theory to nonmarket behavior, creating a metaphorical market in which everything becomes a market transaction.[74] This approach treats human attributes, relationships, and social interactions as commodities.[75] Such an expansive view of tradable goods stems from Hobbes who believed that any part of a person that someone else needs, wants, or values is something with a price.[76] This unrestricted choice of what goods to trade promotes autonomy.[77] Such a system of voluntary transfers is presumptively efficient.[78]

The economic approach sees biometrics as salable or tradable. This approach equates a fingerprint with a bar of soap or a bottle of soda; identities reduced to nuts and bolts. Companies currently provide goods and services in exchange for an individual's personal information.[79] Similar biometric exchanges are already occurring, with companies trading services for characteristics.[80] There is also a growing reliance on biometrics for security.[81] Using biometrics for these purposes creates a market for human attributes and identities. Individuals and companies are suddenly placing a monetary value where there previously was none. A biometric would be traded to whoever values it the most. Economic theory supports these voluntary exchanges so long as they lead to efficient outcomes.

---

[73] *See* ROBIN PAUL MALLOY, LAW IN A MARKET CONTEXT: AN INTRODUCTION TO MARKET CONCEPTS IN LEGAL REASONING 189–90 (2004).

[74] *See* GARY S. BECKER, THE ECONOMIC APPROACH TO HUMAN BEHAVIOR 3–14 (1976) (applying an economic analysis to nonmarket behavior).

[75] *See generally id.* (arguing that discrimination, marriage, and children are market transactions).

[76] *See* THOMAS HOBBES, LEVIATHAN 67 (Oxford Univ. Press 1929) (1651).

[77] *See* MILTON FRIEDMAN, CAPITALISM AND FREEDOM 13–15 (Univ. of Chi. Press 2002) (1962) (arguing that private economic activity in a free market creates economic freedom).

[78] *See* MALLOY, *supra* note 73, at 190.

[79] *See* Schwartz, *supra* note 55, at 2069.

[80] *See supra* Part I.B.

[81] *See id.*

Pareto efficiency depends on ideal circumstances, such as when parties to a transaction are rational, well informed, and operate in a competitive market.[82] However, "market failure" occurs in the absence of such ideals, when the market is no longer efficient.[83] Indicia of market failure include externalities, public goods, information asymmetries, and cognitive limitations.[84] Economists argue that when markets fail, intervention is necessary to remedy the parties' misaligned incentives.[85] Government regulation is a common example of market intervention, but the reform could be any force that changes the behavior of parties in the market.[86]

Many privacy scholars argue that information privacy suffers from market failure.[87] The following sections will use these arguments to draw comparisons between personal information and biometrics. These sections demonstrate that, just as with information privacy, biometrics suffer from market failure.

1. Externalities

It may not always be possible for an individual to fully assess all the costs and benefits of a transaction.[88] Some transactions have implications for society that are not fully realized when an individual pursues her own self-interest.[89] In such a transaction, the individual's cost is less than the true cost to society.[90] She pursues transactions that look good because they do not account for the ac-

---

[82] *See* Joseph Stiglitz, *Regulation and Failure*, *in* NEW PERSPECTIVES ON REGULATION 11, 11 (David Moss & John Cisternino eds., 2009).

[83] *See id.*; THOMAS J. MICELI, THE ECONOMIC APPROACH TO LAW 31 (2004).

[84] *See* MICELI, *supra* note 83, at 31–32; Cass R. Sunstein, *The Storrs Lectures: Behavioral Economics and Paternalism*, 122 YALE L.J. 1826, 1834 (2013).

[85] *See* Stiglitz, *supra* note 82, at 13.

[86] *See id.* at 22 n.2 (considering taxation and tort law as types of market-curing reform).

[87] *See, e.g.*, Schwartz, *supra* note 55, at 2076; EXEC. OFFICE OF THE PRESIDENT: PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 38 (2014), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf; David L. Baumer et al., *Tit for Tat in Cyberspace: Consumer and Website Responses to Anarchy in the Market for Personal Information*, 4 N.C. J.L. & TECH. 217, 242 (2003); Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CALIF. L. REV. 395, 476 (2000).

[88] *See* MALLOY, *supra* note 73, at 117.

[89] *See id.*

[90] *See* MICELI, *supra* note 83, at 31.

tual cost of her actions.[91] The individual cannot internalize all the costs, and thus imposes some costs—or "negative externalities"—on others.[92]

Negative externalities exist when an individual's privacy choices impose harms upon others.[93] An individual could choose to disregard her own privacy by sharing her biometrics with collecting companies. She believes she will benefit from the convenience and safety of using biometrics, and foresees the only potential costs as risking her own data. However, her choice supports questionable business methods.[94] If a company utilizes databases or shares individuals' biometrics, then her choice to enroll in its system supports practices that can harm others. Likewise, she will be supporting the use of biometrics as a security tool, which could become perverse the more widely it is used.

