The Standard for Biometric Data Protection

Fiona Q. Nguyen*

ABSTRACT

Everyone has heard of the trolley problem.[1] *You are the conductor of a train when you suddenly realize that this train cannot be stopped. As the conductor, you have two options: let the train continue on its current track and kill twenty criminals or pull the lever and cause the train to switch to a different track, killing only one doctor who might hold the cure for cancer. Which option would you choose?*[2]

Second scenario: a smart car malfunctions on the interstate highway and, at this moment, it must decide whether to aim for the barrier and kill its only occupant, or swerve to save the one occupant and kill twenty passengers on a nearby bus. What decision would this smart car make based on its algorithm to minimize harm?[3] *What decision would this smart car make if it were equipped with facial recognition technology that enabled it to identify not only its occupant, but also those passengers on the bus? And, what if upon identification, the smart car had real-time access to the public records and social media profiles of these individuals? The smart car would presumably use such information to assist it in its quick decision-making process. If the one occupant were a recovering drug addict and the twenty passengers a team of doctors en route to their conference to explain the*

* J.D. Candidate, 2018, University of Maryland Francis King Carey School of Law. Special thanks to Steven Hung Nguyen and Kelly Tuyen Mai for encouraging my curiosity, and to Danielle Keats Citron for providing comments.

[1] PHILIPPA FOOT, *The Problem of Abortion and the Doctrine of the Double Effect*, *in* VIRTUES AND VICES AND OTHER ESSAYS IN MORAL PHILOSOPHY 19 (1978).

[2] The problem presented in this Article is a combination of the original Trolley problem by Philippa Foot, and its adaptation to smart cars by the Massachusetts Institute of Technology, with current and foreseen capabilities of biometric data and facial recognition technologies.

[3] Moral Machine, MASS. INST. OF TECH., http://moralmachine.mit.edu.

cure for cancer, it's entirely plausible that the smart car would crash into the barrier for the good of mankind.

But what if that one occupant were you? It had taken you years to overcome your struggle with drug addiction, and you were now on your way to a job interview that could finally offer you a new start. You posted on your Facebook page about how excited you were for the interview, and surely the smart car took all of this into account—but none of it seems to override the ultimate judgment of the smart car algorithm assigned to you.

INTRODUCTION

Although this hypothetical may seem like a future envisioned in dystopian films, the vast collection of personal data that is currently accessible to the private sector makes it possible. The technology underlying this hypothetical is also already available, and the connected use of it with mass data is in the near future. While there is a role for ethics to play in the decisions being made, this Article focuses on the importance of standardizing the protection of collected data through biometrics.

Part I provides background information, such as the definition of biometric data and the current legal landscape for biometric data protection. Part II explores why congressional legislation establishing a national standard for biometric data protection is necessary. Part III explores the future of biometric data usage and why having a national standard is the next logical step. Part IV further explores how this national standard can be created through an examination of the uniform standard that went into effect in the European Union on May 25, 2018.[4] In conclusion, this Article argues for a national standard which serves as the floor for biometric data regulation but does not preempt related state legislative action.

[4] Commission Regulation 2016/679 of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) [hereinafter General Data Protection Regulation or GDRP].

I. BACKGROUND

A. What Is Biometric Data?

The definition of biometric data can vary depending on the context.[5] However, biometrics more generally refers to unique and "measurable human biological and behavioral characteristics that can be used for identification, or the automated methods of recognizing an individual based on those characteristics."[6] While statutory definitions differ, some common examples of these "biometric identifiers" include "retina or iris scans, fingerprints, voiceprints, and scans of hand or face geometry."[7] As such, biometric data is the "information derived from biometric identifiers."[8]

B. Why Regulate Biometric Data?

1. Characteristics of Biometric Data Necessitate Protection

The inherent characteristics of biometric data necessitate protection because they are derived from biometrics, and biometrics by their very nature are "unlike other unique identifiers."[9] Biometrics are "biologically unique to the individual" and, unlike other forms of sensitive information, these unique identifiers cannot be changed.[10] Thus, "once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[11] Moreover, the potential uses and abuses of biometric data are not fully known,[12] which is why it is important to protect this critical data at this current moment.

---

[5] Michael P. Daly et al., *Biometrics Litigation: An Evolving Landscape*, PRAC. L. LITIG., Apr.–May 2016, at 38, 39.

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] 740 ILL. COMP. STAT. ANN. 14/5(c) (2008).

[10] *Id.*

[11] *Id.*

[12] *Id.*

2. Biometric Data Protection is Critical for the Enjoyment of the Right to be Incognito

Biometric data must be protected because this information cannot be replaced, and the ability to be incognito is a basic right. In their seminal law review article published in 1890, *The Right to Privacy*, Samuel D. Warren and Louis D. Brandeis advocated for a right to privacy because they believed that an individual should have control over the publication of his or her own information, and that protection from public invasion is necessary for the pursuit of happiness.[13] Warren and Brandeis compared the common law rights to the "right to be let alone" and "inviolate personality" principles.[14] While Warren and Brandeis had public officials in mind, in today's society, the privacy protection they advocated for is undoubtedly even more relevant to the general public.

