UNTAG ME: WHY FEDERAL JUDGES ARE BROADLY CONSTRUING ILLINOIS'S BIOMETRIC PRIVACY LAW

Lisa P. Angeles†

"There is nothing inherently right or wrong with facial recognition technology. Just like any other new and powerful technology, it is a tool that can be used for great good. But if we do not stop and carefully consider the way we use this technology, it could also be abused in ways that could threaten basic aspects of our privacy and civil liberties."[1]

TABLE OF CONTENTS

† Managing Editor, *Cardozo Law Review*. J.D. Candidate (June 2021), Benjamin N. Cardozo School of Law; B.A., Manhattan College, 2016. I owe immense gratitude to the following individuals for their guidance throughout the writing process: Felix Wu, David Rudenstine, Nicholas Hebert, and the editors of the *Cardozo Law Review*, past and present. I dedicate this Note to the young men and women of color who dare to dream beyond their circumstances. You can and you will.

1 *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Priv. Tech. and the Law of the S. Comm. on the Judiciary,* 112th Cong. 1 (2012) (opening statement of Hon. Al Franken, U.S. Sen. from the State of Minn.).

INTRODUCTION

Have you ever wondered how Facebook recommends for you to "tag your friends" in new posts?[2] Biometrics is the umbrella term for any technology that either identifies who you are or authenticates who you are via physiological or behavioral characteristics.[3] These technologies include facial recognition, voice recognition, fingerprinting, vein geometry mapping, heartbeat recognition, and iris and retina scan recognition.[4] Fingerprinting and facial recognition are most familiar to the eighty-one percent of Americans who own smartphones—it is how your smartphone ensures that you are, in fact, you.[5] Facial recognition is also how Facebook recognizes your friends and prompts you to tag your friends in your newly shared posts.[6]

After a popular California tech company that facilitated biometric transactions across Illinois filed for bankruptcy, Illinois spurred to action in 2008 to pass the nation's first statute regulating the collection of biometric information by private companies.[7] Earlier that year, a

---

2 This question is at the heart of litigation under the Illinois Biometric Information Privacy Act. *See infra* Section II.A.

3 Biometrics may sound like a science fiction fantasy, but they have played a significant role in human life for some time now, primarily in the law enforcement field. In the late 1800s, a Frenchman, Alphonse Bertillon, created the first system of physical measurements and photography to identify criminals. *Alphonse Bertillon (1853-1914)*, U.S. NAT'L LIBR. MED., https://www.nlm.nih.gov/exhibition/visibleproofs/galleries/biographies/bertillon.html [https://perma.cc/7P3M-6XZM] (last updated June 5, 2014). Bertillon was superseded by Englishmen Sir Francis Galton and Sir Edward R. Henry, who created a fingerprint classification system based on pattern grouping. J. Edgar Hoover, *Fingerprint*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/fingerprint [https://perma.cc/82LT-UJZN] (last updated April 14, 2016). Thanks to Sir Henry, Scotland Yard became the first law enforcement agency to adopt fingerprinting in 1901. *Id.* Nevertheless, consumer access to biometric technology was scant and cumbersome until very recently. April Glaser, *Biometrics Are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016, 11:00AM), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns [https://perma.cc/WP4R-TZ7F]

4 Glaser, *supra* note 3; Stanley Goodner, *What Are Biometrics?: How this Measurement Technology Is Part of Your Life*, LIFEWIRE, https://www.lifewire.com/biometrics-4154702 [https://perma.cc/U5ZR-QSWT] (last updated Dec. 17, 2019).

5 *Mobile Fact Sheet*, PEW RESEARCH CENTER (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile [https://perma.cc/G4QK-GURP].

6 *See infra* Section II.A.