Similarly, when a company chooses to utilize biometrics, it harms individuals enrolled in the system. A company that decides to implement a biometric system considers the benefits of added security and reduced fraud. However, the company fails to consider the costs imposed on its customers. An individual may not have a choice whether to withhold her biometric, preventing her from making her own privacy decisions. Further, enrollment exposes an individual to unnecessary security risks, forcing her to rely on a vulnerable and irreplaceable security measure. The individual bears the cost, which is external to the company. The company has no incentive to minimize or properly safeguard its use of the technology.

A company collecting biometrics also imposes costs on individuals beyond its own customer base. If a biometric system is compromised, it could cause a ripple effect throughout biometric systems used by other companies because the same characteristic may be enrolled in multiple systems. Individuals in those other systems are harmed, even if they are not enrolled in the hacked system.

---

91 *See* MALLOY, *supra* note 73, at 117.

92 *See id.*

93 *See* Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 425, 445 (2011).

94 *See* Anita L. Allen, *An Ethical Duty to Protect One's Own Information Privacy?*, 64 ALA. L. REV. 845, 862 (2013).

Even where individuals or companies attempt to take precautions, they will be harmed by others who are not as cautious when they use biometrics.

2. Public Goods

A public good is something that is inexhaustible (when consumption of the good by one person does not reduce the available quantity for others) and nonexclusive (when no one can be denied consumption of the good, even if he did not pay for the good).[95] When nonpaying individuals consume public goods, they create the "free rider problem."[96] Failure to exclude the nonpayers causes a good to be overused or degraded.[97] This creates negative externalities because the nonpayer does not experience the full cost of its actions.[98] Often cited examples of public goods include clean air, public parks, and national defense.[99]

Information is also a public good.[100] It is either difficult or inefficient to exclude others from having a piece of information, and once it is paid for it can be used and transferred at no cost.[101] Biometric data is a type of information—whether in the form of data or as a permanent human characteristic—and thus is a public good. Providing a biometric to one company does not preclude an individual from sharing the same biometric with many other companies. Also, as previously discussed, biometrics are often freely available to the public.[102] Society benefits from social interaction and the ability to recognize others. The only way to prevent the sharing of biometrics would be to live in isolation.

Biometric collectors may also be nonpayers. Because many characteristics can be collected at a distance, companies may capture

---

95 *See* MICELI, *supra* note 83, at 32.

96 *See id.*

97 *See* MALLOY, *supra* note 73, at 124.

98 *See id.*; *supra* Part II.A.1.

99 *See* Schwartz, *supra* note 55, at 2084; Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1527 (2013).

100 *See* Joseph E. Stiglitz, *The Contributions of the Economics of Information to Twentieth Century Economics*, 92 Q.J. ECON. 1441, 1448 (2002); Niva Elkin-Koren & Eli M. Salzberger, *Law and Economics in Cyberspace*, 19 INT'L REV. L. & ECON. 553, 559 (1999).

101 *See* Stiglitz, *supra* note 100, at 1448.

102 *See supra* Part I.C.

biometrics without an individual's knowledge. Further, companies may use the same biometric in nonrivalrous ways.[103] In fact, it would be inefficient for every company to collect the same information, thus incentivizing the sharing of biometrics. The more companies that use a characteristic, the less valuable that characteristic will be for security purposes. Individuals, unable to exclude such companies, will be harmed by a company's choice to use their biometrics.

3. Information Asymmetries

Inefficiency can stem from information asymmetry—the scenario where the information available to the transaction parties is very different.[104] The imbalance may occur when information is withheld, misrepresented, or too costly to uncover.[105] While information asymmetries are common, that one party merely has more information than another party is not the critical problem.[106] Rather, inefficiencies arise where the information disparity has a negative effect on the parties' negotiations and the functioning of the market.[107]

In the personal information market, information asymmetries exist between collectors and the individuals whose information is collected.[108] First, individuals are often unaware that their information is being collected.[109] Second, even if an individual is aware, she does not know how the information may be used or if it will be shared.[110] Many individuals also lack an understanding of how privacy and security are affected by technology.[111]

---

[103] *See* Bruce H. Kobayashi, *Private Versus Social Incentives in Cybersecurity: Law and Economics*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY 13, 21 (Mark F. Grady & Francesco Parisi eds., 2006) (discussing cybersecurity information as a public good).

[104] *See* MALLOY, *supra* note 73, at 171–72.

[105] *See id.*

[106] *See* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 24 (1997).

[107] *See id.*

[108] *See* Netanel, *supra* note 87, at 476; Schwartz, *supra* note 55, at 2080.

[109] *See* Schwartz, *supra* note 55, at 2078.

[110] *See* Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality: A Survey*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 15, 17 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006).

[111] *See id.* at 24.

The same disparities occur with the collection of biometrics. Some biometrics can be captured without an individual's knowledge. A fingerprint can be lifted from another object, gait can be recorded from a distance, and face and voice samples are easily captured by cameras, phones, and other devices. Even if an individual consents to the collection, the processing of that information may be unknown. For example, the banks collecting voice samples did not disclose all relevant information to their customers. While the bank provided a warning that calls may be recorded, the notice did not specify that the voice samples are processed into voiceprints, or that the bank may share the voiceprint with other companies.[112]

Collectors are not incentivized to be forthright. Rather, companies use vague privacy policies and terms of service that do not accurately explain the company's practices.[113] A company often reserves the right to change its policy or terms at any time and without notice.[114] If individuals had all relevant information, they may not choose to freely trade their biometrics. As such, information asymmetries in a biometric market lead to inefficiencies.