In a society of social media, the right to be incognito, or to be unknown by others,[15] echoes the principles Warren and Brandeis addressed in their article. However, Warren and Brandeis carved out exceptions where publication would be appropriate even though it intrudes on one's privacy. An important consideration discussed in their article is the invasiveness of such intrusion on the individual's privacy. This invasiveness consideration is still relevant today. The proposition, echoed in the concurring opinions in *United States v. Jones*,[16] is that even though one might not have a reasonable expectation of privacy in segments of public information, the individual has a reasonable expectation of privacy in the aggregation of that data.[17]

The mosaic theory illustrates why the aggregated product of our

---

[13] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890).

[14] *Id.*

[15] *Incognito*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/incognito (last visited Oct. 28, 2018).

[16] 565 U.S. 400 (2012) (Sotomayor, J., concurring); *see id.* (Alito, J., concurring).

[17] *See, e.g.*, Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 270 (2013).

personal public information is troubling.[18] Although a stranger having one segment of information that is already publicly available does not bother us, the aggregation of those segments can together form a mosaic, revealing intimate details about us that the individual segments by themselves do not reveal.[19] The aggregated product weaves information from different facets of our lives and the different personas we portray to the various people in our lives. This aggregation can reveal our insecurities and expose revelations about us that we may not even realize about ourselves.[20] Danielle Citron suggests that "[l]imiting the scope of information dossiers does little to address [this] concern[]."[21] Thus, biometric data must be protected at the beginning stages. These dossiers with intimate data that can intrude on our right to privacy can easily be linked to our unique identifiers and follow us for an eternity if we do not have control over the collection, aggregation, use, and retention of our biometric data.

With today's technology and future technology, the right to be incognito will be violated if biometric data is not protected. The collection, aggregation, use, and retention of information can formulate a digital rap sheet that can be traced back to an individual. Both the government and the private sector use of fusion centers[22] take an extra-unwelcomed step into our lives. Fusion centers use data-mining tools to collect, aggregate, and share our personal data from public and "private-sector databases, the Internet, and public and private video cameras."[23] Fusion centers also have access to "dossiers on hundreds of millions of individuals" and some even "gather biometric data and utilize facial-recognition software."[24] With emerging technology that allows fusion centers to gather more personal information about us, including storage and examination of our online activities and

---

[18] David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381 (2013).

[19] *Id.* at 388.

[20] *Id.* at 398.

[21] Citron & Gray, *supra* note 17, at 271.

[22] *Id.* at 270.

[23] *Id.* at 264.

[24] *Id.*

communications,[25] it becomes increasingly difficult to be anonymous in today's society. Not only does the overwhelming amount of personal information compiled about us expose us to strangers for differing uses, this information allows strangers to know more about us than we are comfortable with sharing with close family members.[26] The level of intrusiveness of the collection, aggregation, and retention of personal data is highly troubling. Strangers with our data have the potential to "reveal, predict, and manipulate instinctual behavioral patterns of which we are not even aware."[27]

C. Current Biometric Data Laws in the United States

Currently, there are no federal laws that protect consumers' biometric data.[28] Although the Privacy Act[29] protects information privacy against government actors, there is no such protection in the private sector.[30] Moreover, the sheer lack of federal regulation of biometric data allows the government to bypass some requirements of the Privacy Act with the help of fusion centers and the unregulated private sector. While the Federal Trade Commission educates private companies on best practices and binds them through decrees, the best practices are suggestions and not law.[31] Despite the many current uses of biometric data in the United States and the many to come in the future, only Illinois and Texas have successfully passed laws to protect biometric data.[32]

The Illinois Biometric Information Privacy Act (BIPA),[33] passed in 2008, aims to protect biometric data since its use "is growing in the business and security screening sectors and appears to promise

[25] *Id.* at 265.

[26] *Id.*

[27] *Id.*

[28] *See* Daly, *supra* note 5, at 41.

[29] Privacy Act of 1974, Pub. L. 93–579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a (2018)).

[30] *See* Daly, *supra* note 5.

[31] *Id.*

[32] *Id.* at 41.

[33] 740 ILL. COMP. STAT. 14/1–14/99 (2008).

streamlined financial transactions and security screenings."[34] The General Assembly also saw the need for biometric data protection because the "full ramifications of biometric technology are not fully known."[35] The Texas Capture or Use of Biometric Identifier Act (CUBI)[36] is similar to BIPA, but it does not create a private right of action for consumers.[37] Instead, CUBI prescribes a penalty of "not more than $25,000 for each violation."[38]

The newly enacted California Consumer Privacy Act (CCPA)[39] of 2018 provides many protections for consumer data, including biometric data. The CCPA was adopted on June 28, 2018, and there has already been many amendments to the bill to clarify its technical aspects.[40] The CCPA will not go into effect until January 1, 2020, but it will provide many protections similar to the European Union's General Data Protection Regulation.[41]

Other states that have pending legislation addressing biometric data include: Alaska, Connecticut, New Hampshire, and Washington.[42] However, as the next Section seeks to demonstrate, state-by-state legislation can prove to be problematic for the protection of an individual's biometric data when there are no existing national standards.