7 Illinois Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14 (2020); *e.g.*, Natasha Kohne & Kamran Salour, *Biometric Privacy Litigation: Is Unique Personally Identifying*

California tech company, Pay By Touch, had just gone bankrupt.[8] Pay By Touch had installed kiosks across Illinois that connected thousands of Illinoisans to biometric-facilitated transactions by allowing them to use their fingerprint to pay for groceries.[9] The California bankruptcy court approved the sale of Pay By Touch's database—a database containing the sensitive information, including fingerprints and financial data, of thousands of Illinois consumers.[10]

With few options for how to best protect consumers from biometric technology, the Illinois legislature targeted this market hoping to ensure it does not become the Wild West of sensitive, permanent identifying information. The Illinois legislature passed the Biometric Information Privacy Act (BIPA) in 2008—the first law of its kind.[11] The legislature intended to safeguard the public from the high risks associated with the use of commercial biometric transactions by granting citizens a private

---

Information Obtained from a Photograph Biometric Information?, 25 COMPETITION: J. ANTITRUST, UCL, AND PRIVACY SEC. ST. B. CAL. 150, 153 (2016).

8 Matt Marshall, *Pay By Touch in Trouble, Founder Filing for Bankruptcy,* VENTUREBEAT (Nov. 12, 2007, 2:09 PM), https://venturebeat.com/2007/11/12/pay-by-touch-in-trouble-founder-filing-for-bankruptcy [https://perma.cc/VUL2-NGCL]; Joseph Menn, *Turmoil Grips Pay By Touch Start-Up,* L.A. TIMES (Dec. 6, 2007, 12:00 AM), https://www.latimes.com/archives/la-xpm-2007-dec-06-fi-paybytouch6-story.html [https://perma.cc/U7FH-L6VP]; *Pay By Touch Shuts Down Biometrics Services*, FINEXTRA (Mar. 20, 2008) https://www.finextra.com/pressarticle/20514/pay-by-touch-shuts-down-biometrics-services [https://perma.cc/H7J5-Y7DQ].

9 Jon Van & Becky Yerak, *Payment by Fingerprint Disappears*, CHI. TRIB. (Mar. 21, 2008), https://www.chicagotribune.com/news/ct-xpm-2008-03-21-0803200909-story.html [https://perma.cc/DU7M-5EAU].

10 Kohne & Salour, *supra* note 7, at 152; *Pay By Touch Fades into History as Lenders Buy Core Assets,* DIGITAL TRANSACTIONS (Apr. 7, 2008), http://www.digitaltransactions.net/news/story/Pay-By-Touch-Fades-into-History-As-Lenders-Buy-Core-Assets [https://perma.cc/7GU6-EUTJ].

11 ILL. COMP. 14; Kohne & Salour, *supra* note 7, at 152–53; *see generally* Molly K. McGinley, Kenn Brotman, & Erinn L. Rigney, *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, NAT'L. L. REV. (Mar. 25, 2019), https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states [https://perma.cc/76MY-5VDP]. The legislature noted that major national corporations used Illinois as pilot test sites for biometric-facilitated transactions in grocery stores, gas stations, and school cafeterias. COMP. 14/5(b). The legislature also struggled with the uniqueness of biometric information—once the information is comprised, you cannot change your fingerprint or face. *Id.* 14/5(c).

right of action.[12] BIPA spurred other legislatures to propose and enact biometric privacy laws, though none with a private right of action.[13]

BIPA created a litigation onslaught by private citizens against America's largest internet companies, including Facebook, Google, and Shutterfly.[14] Many of these cases reflected the same central claim: the defendant is accused of taking the following steps without plaintiff's consent as required under BIPA: (1) scanning a photograph of plaintiff's face; (2) extracting plaintiff's unique facial geometry from the photograph; (3) using the extracted data to create a faceprint; and (4) comparing the plaintiff's faceprint to an existing database for purposes of identifying the plaintiff.[15] The most popular defense is a 12(b)(6) motion arguing that BIPA itself explicitly denies statutory protection to photographs and data derived therefrom. One would expect the clear statutory language to prevail, but it *does not*.[16] This Note intends to provide a reason why Article III judges are eschewing clear statutory language.