4. Cognitive Limitations

Economic theory assumes that humans are rational actors who make rational decisions in the face of uncertainty.[115] Individuals are presumed to be forward-looking "utility maximizers."[116] However, behavioral economists argue that humans err, causing significant harms and leading to market failure and inefficiency.[117] Common cognitive mistakes include time inconsistencies, ignoring shrouded attributes, unrealistic optimism, and difficulty assessing risk.[118]

Economists believe that humans consider both the short-term and long-term costs and benefits.[119] However, studies have found

---

112 *See* Satter, *supra* note 46.

113 *See* Schwartz, *supra* note 55, at 2080.

114 *See id.*

115 *See* MALLOY, *supra* note 73, at 145; Melvin Aron Eisenberg, *The Limits of Cognition and the Limits of Contract*, 47 STAN. L. REV. 211, 213 (1995).

116 *See* Acquisti & Grossklags, *supra* note 110, at 16.

117 *See* Sunstein, *supra* note 84, at 1830, 1842.

118 *See id.* at 1842–52.

119 *See id.* at 1842–44.

that humans are impulsive and have difficulty accounting for the future.[120] Humans have a tendency to place more weight on the present than the future.[121] These judgment errors cause individuals to make choices with short-term benefits without considering the long-term costs, and vice-versa.[122] When faced with a privacy decision, individuals often accept whatever terms a collector proposes in exchange for personal information.[123] Individuals will make the same errors when confronted with a decision about providing biometrics. An individual will be more concerned with gaining access to a service than with considering the consequences to her identity if the biometric system is compromised in the future.

Studies have also shown that humans are only able to pay attention to a limited number of things, and items that are inconspicuous often get ignored.[124] Even if the hidden items—"shrouded attributes"—are important, humans are prone to ignore them, sometimes to their detriment.[125] Even if they do not ignore shrouded costs or benefits, humans may undervalue them or fail to recognize them until the future.[126] These human errors are highlighted in privacy decision making, where the costs and benefits are complex and frequently bundled with other items.[127] Individuals have difficulty processing all the relevant information and instead rely on simplified models.[128] The same occurs when biometrics are part of a transaction. A person may not see or consider factors such as if the characteristic is stored or disclosed. Using limited information, particularly excluding such important items, leads an individual to suboptimal decisions regarding her biometrics.

---

120 *See* Acquisti & Grossklags, *supra* note 110, at 27–28; Sunstein, *supra* note 84, at 1830.

121 *See* Acquisti & Grossklags, *supra* note 110, at 27.

122 *See* Sunstein, *supra* note 84, at 1842–44.

123 *See* Schwartz, *supra* note 55, at 2081.

124 *See* Sunstein, *supra* note 84, at 1846 (describing the gorilla experiment).

125 *See id.* at 1846–47.

126 *See id.* at 1848.

127 *See* Acquisti & Grossklags, *supra* note 110, at 17.

128 *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1887 (2013); Acquisti & Grossklags, *supra* note 110, at 26.

Another cognitive mistake is that humans are unrealistically optimistic.[129] Humans tend to downplay bad news, preventing them from taking precautions against serious harms.[130] An individual faced with the choice about providing her biometric may weigh the promised security against potential disclosures. Collectors may also be faced with the same situation, where they must choose whether to implement a biometric system. A company may mispredict the dangers involved with utilizing the technology.

Finally, evidence suggests that humans are poor risk assessors.[131] Decisions are often based on emotions and heuristics.[132] An individual will consider immediately available knowledge without further investigation.[133] This practice leads to miscalculating the probability of certain outcomes, either overestimating or underestimating the risk.[134] An individual faced with a choice about biometrics will not likely have available examples or knowledge to rely upon. As an emerging consumer technology, most individuals are unfamiliar with how the technology works or the dangers it poses.

B. Personhood and Market-Inalienability

Opposite to economic theory is Margaret Radin's personality theory, which focuses on the importance of identity and preserving the integrity and continuity of the self.[135] She views entitlements, rights, or attributes on a continuum from fungible to personal, based on how connected it is to personhood; the more personal, the more the entitlement should be protected.[136] When something is significant to personhood, loss of that thing will cause pain that cannot be relieved even by replacing the item.[137] This is because personhood depends on the expectation of continuity, where an

---

129 *See* Sunstein, *supra* note 84, at 1849.
130 *See id.* at 1849–50.
131 *See id.* at 1852.
132 *See id.* at 1851–52; Solove, *supra* note 128, at 1887.
133 *See* Sunstein, *supra* note 84, at 1851–52.
134 *See id.*
135 *See* MARGARET JANE RADIN, CONTESTED COMMODITIES 55 (1996).
136 *See* Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957, 986, 1014–15 (1982).
137 *See id.* at 959.