II. WHY A FEDERAL BIOMETRIC DATA LAW IS NECESSARY

A. Biometric Data Case Law Demonstrates the Need for a National Standard

The enactment of biometric data protection laws in Illinois and Texas ushered in plaintiffs demanding redress for unconsented

---

[34] *Id.* 14/5(a).
[35] *Id.* 14/5(f).
[36] TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).
[37] *See* 740 ILL. COMP. STAT. 14/20.
[38] TEX. BUS. & COM. CODE ANN. § 503.001(d).
[39] CAL. CIV. CODE § 1798.198(a) (2018).
[40] S.B. 1121, 2017–2018 Leg., Reg. Sess. (Cal. 2018).
[41] CAL. CIV. CODE § 1798.120(a); GDRP, *supra* note 4.
[42] Daly, *supra* note 5, at 42–43.

collection, use, and storage of their biometric data. But the defendants in these cases have raised similar defenses, and with some success,[43] demonstrating the problem with state-by-state legislation as a means for protecting biometric data in the age of rapid development.

1. *In re Facebook Biometric Information Privacy Litigation*

An ongoing case against Facebook, Inc. illustrates the difficulties of litigating against private companies under a state statute. In the class action, *In re Facebook Biometric Information Privacy Litigation*,[44] the plaintiffs sued under Illinois' Biometric Information Privacy Act (BIPA), alleging that Facebook unlawfully collected and stored biometric data derived from plaintiffs' faces to identify them in photographs for its "Tag Suggestions" program.[45] In response, Facebook argued that (1) Illinois law did not apply because of a choice-of-law provision in its users' agreement, and that, even if it did, (2) the statute does not apply to tag suggestions.[46]

To summarize, the defendant argued that because the plaintiffs agreed to the choice-of-law provision in their user agreement when they signed up for a Facebook account, California law governed. Thus, the plaintiffs did not have a cause of action against Facebook under California law.[47] Facebook's second argument was that, even if BIPA does provide plaintiffs with a cause of action for the collection and usage of their biometric data, Facebook's tag suggestions are not protected biometric data as defined by BIPA.[48] The court discussed each of these defenses at length, finding that (1) plaintiffs did agree to the choice-of-law provision but that the court would not apply California's law to this case, and that (2) for the purpose of a motion to dismiss, plaintiffs alleged sufficient facts to show that tag suggestions

---

[43] *See id.* at 43–45.

[44] 185 F. Supp. 3d 1155 (N.D. Cal. 2016) [hereinafter *In re Facebook*].

[45] *Id.* at 1158–59.

[46] *Id.* at 1159.

[47] *Id.* at 1169–70.

[48] *Id.* at 1159.

may be protected under BIPA.[49] However, because this was a ruling on a motion to dismiss, the court noted that "[a]s the facts develop, it may be that 'scan' and 'photograph' with respect to Facebook's practices take on technological dimensions that might affect the BIPA claims."[50]

2. *Rivera v. Google Inc.*

In *Rivera v. Google Inc.*,[51] the plaintiffs brought suit against Google, alleging violations of BIPA for its unconsented use of similar face-scanning technology. Google raised issues of statutory scope, personal jurisdiction, and constitutional concerns.[52] Google offered three arguments: (1) the plaintiffs' complaints were about "Google's use of their *photographs*, and the Illinois [BIPA] does not cover photographs or information derived from photographs;" (2) "even if what Google is doing would run afoul of [BIPA] if done in Illinois," Google did not do anything in Illinois so the law cannot apply; and (3) "if [BIPA] does purport to cover what Google did outside of Illinois, then the state statute actually conflicts with the federal Constitution's Dormant Commerce Clause."[53] While the court denied Google's motion to dismiss, it also explained that BIPA "was not intended to and does not have extraterritorial application," and that more facts were needed for the court to see how "Google's specific transactions fit into the current legal landscape on Internet-based Commerce Clause violations."[54]

3. *Palomino v. Facebook, Inc.*

Palomino v. Facebook, Inc.[55] further demonstrates why a national standard for biometric data protection is necessary. Instead of suing under Illinois' BIPA, the plaintiffs sued under New Jersey's

[49] *Id.* at 1167–71.
[50] *Id.* at 1172.
[51] 238 F. Supp. 3d 1088 (N.D. Ill. 2017).
[52] *Id.*
[53] *Id.* at 1092.
[54] *Id.* at 1104.
[55] No. 3:16-CV-04230-HSG, 2017 WL 76901 (N.D. Cal. Jan. 9, 2017).