This Note explores a sampling of United States Supreme Court decisions to parse a common thread affirming the right to privacy that weaves through our constitutional rights and, at times, is the fundamental basis for overturning state legislation. This Note does not argue that constitutional checks control in the case of biometric privacy laws, but that the fundamental interest in a right to privacy exists and is triggered when third parties collect biometric data. This Note then further justifies allowing judges to broadly construe biometric privacy laws because commercial entities are the least-cost-avoiders for preventing harm to citizens and there is little incentive to self-regulate in the booming biometric market.

Part I of this Note explains how biometric systems, like facial recognition systems, function. Part I also surveys state biometric privacy laws, and details which states have enacted laws, which states have proposed laws, and what federal legislators have proposed. Part II begins

---

12 ILL. COMP. 14/5 (g).

13 *Infra* Section I.B.

14 *Infra* Section II.A.

15 *Infra* Section II.A.

16 *Infra* Section II.A; *see also* FED. R. CIV. P. 12(b)(6) ("Every defense to a claim for relief in any pleading must be asserted in the responsive pleading if one is required. But a party may assert the following defenses by motion . . . failure to state a claim upon which relief can be granted.").

by interpreting the statutory language of the surveyed laws. This interpretation creates a baseline by which we can expect courts to operate. Next, Part II considers the decisions that turn BIPA, and similar laws, on their head. Part II.B highlights the Supreme Court's discussions on privacy through time via the Fourth Amendment and when the Court has used privacy to rule supreme over state legislation. Part II.C introduces how the least-cost-avoider theory, the lack of incentives for corporations to self-regulate, and the commercial ubiquity of biometrics justifies placing a greater onus on corporations concerning the biometric privacy of consumers. Finally, Part II.C provides an example of when a biological privacy law was broadly construed to place a higher burden on the collector.

I. BACKGROUND

A. *Ins and Outs of Biometric Data Systems*

Before examining the law, we must ask: how do the systems lawmakers seek to regulate function? Biometric information is, generally, physiological or behavioral characteristics that may function as personal identifiers.[17] Fingerprinting, palm printing, iris and retina scans, face geometry, vein geometry, and scent testing are physiological identifiers.[18] Behavioral identifiers include mapping of the voice, gait, signature, keystroke, or heartbeat.[19] Whether physiological or behavioral, these identifiers are ideal because they are universal, unique, permanent, collectable, distinguishable, and difficult to duplicate.[20] Thus, instead of using a key or password, biometric systems use who you are to identify you.

Biometric systems are complex, but most boil down to three distinct processes.[21] First, the enrollment process records your basic information

---

17 *See* Goodner, *supra* note 4.

18 *Id.*

19 *Id.*

20 *Id.*

21 AWARE, INC., WHAT ARE BIOMETRICS? 2–3 (2014), https://www.aware.com/portfolio-items/what-are-biometricswhite-paper [https://perma.cc/WAD4-9N5C] [hereinafter AWARE

and captures a live image of the trait to be used.[22] Second, the storage process extracts a template from the live image and stores the new template in a template database while preserving the live image in an archive.[23] Finally, the comparison process: (1) captures a live image; (2) extracts a template from the live image; (3) uses algorithms to compare the new templates in the template database; and (4) presents match or no match results.[24]