individual anticipates something to be part of her future self.[138] Radin notes that bodies are literal components of personhood.[139] She believes that the concept of "universal commodification"—that personal attributes are monetizable and detachable from the person—undermines personal identity; instead, substantive characteristics of personality must be inalienable.[140]

Inalienability is the notion that something cannot be separated from its holder.[141] The term is often used for entitlement, rights, or attributes that may not be forfeited, cancelled, waived, relinquished, given, sold, or transferred.[142] The category of inalienability at issue here is salability—the extent to which an entitlement cannot be transferred between buyers and sellers.[143] Radin argues that some things should be outside the market but not necessarily outside of social interactions, a category she calls "market-inalienability."[144]

Market-inalienability supposes that commodification is a continuum. Something does not have to be completely inside or outside the market, but rather it may only be nonsalable in certain contexts.[145] For example, human organs cannot be sold on the free market but may be transferred by gift. Unlike inalienabilities that cannot be separated from the person—social security benefits or the right to vote—market-inalienabilities are not inseparable from the person, only that the market is not the cause of separation.[146]

Under the concept of market-inalienability, Radin believes things have commodified and noncommodified versions, and argues that it may be necessary to prohibit the commodified version of certain things.[147] Prohibition should be used when the market harms personhood, such as allowing individuals to freely commodi-

---

138 *See id.* at 968.
139 *See id.* at 966.
140 *See* RADIN, *supra* note 135, at 36, 56.
141 *See id.* at 16–17.
142 *See id.* at 17.
143 *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972).
144 *See* RADIN, *supra* note 135, at 18.
145 *See id.* at 20.
146 *See id.* at 19.
147 *See id.* at 94–95.

fy themselves; separately, it may be necessary to protect the non-commodified version of a good because it fosters personhood.[148] Radin uses "love, friendship, and sexuality" as examples: commodification of these goods will degrade the person and noncommodification is morally necessary for society.[149] She claims that the appropriate mechanism to simultaneously protect and foster personhood is regulation.[150]

Under Radin's personality theory, biometrics are personal. The pain of losing one's identity, through a biometric system or otherwise, would be quite severe. Human attributes that allow others to recognize each other are closely aligned with a person's being, and individuals identify themselves through these attributes. As such, they are essential to personhood and warrant protection. However, that is not to say biometrics are so central to a person's being that they cannot be separated from that person. That notion would render biometrics inalienable. Humans cannot be restricted from enjoying each others' characteristics, many of which are accessible and freely given away. Individuals interact with others every day, using their voice, showing their faces, and touching things around them. There is no way to prevent a transfer of that information. The only way to make biometrics completely inalienable would be to put all humans in isolation.

Therefore, Radin's concept of market-inalienability fits biometrics well. Just as with emotions, bodily integrity, and other social interactions, biometrics should be precluded from market transactions. Allowing a human attribute to be traded and monetized will degrade personhood. Applying Radin's theory that commodified and noncommodified versions can coexist, only the commodified version of biometrics should be prohibited. A noncommodified version of biometrics fosters personhood by promoting social interaction. As stated above, human attributes that make an individual recognizable are essential to daily life in society. Humans cannot function in society without the ability to share their identities with those around them. Therefore, a nonmonetized version, where biometrics may be given away, should be protected.

---

148 *See id.* at 94, 96.

149 *See id.* at 96.

150 *See id.* at 109 (discussing regulations on labor and housing).

Radin notes that regardless of whether a market is efficient, intervention is still justified where there is a commitment to protect things important to humanity.[151] Restrictions on commodification would take into account personhood and foster nonmonetized identities. Therefore, some form of oversight and intervention is justified in order to balance commodified and noncommodified biometrics.

III. AVAILABLE LEGAL TOOLS

Privacy is handled, or mishandled, in a number of ways around the world. As the Part II discussed, there is a need to govern biometrics in order to keep them from the market and prevent commodification. This Part considers the existing legal structures and how they apply to biometrics. First, there is an examination of self-regulation, which dominates privacy in the United States, and how the notice-and-consent structure fails to adequately protect privacy. Second is a review of current biometric legislation; specifically, the strategies utilized in the United States, European Union, and Canada. Finally, this Part considers choice architecture as a balance between autonomy and government regulation, and argues that a combination of disclosures, incentives, and light government regulation may lead individuals and industry to make informed and better decisions.

A. Self-Regulation

Privacy protection in the United States relies on self-regulation.[152] Privacy self-regulation is based on the Federal Trade Commission's Fair Information Practice Principles (FIPPs) of notice, choice, access, security, and enforcement.[153] The cornerstone to this structure is notice and consent, allowing many forms of collection, use, and disclosure to be permissible.[154] This model assumes that individuals are rational and make informed decisions;

---

151 *See id.* at 111.

152 *See* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 877 (2003).

153 *See* Solove, *supra* note 128, at 1882.