Truth-in-Consumer Contract, Warranty, and Notice Act.[56] While Facebook's arguments in this case were similar to those that it raised to no avail in *In re Facebook*, the court granted their motion and dismissed the plaintiffs' case with prejudice.[57] The court explained that California's choice-of-law governed the dispute, and because the New Jersey and California laws aimed for the same end, California law governed.[58] Thus, if New Jersey had a biometric data protection law like BIPA, then plaintiffs could sue under that law and the choice-of-law analysis would favor plaintiffs.

4. *Monroy v. Shutterfly, Inc.*

In *Monroy v. Shutterfly, Inc.*,[59] the plaintiff brought suit under BIPA and the court denied defendant Shutterfly's motion to dismiss.[60] In its ruling, the court held that: (1) BIPA applies to the type of data Shutterfly obtained through facial recognition technology; (2) BIPA did not need to have extraterritorial reach, nor be applied in a manner that violated the Dormant Commerce Clause; and (3) that the plaintiff sufficiently alleged he suffered actual damages.[61] Shutterfly raised some of the same arguments as Facebook did in *Palomino*. However, because the plaintiff in this case had a cause of action under BIPA, the litigation was allowed to proceed.

5. Other Biometric Data Cases

Other cases brought by plaintiffs under BIPA have been removed from state court to federal court, or defendants have at least

[56] *Id.* at *1.
[57] *Id.* at *2, *5.
[58] *Id.* at *3–4.
[59] No. 1:16-CV-10984, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017).
[60] *Id.* at *10.
[61] *Id.* at *5–6, *8.

tried to do so.[62] In *Smith v. Pineapple Hospitality Co.*,[63] the plaintiff sued under BIPA for its employer's failure to notify her and coworkers regarding the collection and storage of their fingerprints.[64] The explosion of cases after the enactment of BIPA shows that Americans are concerned about the collection, aggregation, use, and retention of their biometric data. While different defendants raise similar issues, the varying facts of these cases demonstrate the need not just for biometric data protection laws, but a federal standard.

B. The Problem with State-by-State Legislation

State-by-state legislation for biometric data protection encounters three main problems: speed, variance, and confusion. State-by-state legislation is often too slow to combat the speed at which biometric data is collected and processed. Also, its varying definitions may protect consumers in certain states, but harm consumers in other states with weaker or no protection laws. A company can simply collect information from residents of the states with the more lenient protection laws. In the cases mentioned, defendants have moved to dismiss on the basis of a choice-of-law provision. This will likely continue to happen if some states legislate and others do not. This will also happen if some states implement stricter standards than others. As a result, states that are slower to legislate will be vulnerable to unprotected biometric data processing. Moreover, for companies that have consumers across multiple states, compliance can become confusing and burdensome. The argument is not that they cannot comply with state-by-state legislation, but that compliance would be more likely if there was one clear national minimum standard for them to adhere to and for the courts to enforce.

Also, judicial economy is wasted when defendants in biometric data suits argue the same defenses, despite their defeat in certain states simply because the state laws differ. The often-heard arguments are:

---

[62] Hannah Meisel, *Hotel Co. Wants Biometric Class Action Moved to Fed. Court*, LAW360 (Nov. 9, 2017, 9:44 PM), http://www.law360.com/articles/984083/hotel-co-wants-biometric-class-action-moved-to-fed-court.

[63] No. 1:17-CV-08106 (N.D. Ill. filed Nov. 9, 2017).

[64] Meisel, *supra* note 62.

(1) statutory scope, (2) personal jurisdiction, (3) choice of law, and (4) constitutional and statutory standing.[65] It would be the best use of judicial economy to have one clear standard which would render most jurisdictional and choice of law arguments moot, and better focus resources to clarifying statutory scope and constitutional concerns.

III. THE NEXT STEP: A NATIONWIDE STANDARD

A. Biometric Data Uses Are Numerous and Growing

Biometric data usage can be separated into three categories: (1) to protect us, (2) to improve our lives, and (3) to classify us. Biometric data can also offer many benefits for our society, yet when considering the different reasons for its collection and usage, the results can be concerning.

1. Biometric Data Used to Protect Us

Biometric data have been used to protect us both from domestic and foreign threats. Programs like FAST, Secure Flight (No-Fly List), Terrorist Watch List and Terrorist Identities Datamart Environment (TIDE) database, Automated Targeting System (ATS), Adversary Behavior Acquisition, Collection, Understanding, and Summarization (ABACUS), Clear Heart, and Drone "Signature Strikes" are utilized in counterterrorism and national security efforts. As of today,

> vetting and screening protocols often begin with biometric identification—for example, the digital collection and screening of scanned fingerprints through federal and state biometric databases in the United States and international biometric databases, such as those operated by ICPO-INTERPOL (Interpol). Biometric data currently collected by DHS include scanned fingerprints and irises, digital photos for facial recognition technology, and DNA.
>
> Consequently, implementation of extreme vetting protocols will likely include proposals for a tamper-resistant and fraud-proof biometric electronic identity card, such as a biometric ePassport. The Trump administration's Executive Orders, for example, specifically mandate "Expedited Completion of the Biometric Entry-Exit

[65] Daly, *supra* note 5, at 43–45.