154 *See id.*

however, as shown in the discussion on market failure, that human construct is a fallacy.[155] Consent is deemed essential because it preserves an individual's autonomy.[156] However, individuals are often left with a binary choice: They must agree to provide personal information, or they will not receive the good or service. This often appears to be a choice to an individual, but in reality there is no negotiating.[157] Further, providing choices is not the same as protecting privacy.[158]

Notice is preferred over forms of government regulation because it is easy and cheap to administer.[159] A collector often provides notice through a privacy policy or terms of service, and an individual often has to affirmatively agree to the terms.[160] However, there are problems with these notices reaching individuals.[161] Even if an individual does receive a notice, studies show that individuals do not read or understand the policies or terms.[162] Further, particularly with social media or other accounts, individuals often do not know how to change privacy settings.[163]

The shortcomings of privacy self-regulation will have a detrimental impact on biometric decisions. If biometrics are treated like all other personal information, their collection and use will be governed by consent and privacy policies. Further, as more institutions implement biometric systems, individuals will be left with fewer choices as to whether they must enroll their characteristics. The burden is on the individual to make decisions that could have serious consequences. Notice and choice do not protect individuals from their bad decisions, nor do they incentivize collectors to avoid biometrics or adequately protect any collected characteristics.

---

155 *See supra* Part II.A.1–4.

156 *See* Solove, *supra* note 128, at 1892.

157 *See* Fred H. Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice*, 98 CALIF. L. REV. 1765, 1773 (2010).

158 *See id.*

159 *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1048 (2012).

160 *See* Solove, *supra* note 128, at 1898.

161 *See* Calo, *supra* note 159, at 1051.

162 *See* Solove, *supra* note 128, at 1885; Calo, *supra* note 159, at 1051 (describing how Chief Justice Roberts does not read privacy notices).

163 *See* Solove, *supra* note 128, at 1884.

B. Government Regulation

1. United States

Privacy laws in the United States are narrow, related to specific industries and based on who is collecting information rather than the nature of the information itself.[164] The broadest legislation is the Privacy Act of 1974, which governs the federal government's collection, use, and disclosure of personal information.[165] However, there are a number of exceptions and gaps that preclude biometrics from receiving protection.[166] In fact, many federal agencies have been granted the authority to collect, use, and store personal information, including biometrics.[167] Notably though, there is no federal legislation directly governing the collection and use of biometrics by the private sector, nor is there comprehensive privacy legislation governing the private sector in which biometrics could fit.

There is some oversight available from the Federal Trade Commission (FTC), which has taken on the role of enforcing privacy and data security.[168] The FTC's authority to regulate privacy and data security arises out of Section 5 of the FTC Act, which allows the agency to regulate "unfair or deceptive acts or practices in or affecting commerce."[169] However, enforcement is only based on written privacy policies provided by companies. Furthermore, there are no regulations or oversight of the security standards that should be used in biometric systems.[170] As the technology becomes more pervasive, this lack of consistency will exacerbate the vulnerabilities of biometric systems.[171] Individuals will enroll characteristics in weak systems; because the same characteristic may be enrolled in more than one system, when the weak system is compromised, it will compromise the other biometrics systems as well.

---

164 *See* Reidenberg, *supra* note 152, at 877.

165 *See* Donohue, *supra* note 6, at 468.

166 *See id.* at 468–76.

167 *See id.* at 466–67.

168 *See* Daniel J. Solove, *One of the Most Important Data Security Cases Was Just Decided:* FTC v. Wyndham, TEACHPRIVACY (Apr. 15, 2014), https://www.teachprivacy.com/one-important-data-security-cases-just-decided-ftc-v-wyndham/.

169 *See* 15 U.S.C. § 45(a)(2) (2012).

170 *See* Hu, *supra* note 6, at 1536.

171 *See supra* Part I.A.

On the local level, many states include biometrics within their definition of sensitive data or personal information under fraud, identity theft, or breach notification statutes.[172] However, these laws are reactive—they address the information after it has been breached or misused. A few states have passed very specific restrictions on the collection and use of biometrics. For example, four states restrict collecting biometrics of children at school; however, with the exception of Florida, the laws still allow collection with a parent's written consent.[173] Another example is that New York generally prohibits fingerprinting as a condition of employment, but there are a number of exceptions for employees of state, municipal, and certain private industries.[174]

Two states, Illinois and Texas, have passed laws that specifically apply to the private sector's collection and use of biometrics.[175] Both state laws require an individual to be notified and consent to the collection, and restrict the collector's ability to sell, lease, trade, or disclose the biometric without the individual's further consent.[176] Illinois also requires that a collector create a written policy with retention guidelines whereby the biometric is destroyed once the initial purpose has been satisfied or within three years of the individual's last contact with the collector.[177] Texas does not explicitly state any retention requirements beyond storage with reasonable care.[178] Finally, both laws provide remedies for violations of the statute: Texas imposes a civil penalty, while Illinois creates a private right of action for affected individuals.[179]

It is unclear how effective either the Illinois or Texas laws will be because many companies operate across state and national borders. It is also unlikely that many other states or the federal gov-

---

[172] *See generally* ANDREW B. SERWIN, INFORMATION SECURITY & PRIVACY: A GUIDE TO FEDERAL AND STATE LAW AND COMPLIANCE § 22 (2014) (describing state identity theft laws).

[173] *See* ARIZ. REV. STAT. ANN. § 15-109 (2014); FLA. STAT. § 1002.222 (2014); LA. REV. STAT. ANN. § 17:100.8 (2014); 105 ILL. COMP. STAT. 5/34-18.34 (2014).

[174] *See* N.Y. LAB. LAW § 201-a (McKinney 2014).

[175] *See* 740 ILL. COMP. STAT. 14/1–99 (2014); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2013).

[176] *See* 740 ILL. COMP. STAT. 14/15(b)–(d); BUS. & COM. §§ 503.001(b)–(c)(1).

[177] *See* 740 ILL. COMP. STAT. 14/15(a).

[178] *See* BUS. & COM. § 503.001(c)(2).

[179] *See id.* § 503.001(d); 740 ILL. COMP. STAT. 14/20.

ernment will pass similar laws. Ultimately, the inconsistencies and lack of regulation will do little to dissuade the private sector from upholding proper privacy or security practices with regard to biometrics.

2. European Union

European Union Directive 95/46/EC,[180] which governs the processing of personal data, also applies to biometrics. In a subsequent opinion, the Article 29 Data Protection Working Party stated that the use of biometrics indicates processing personal data.[181] Therefore, biometrics "may only be processed if there is a legal basis and the processing is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."[182] The opinion applies the principles of purpose, proportionality, necessity, and minimization to biometrics: it is a prerequisite to clearly define the purpose for which the biometrics will be collected and used; there must be consideration as to whether a biometric system is necessary and if the invasion of privacy is balanced by the anticipated benefit from using biometrics—the opinion states that convenience is not a significant benefit to warrant the loss of privacy; only the information that is required for the specified purpose should be collected; and the information may only be stored for as long as it is necessary for the stated purpose.[183]

The opinion also requires that biometrics be used legitimately. An individual whose biometric is collected and used must be aware that her biometric is being processed and she must provide freely given, specific and revocable consent.[184] Further, the opinion seemingly precludes many private sector uses of biometrics by noting that:

> "Personal data are not goods that can be asked for in exchange of a service, therefore contracts that fo-

---

[180] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281).

[181] *See* WP 193, *supra* note 5, at 7.

[182] *Id.*

[183] *See id.* at 7–10.

[184] *See id.* at 10–12, 14.

> resee that or contracts that offer a service only under the condition that someone consents to the processing of his biometric data for another service cannot serve as legal basis for that processing."[185]

The opinion notes that the security of biometric systems is a concern because the characteristics are irrevocable and that the risk of theft increases with the more entities using biometrics.[186] Therefore, the opinion includes a number of technical recommendations, including that biometrics should be stored as templates instead of storing a sample or image of the actual characteristic; centralized databases should be avoided and local storage in cards, tokens, or other devices should be utilized instead; biometric data should be encrypted; and the data should be automatically deleted when no longer necessary.[187]

EU member states may pass local laws that provide more protection than the Directive.[188] Germany's Passport Act prohibits a federal database of passport biometrics, and requires that passports may not be used by other agencies for automated retrieval of personal data.[189] This provides that biometrics may only be stored on the passport chip and may only be used for border crossing security purposes.[190] There is also pending law in France to restrict use of biometrics.[191] The proposed law would ensure that biometrics are only used for strict security purposes, such as the safety of individuals, property or information that could cause serious harm.[192] Further, biometrics would only be allowed if the risks to security are

---

185 *Id.* at 12.

186 *See id.* at 28.

187 *See id.* at 31–33.

188 *See* Marc Rotenberg & David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, 36 HARV. J.L. & PUB. POL'Y 605, 618 (2013) (stating that member state implementation of the directive must meet only "minimum requirements").

189 *See* Passgesetz [PassG] [Passport Act], Apr. 19, 1986, BGBL. I at 537, last amended by Gesetz [G], July 25, 2013, BGBL. I at 2749, art. 8, *available at* http://www.gesetze-im-internet.de/englisch_pa_g/index.html.

190 *See id.*

191 *See French Senate Proposes New Laws to Limit Use of Biometrics*, PLANET BIOMETRICS (May 1, 2014), http://www.planetbiometrics.com/article-details/i/1967/.

192 *See id.*

high and if there is proportionality between the nature of the thing being protected and the biometric technology used.[193]

3. Canada

Canada's approach to privacy regulation falls in between the extremes of the United States and the European Union.[194] For many years, Canadian privacy protection was directed at government entities.[195] However, Canadian policy has shifted towards stricter regulation. In 2000, Canada passed the Personal Information Protection and Electronic Documents Act (PIPEDA) which protected personal information across all private industries.[196] Quebec, and other provinces, subsequently passed more stringent privacy laws.[197]

Quebec law includes rigid limitations on the collection, use, and storage of biometrics. Under this law, biometrics may not be used for identification or verification without express consent of the individual.[198] The law stipulates that the characteristics collected must be ones that require the individual's knowledge and that the number of characteristics is the minimum and necessary number for the purpose.[199] Further, the biometric data must be destroyed once the initially stated purpose has been met or no longer exists.[200]

The Quebec law also imposes requirements and restrictions on the use of databases.[201] Prior to creation, a biometric database must be disclosed to the Commission d'accès à l'information, and any

---

193 *See id.*

194 *See* Jennifer McClennan & Vadim Schick, *"O, Privacy" Canada's Importance in the Development of the International Data Privacy Regime*, 38 GEO. J. INT'L L. 669, 674 (2007).