> Tracking System" by DHS. As part of new vetting protocols, DHS also seeks social media identification data and plans to seek social media user credentials, such as passwords to Facebook accounts of refugees and visa applicants. Newly developed "big data" cybersurveillance tools fuse biometric data with biographic data and internet and social media profiling to assess risk.[66]

Such uses and developments in security technology may make us feel safer, and even give us the comfort that the government is watching out for and protecting us. But this comforting feeling only lasts as long as we perceive that the government is watching others for us, and not that the government is watching us for any possible future needs.

2. Biometric Data Used to Improve Our Lives

From finance to social media to security access, the average person has many passwords to remember, and biometric data-enabled access helps to speed up the process. Proponents of biometric data access argue that biometric data also make accounts more secure because biometrics are unique identifiers, and at this current moment, they are not easily replicated.[67] Other proponents of embedding biometric data into our daily lives argue for the efficiency and attractiveness of having items that can be accessed and commanded with biometric data.[68] Some examples of biometric data uses to improve our lives include financial account access and payments with facial recognition;[69] detecting medical concerns;[70] and facial

---

[66] Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633, 640–41 (2017) (citations omitted).

[67] *See, e.g.*, 740 ILL. COMP. STAT. 14/5(a).

[68] *See, e.g.*, Chris Burt, *Yamaha Demonstrates MOTORiD with Facial and Gesture Recognition*, BIOMETRICUPDATE.COM (Nov. 14, 2017), http://www.biometricupdate.com/201711/yamaha-demonstrates-motorid-with-facial-and-gesture-recognition.

[69] *See, e.g.*, Chris Burt, *Facebook Files Patent for Facial Recognition for Physical Payments*, BIOMETRICUPDATE.COM (Nov. 13, 2017), http://www.biometricupdate.com/ 201711/facebook-files-patent-for-facial-recognition-for-physical-payments.

[70] *See, e.g.*, Bruce Brown, *AI Converts Biometric Data to Actionable Insights*,

recognition to unlock mobile phones.[71] Regardless of whether biometric data lives up to these claims, its use is becoming ubiquitous in our lives. The market of biometrics is expanding, and it is profitable. Market Research Engine's recent research report forecasts that the global healthcare biometrics market alone will exceed more than $2.8 billion by 2022.[72] More related to the hypothetical at the beginning of this paper, Goode Intelligence forecasts that the biometric market for connected cars alone will be just under $1 billion by 2023.[73] With a large market for this sensitive data, biometric data needs to be regulated before it is too late to protect consumers' rights.

3. Biometric Data Used to Classify Us

The more concerning use of biometric data is when it is used to classify us. The programs in which individuals in the population are classified are called identity inference systems.[74] The systems classify us through "'[p]robabilistic algorithms th[at] determine the likelihood of adversarial intent' or conduct other threat risk assessments, including simple aggregation of data."[75] This use of biometric data, combined with the vast personal data already publicly available about us, reveals the fact that the hypothetical from the beginning of this Article is not so far off in the distant future.

HEALTH TECH INSIDER (July 26, 2017), http://healthtechinsider.com/2017/07/26/ai-converts-biometric-data-actionable-insights.

[71] *See, e.g.*, Natasha Lomas, *iPhone X's Face ID Raises Security and Privacy Questions*, TECHCRUNCH (Sept. 13, 2017), https://techcrunch.com/2017/09/13/iphone-xs-face-id-raises-security-and-privacy-questions.

[72] Justin Lee, *Global Healthcare Biometrics Market to Surpass $2.8B by 2022*, BIOMETRICUPDATE.COM (July 20, 2017), http://www.biometricupdate.com/201707/global-healthcare-biometrics-market-to-surpass-2-8b-by-2022.

[73] ALAN GOODE, GOODE INTELLIGENCE, BIOMETRICS FOR THE CONNECTED CAR – AUTOMOTIVE BIOMETRICS ANALYSIS & FORECASTS 2018-23, (2017), http://www.goodeintelligence.com/report/biometrics-for-the-connected-car-automotive-biometrics-market-analysis-forecasts-2018-2023.

[74] Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475, 1491 (2013).

[75] *Id.* at 1492 (quoting Noah Shactman, *Army Tracking Plan: Drones That Never Forget a Face*, WIRED (Sept. 28, 2011, 6:30 AM), http://www.wired.com/2011/09/drones-never-forget-a-face).

B. The Intersection of Artificial Intelligence and Biometric Data

The hypothetical outlined at the beginning of this Article involves the intersection of artificial intelligence and biometric data processing, which is currently happening. An example of this is Alibaba's use of artificial intelligence and facial recognition technology to allow customers to pay without a cashier.[76] Artificial intelligence makes biometric data processing better.[77] A perfect match is not the goal in biometric data because it can be a result of fraud.[78] With the added power of artificial intelligence, security access using biometric data will operate more smoothly and be able to detect fraud more easily.[79] The fact that the integration of these two technologies has not yet enveloped our lives provides us with some comfort that the hypothetical's population categorizing and autonomous decision-making based on those categories is far from our present concerns. However, it should be noted that "the integration of AI with biometric technology is observed for mass surveillance and remote authentication in the public and commercial sector respectively."[80] Also, the various possibilities for biometric identifiers such as brainwaves, odor, heart signals, and ear force fields calls for the intersection with artificial intelligence.[81] This intersection has already begun and will continue

---

[76] Justin Lee, *Alibaba Demonstrates Face Recognition System at Cashier-Less Concept Café*, BIOMETRICUPDATE.COM (July 17, 2017), http://www.biometricupdate.com/201707/alibaba-demonstrates-face-recognition-system-at-cashier-less-concept-cafe.

[77] Kevin Alan Tussy, *Is AI the Missing Link in Biometric Security?*, TECHONOMY (Aug. 14, 2017, 9:01 PM), http://techonomy.com/2017/08/ai-missing-link-biometric-security.

[78] *Id.*

[79] *Id.*

[80] Perspective, *The Integration of Biometrics and Artificial Intelligence Promises Improved Security*, FROST & SULLIVAN (July 17, 2017), http://ww2.frost.com/frost-perspectives/integration-biometrics-and-artificial-intelligence-promises-improved-security.

[81] Cas Proffitt, *The Future of Biometrics with Artificial Intelligence*, DISRUPTOR DAILY (Aug. 9, 2017), http://www.disruptordaily.com/future-biometrics-artificial-intelligence.

into the future.[82] Margaret Hu noted in her article that biometric classification "can be based in part or in whole on artificial intelligence" and thus, that "in a big data world, classification and screening protocols can be combined, digitized, and automated."[83]

Once automated, although "big data regimes do not overtly seek to create subordinate social classes," this "may well be the result."[84] Not only will we be classified and our futures determined by the dossiers and automated decisions of artificial intelligence, "threat risk assessments will attempt to predict criminal or terroristic predisposition."[85] In *NASA v. Nelson*,[86] the court "pave[d] the way for the implementation of a biometric credentialing program and uniform biometric-based dataveillance program on a national scale."[87] Margaret Hu noted "how suitable character testing or morality testing can be built into modern vetting protocols in civilian background checks, as the facts of the case demonstrated that NASA employees and contractors were required to demonstrate trustworthiness and good character before receipt of the biometric identification card."[88] While legal scholars may view automated biometric categorizing to be unlikely, the Jim Crow system initially used "classification and markers of racial identity to determine who would be subject to laws that designated individual treatment, rights, and privileges based on those classifications."[89] Our biometric identifiers are being used to classify us, and it is very possible that such a system can be used to predict what each person is capable of, and if their potential is worth sacrificing for the good of the nation.

C. *Critiques to a Nationwide Standard*

Legal scholars may raise the concern that a weak national standard could be a problem, because states then are unable to protect

---

[82] *See* Lee, *supra* note 76.
[83] Hu, *supra* note 66, at 659.
[84] *Id.* at 660.
[85] *Id.* at 661.
[86] 562 U.S. 134 (2011).
[87] Hu, *supra* note 66, at 676.
[88] *Id.*
[89] *Id.* at 654.

their residents. However, these concerns would be addressed if we adopted the approach of the European Union's General Data Protection Regulations (GDPR), by setting a national standard as the floor for biometric data protection that does not preempt state laws with more stringent requirements.

Another critique of the push for a national biometric data processing standard may result in the lock-in effect and stifle competition. However, a national standard would encourage reasonable collection, aggregation, use, and retention of user biometric data. The requirements may financially burden small companies more than large corporations with exponentially more resources, but the idea of "privacy by design" embodied in the GDPR approach reduces the compliance costs for all companies by pushing them to think about privacy from the onset.[90] Scholars may also raise the difficulty of crafting a nationwide standard that could be agreed upon to become the law, due to the differing concerns of different states. However, as difficult as it will be to create a national standard that the states can agree on now, this difficulty will only increase in the future as biometric data becomes more embedded into our lives and monetization of it increases. It is critical that we begin working a national standard for biometric data processing now.

IV. ADOPTING THE GDPR APPROACH: SETTING A NATIONAL STANDARD AS THE FLOOR WOULD NOT PREEMPT STRONGER STATE LAWS

A. What is the General Data Protection Regulation?

The General Data Protection Regulation (GDPR)[91] was passed in April 2016 and went into effect on May 25, 2018.[92] The GDPR applies both to organizations located within the European Union (EU) and those "located outside of the EU if they offer goods or services to,

[90] *GDPR Key Changes*, EU GDPR.ORG, http://www.eugdpr.org/key-changes.html.

[91] General Data Protection Regulation, *supra* note 4 .