195 *See id.* at 674–75.

196 *See* Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.), *available at* http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf; McClennan & Schick, *supra* note 194, at 671.

197 *See* McClennan & Schick, *supra* note 194, at 686 (discussing how Quebec and other provinces have privacy laws "substantially similar" to PIPEDA).

198 *See* An Act to Establish a Legal Framework for Information Technology, C.Q.L.R., c. C-1.1, c. 32, s. 44, *available at* http://canlii.ca/t/lgvb.

199 *See id.*

200 *See id.*

201 *See id.* c. C-1.1, c. 32, s. 45.

existing databases must be disclosed as well.[202] The Commission reserves the right to govern how a biometric database may be established and used, as well as how the stored charactertics are maintained and destroyed.[203] The Commission also reserves the right to prohibit any databases and order that existing databases be destroyed.[204]

As this section on government regulation demonstrated, the level of regulation over privacy and biometrics varies among jurisdictions. The European and Canadian approaches are comprehensive and strict; however, the United States is unlikely to pass any similar laws. On the other hand, the United States has no adequate system in place to govern biometrics. As the following section will show, there is an intermediary approach that may be the most feasible solution for biometrics in the United States.

C. Choice Architecture

If self-regulation and government regulation are polar opposites, then choice architecture sits in the middle. Scholars Cass Sunstein and Richard Thaler call this "libertarian paternalism."[205] This theory is based on behavioral market failures, which exist in the privacy context.[206] Paternalism is favored, but not necessarily in the form of strict government mandates.[207] Instead, the response may be through disclosures, warnings, and default rules.[208] These structures preserve autonomy but lead an individual towards making the correct choices.[209]

Choices are often determined by how they are framed. One example is if an individual is considering a medical operation, she will be more agreeable if told the success rate than the mortality rate.[210]

---

202 *See id.*
203 *See id.*
204 *See id.*
205 *See* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 5 (2008).
206 *See* Sunstein, *supra* note 84, at 1834–35; *supra* Part II.A.1–4.
207 *See* Sunstein, *supra* note 84, at 1835.
208 *See id.*
209 *See id.*
210 *See* CASS R. SUNSTEIN, WHY NUDGE?: THE POLITICS OF LIBERTARIAN PATERNALISM 29 (2014).

This loss aversion explains why individuals are affected more when faced with a tax than a bonus.[211] Similarly, they are more sensitive to price terms than nonprice terms.[212] An example of this framework is cigarettes.[213] Smokers know cigarettes are unhealthy, but are more discouraged by the increasing tax than the health risks.[214] Smokers who are heavily taxed may eventually quit, a decision that makes them better off.[215]

One method of employing choice architecture is through default rules. Humans are propelled by inertia, and most end up choosing the default rules or settings.[216] Another means is through what Sunstein and Thaler call "RECAP" or record, evaluate, and compare alternative prices. Government regulation would govern disclosure, not prices, to better inform an individual's decision making.[217] Yet another means to lead individuals towards making the right choice is through incentives. Choice architects consider how to get the right incentives to the right individual in order to influence decisions.[218] Loss aversion seems like a powerful incentive on individuals, but it could be applied to companies as well. If acquiring consent is cumbersome and costly, a company will be discouraged from engaging in that particular collection and use.[219]

Choice architecture provides a set of tools that can be constructed in such a way to deter the use of biometrics. It may be the most realistic solution available to govern biometrics in the United States. As the following Part discusses, building a regime of defaults, disclosures, and incentives will allow both the private sector and individuals to choose how to manage privacy and security yet slow the commodification of biometrics.

---

211 *See id.*
212 *See* Solove, *supra* note 128, at 1898.
213 *See* SUNSTEIN, *supra* note 210, at 111.
214 *See id.*
215 *See id.*
216 *See* THALER & SUNSTEIN, *supra* note 205, at 83.
217 *See id.* at 93–94.
218 *See id.* at 97.
219 *See* Solove, *supra* note 128, at 1899.

IV. DISCOURAGING THE ADOPTION OF BIOMETRICS

Ideally, the best way to prevent the commodification of biometrics would be to prevent their use all together. Individuals place personal and nonmonetized value in their fingers, eyes, face, voice, and other attributes. The use of biometrics by the private sector, for a variety of purposes, monetizes the characteristics. The rapid growth of biometrics has led to the commodification of human characteristics and greater overall risks in using the technology. Considering how self-regulation fails to adequately protect personal privacy and government regulation is impractical in the United States, this Part argues that the best solution to protect biometrics is through choice architecture. A system of defaults, disclosures, and taxes will not completely prohibit the use of biometrics, but it will discourage companies and individuals from establishing and using such systems. The goal is to buy time by slowing the adoption of biometric technology in the hopes that more adequate protections and safeguards can be established. The following are a set of principles and tools, organized by phase of the biometric process, to guide the current transition towards biometrics.