[92] *See GDPR Key Changes*, *supra* note 90.

or monitor the [behavior] of, EU data subjects."[93] GDPR also applies to "all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location." [94] The GDPR approach differs from the United States approach. GDPR places the burden on the private companies to justify their collection, use, and storage, of personal data rather than the consumer to protect their data.[95]

1. GDPR Specifics

GDPR aims to "protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established."[96] GDPR's key changes include: increased territorial scope (extra-territorial applicability), penalties, consent, breach notification, right to access, right to be forgotten, data portability, privacy by design, and the requirement for companies to appoint a data protection officer.[97]

The scope of the GDPR includes not just companies located in the European Union that process personal data of subjects residing in the Union, but also companies located outside of the European Union as well, provided that they process data from those data subjects.[98] The GDPR also requires businesses not located within the European Union, but who process data of EU citizens, to appoint a representative in the European Union.[99]

The GDPR imposes penalties on organizations that do not comply with its requirements of up to four percent of their annual global turnover or twenty million euros, whichever is greater.[100] While the GDPR takes a tiered approach to penalties, the penalties apply to

[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*
[99] *Id.*
[100] *Id.*

controllers and processors.[101] Thus, clouds will also have to comply with GDPR requirements.[102]

The GDPR's consent requirement is one that is heightened, requiring the request for consent be given in "an intelligible and easily accessible form, with the purpose for data processing attached."[103] Also, the consent "must be as easy to withdraw as it was to give it."[104]

As for data subject rights, the GDPR provides the right to breach notification, right to access, right to be forgotten, and right to data portability.[105] These rights require that all member states will have to give customers and controllers notice of data breach within seventy-two hours.[106] Also, data subjects have the right to know "whether or not personal data concerning them is being processed, where and for what purpose."[107] Data subjects are also entitled to a free copy of their personal data in electronic format.[108] Most importantly, if data subjects meet the conditions, they "have the right to have the data controller erase his [or] her data, cease further dissemination of the data, and potentially have third parties halt processing of the data.[109] The GDPR also gives data subjects the right to obtain personal data related to them in a "commonly use and machine readable format."[110] They also have the right to transfer that data to another controller.[111]

GDPR requires data protection from the onset, and not just an afterthought. [112] Data controllers are required to "implement appropriate technical and organizational measures . . . in an effective way."[113] Data controllers are also only to process data "absolutely

---

[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] *Id.*

necessary for the completion of its duties" and to limit "access to personal data to those needing to [process the data]."[114] The GDPR also requires certain controllers and processors to have data protection officers (DPOs) and outlines the duties of the DPOs[115] making data processing less bureaucratic and more accountable.

2. Germany's Elevated Standard

Germany's information privacy standards are elevated from the fundamental GDPR requirements. The principal data protection legislation in Germany is the Federal Data Protection Act (FDPA).[116] The German federal states also have state-level data protection laws.[117] While in Germany these state-level laws only apply to the public sector, there are other sector specific legislations to protect data.[118]

The FDPA was last amended on July 5, 2017, and it fully replaces the previous FDPA.[119] The new FDPA "is intended to adjust the German legal framework to the new [GDPR]" and is effective as of May 25, 2018.[120] In addition to the key principles of the GDPR, the FDPA also mandates a complex regime for sensitive data that "reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or genetic data, biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation."[121] While the GDPR prohibits processing of such sensitive data unless exceptions apply, the FDPA "widens the scope of these exceptions" but requires

---

[114] *Id.*

[115] *Id.*

[116] Anna Pateraki, *Germany*, *in* THE INTERNATIONAL COMPARATIVE LEGAL GUIDE TO: DATA PROTECTION 2017, 93 (4th ed. 2017), http://www.hunton.com/files/upload/International-Comparative-Legal-Guide-to-Data-Protection-2017-Hunton-Chapters.pdf (citing *Bundesdatenschutzgesetz* [BDSG] [Federal Data Protection Act], June 30, 2017, BGBL I at 2097 (Ger.)).

[117] *Id.*

[118] *Id.*

[119] Viola Bensinger & Carsten Kociok, *New German Federal Data Protection Act Officially Published*, GREENBERGTRAURIG (July 26, 2017), http://www.gtlaw.com/en/insights/2017/7/new-german-federal-data-protection-act-officially-published.

[120] *Id.*

[121] *Id.*

extensive steps be taken to protect the information processed.[122] As for employee data, the GDPR does not protect employee data processing.[123] However, the FDPA allows for employee data processing only for the necessity of "setting up, performing, or terminating an employment relationship."[124] The new FDPA has other elevated standards in addition to the GDPR and they move toward the goal of securing personal data. Germany's FDPA is an example of a uniform standard that does not preempt states from implementing elevated standards.

B. GDPR Approach Applied to Biometric Data Protection in the United States

If we applied the GDPR approach to information privacy to protect biometric data, then we could have a national standard that would not preempt related and more stringent state legislation. The ideas of increased territorial scope (extra-territorial application), penalties, consent, breach notification, right to access, right to be forgotten, data portability, privacy by design, and the requirement of data protection officers from the GDPR should be adopted in our national standard.

The scope element would be through having a national standard that applies to all states. By having a high penalty like GDPR, companies will be deterred from violating the national standard. The penalties imposed by the national standard should also have a tiered approach to account for companies' efforts to encourage them to try to comply with the national standard. Most importantly, penalties should be applied to controllers and processors.[125] Thus, fusion centers will also have to comply with GDPR-like requirements.