A. Collection

Privacy is individualistic and varies between any two individuals. Therefore, it is critical to maintain autonomy and freedom of choice with biometric privacy. This will be accomplished through a strengthened model of notice and choice. First, there cannot be any collection without expressly informing an individual that her characteristic is being collected and for what purpose. Simply providing notice that voice samples are retained or images are stored is insufficient; the collector must warn that this information will be processed and used for recognition purposes. Furthermore, such notice must disclose the risks and vulnerabilities of using biometrics. The misconceptions of biometric accuracy and security must be dispelled. Liability for failing to adequately notify an individual will fall under the FTC's authority to regulate unfair or deceptive trade practices.

The next step is consent, which must be affirmative and specific to each biometric. The default should be to use means other than biometrics, requiring individuals to opt-in to the collection. To ef-

fectively construct an opt-in default, goods and services should not be conditioned upon providing biometrics. Opt-in permission forces an individual to consciously choose biometric collection. If an individual makes the choice to enroll in a biometric system, there should be sufficient and conspicuous warnings before the enrollment takes effect.

Collectors must not use biometrics unless other means are considered insufficient for the stated purpose, and only resort to using biometrics if absolutely necessary. If a biometric system does appear to be required, only the minimum amount of information should be collected. Further, taxation should be used as a means to incentivize individuals and companies. Taxing companies that collect and use biometrics would discourage the companies from implementing such systems. A tax would force companies to conduct a cost-benefit analysis to determine if the tradeoffs were economical, and ultimately weigh whether the supposed security from using biometric systems outweighs the tax. These tax costs would trickle down to individuals, whereby they are charged a fee or premium to enroll in biometric systems. Since humans are more concerned with prices than intangible concepts like privacy, this tax will discourage both companies and individuals from resorting to biometrics.

B. Use

Biometrics should not be used for security purposes, but instead be limited to value-add or innovation uses. These purposes are more consistent with society's current acceptance of biometrics, as something personal and nonmonetized. The goal is to promote a use of biometrics that enhances social interactions, without stifling scientific innovation. Furthermore, use of biometrics for security purposes makes the characteristics and security systems appealing to criminals. Since the technology is vulnerable, the more biometrics are used for security the more likely it is that the systems will be targeted and compromised. However, the movement towards biometrics for security seems to be inevitable.

Should security purposes be a necessary use of biometrics, all biometric systems should be used for multi-factor authentication with two or more characteristics being matched simultaneously.

This reduces the risk of certain types of attacks, such as spoofing, and ensures that even if one biometric has been compromised, hackers will have to expend a significant amount of resources in order to attack two or more characteristics. Finally, any collected biometric data should not be sold, traded, or disclosed. This includes sharing with other entities within the same industry. The value of the biometric will be diluted the more places it is used.

C. Storage and Access

Centralized storage of information increases the risk of disclosure and breaches. To the extent the characteristics can be stored locally instead of in a central database, the less risky it will be to the collector and individual. To this end, there should be a tax on biometric databases. There must be a system that incentivizes companies away from centrally storing biometrics. The tax will also force a company to evaluate if balkanized storage will be a sufficient, and ultimately less risky method of storing the information. However, regardless of whether the biometric is stored in a database or locally, the data must be properly encrypted to add a further layer of protection. As with notice, the FTC may impose liability for inadequate data security under its authority to regulate unfair and deceptive business practices.

Additionally, it is important that biometric systems allow individuals a right of access. Characteristics change over time, and the technology occasionally makes mistakes. An individual should have the ability to correct the template. Further, an individual should also have the ability to request that her biometric template be destroyed. For example, if an individual chooses to enroll in one bank's authentication system, but then chooses to bank elsewhere, her biometric should not remain in a different bank's system. Finally, the choice to enroll in a biometric system must be reversible. There have to be available alternatives that allow an individual to receive the same good or service without enrolling her biometrics.

CONCLUSION

With the help of technological advances and the private sector's interest, biometrics are rapidly invading daily life. Fingers are

more than parts of the body; they are they keys to an account. Faces and voices are no longer something only shared with individuals nearby, but tradable goods with value to companies. The rapid growth of biometrics is turning once nonmonetized attributes into something that can be traded and sold. This commodification in turn exposes the flaws of biometric technology, which will only become exacerbated as more systems are implemented. Worse yet, biometric systems have inherent security flaws, and hackers will always be knocking at the door. Proponents looking to utilize biometrics for security purposes are essentially handing identities to hackers and leaving individuals with irreplaceable identifiers.

Without comprehensive privacy legislation, we are on the brink of a biometric crisis. The private sector will continue to find new ways to use biometrics, and the security systems that rely on that data will become useless. Therefore, it is wise to be proactive and structure a system of principles and incentives to at least discourage reliance on biometrics. The proposed set of principles and tools in this Note will create hurdles in the race to adopt biometrics. Buying time to strengthen the technology and educate the public may be essential to protecting biometrics. Ultimately, individuals, companies, and the legal system must be better informed and prepared for when the technology fails.