Requiring that consent be given in "an intelligible and easily accessible form" and having the purpose for processing attached will keep consumers informed and pressure companies to collect and use consumers' biometric data responsibly instead of mass collecting

[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.*

anything they can.[126] The requirement that the consent "must be as easy to withdraw as it was to give" will allow individuals who are not familiar with technology or who do not have time to go through the lengthy withdrawal process to protect their biometric data.[127]

The rights that the GDPR provides individuals will resolve the issue that many plaintiffs in biometric data suits face: having a cause of action. These rights include: the right to breach notification, right to access, right to be forgotten, and right to data portability.[128] The requirement that customers and controllers be given notice of data breach within seventy-two hours allows individuals to react in the instance of a data breach.[129] Since biometric data could be used as security access to different aspects of an individual's life, immediate reaction to data breach is crucial. Similar to credit score notifications, being able to know "whether or not personal data concerning them is being processed, where and for what purpose" allows individuals to verify and correct any incorrect data.[130] This is crucial when our biometric identifier is unique to us and cannot be changed. The free copy of personal data in electronic format will allow individuals to be confronted with what strangers already know about them.[131] If people are content with strangers knowing intimate details about their lives, it should be an informed decision. The ability to request information that is linked to our biometric identifiers easily can mitigate misuse. Consumers will be able to know who has access to such information and how they are using that information. By providing individuals with easy access to this information, it will teach people about the information they are sharing and pressure private companies to justify the collection, aggregation, and retention of our data.

In a recent article, an individual in the European Union requested a copy of the information that Tinder collected about her through her use of the application.[132] She received 800 pages of her

---

[126] *Id.*

[127] *Id.*

[128] *Id.*

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] Judith Duportail, *I Asked Tinder for My Data. It Sent Me 800 Pages of My*

"deepest, darkest secrets."[133] From those 800 pages, she learned things about her hopes, her fears, and sexual preferences that she had never known.[134] The realizations she had from reading her 800-page report could have been viewed by the many Tinder employees or whoever the company sells her information to. It is an uncomfortable thought that strangers can know more about our insecurities, thoughts, and feelings than we know about ourselves. The aggregation of this data linked to our biometric identifiers enables strangers to envision who we are, with a vision that is more complete than we may have ourselves. People who have never met us have access to such intimate details about our lives, our feelings, and our thoughts. It is only right that we are able to see that complete picture too.

The option to have certain biometric data erased and to make others "cease further dissemination of the data, and potentially have third parties halt processing of the data" is the level of control we need for our biological unique identifiers.[135] The right to obtain personal data related to them in a "commonly use and machine readable format," and the right to transfer that data to another controller will add to the control individuals will have over their biometric data and relieve them of the need to obtain new ones if they need them.[136]

Implementing the GDPR's privacy by design would change the current system from an opt-out to an opt-in system.[137] This will reduce the burden on consumers and shift the burden to companies processing biometric data since they are in the better position financially to act responsibly and protect our biometric data. As the controllers and processors of such sensitive data, it is vital that companies be required to "implement appropriate technical and organisational measures . . . in an effective way."[138] Companies should only process data that is

---

Deepest, Darkest Secrets, THE GUARDIAN, (Sept. 26, 2017, 2:10 PM), http://www.the guardian.com/ technology/ 2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold.

[133] *Id.*

[134] *Id.*

[135] *GDPR Key Changes*, *supra* note 90.

[136] *Id.*

[137] *Id.*

[138] *Id.*

"absolutely necessary for the completion of its duties" and limit "access to personal data to those needing to" process the data.[139] This requirement will be crucial when the monetization of biometric data increases to prevent companies from mass collection simply to sell consumers' biometric data. The requirement of companies to have data protection officers (DPOs) would not likely be a heavy burden on the private sector because the requirement would only apply to well-staffed companies that heavily process biometric data. Whereas larger companies that process biometric data internationally would likely already be in compliance with this requirement pursuant to the GDPR, provided that they process any data from EU residents.[140]

Applying the GDPR approach in the United States would allow consumers to have control over the collection, aggregation, and retention of their biometric data and shift the burden over to companies to justify their use of and protect this data.

V. CONCLUSION

The trolley scenarios discussed at the onset of this Article paint a haunting picture of how today's fragmented data can be used when connected, resulting in the need for national data protection, especially for our unique identifying biometric information.

As subjects of a mosaic, it is time we gain control over the mosaic of our lives that everyone else has already seen.[141] We should be able to see this mosaic and say, "this one piece of information is too intimate for the world to see, remove it." We should be able to say, "this piece of data no longer represents who I am or what my life is about, remove it." But as of right now we are incapable of doing so. We don't even have the ability to enter the art museum to view the entire mosaic portraying us that private companies and possibly even our government can see.

---

[139] *Id.*

[140] *Id.*

[141] *Id.*