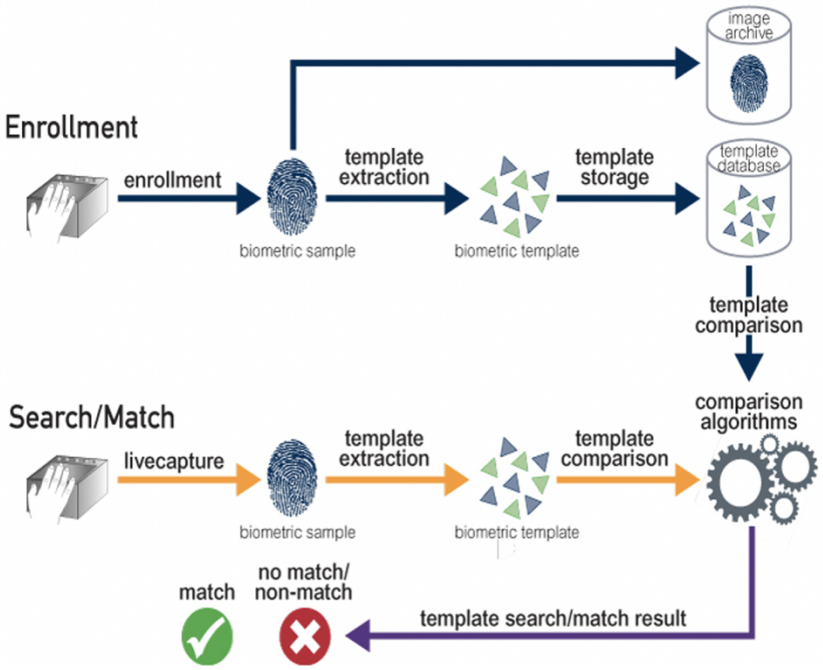

Figure 1, above, depicts a biometric process for fingerprints.[25] Figure 1 exemplifies how a biometric process can be used for security. Processes, like those depicted in Figure 1, can be used to clock-in at work, enter a limited-access room, and more. In the enrollment branch of Figure 1, fingerprint images are converted to a template stored for future comparison. The search/match branch shows how the system takes a

WHITE PAPER]; Tracy V. Wilson, *How Biometrics Works,* HOWSTUFFWORKS (Nov. 11, 2005), https://science.howstuffworks.com/biometrics.htm [https://perma.cc/9QDW-VWPQ].

22 AWARE WHITE PAPER, *supra* note 21; Wilson, *supra* note 21.

23 AWARE WHITE PAPER, *supra* note 21; Wilson, *supra* note 21.

24 AWARE WHITE PAPER, *supra* note 21; Wilson, *supra* note 21.

25 AWARE WHITE PAPER, *supra* note 21, at 3.

"livecapture" or image of the fingerprint, extracts the template, and uses comparison algorithms to decide whether a match exists in the database.[26]

B. *Survey of State Laws*

In response to the rapidly growing use of biometrics, some state governments have sought to create protective schemes for their citizens. Currently, California, Illinois, Texas, and Washington have enacted biometric privacy laws.[27] Legislatures from Alaska, Arizona, Delaware, Florida, Massachusetts, Michigan, and New York have proposed biometric privacy laws.[28] Biometrics have even captured the attention of the United States Senate. On March 14, 2019, Senator Roy Blunt introduced the Commercial Facial Recognition Privacy Act of 2019.[29] Senator Maria Cantwell then submitted her proposal, the Consumer

---

26 *Id.*

27 California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798 (West 2020); BIPA, 740 ILL. COMP. STAT. 14 (2020); Capture or Use of Biometric Identifier (CUBI), TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019); Biometric Identifiers, WASH. REV. CODE. § 40.26 (2020).

28 Biometric Identifiers, H.B. 2478, 44th Leg., Reg. Sess. (Ariz. 2019), https://legiscan.com/AZ/text/HB2478/id/1857901 [https://perma.cc/P8P4-8HFZ] (introduced in January 2019 and voted "do pass" by House minority caucus in February 2019); Florida Biometric Information Privacy Act, H.B. 1153, 2019 Sess. (Fla. 2019), https://www.flsenate.gov/Session/Bill/2019/1153/BillText/Filed/PDF [https://perma.cc/95NS-U84Y] (withdrawn on May 3, 2019; included a private right of action and was very similar to Illinois's BIPA); An Act Relative to Consumer Data Privacy, S. 120, 191st Gen. Court, Reg. Sess. (Mass. 2019), https://malegislature.gov/Bills/191/SD341 [https://perma.cc/PGG9-QGTB] (referred to Massachusetts' Senate committee on Consumer Protection and Professional Licensure on January 22, 2019); Biometric Privacy Protection Act, H.B. 350, 149th Gen. Assemb. (Del. 2018), https://legis.delaware.gov/BillDetail/26395 [https://perma.cc/Q25U-6GBH] (failed to leave committee); Biometric Privacy Act, Assemb. B. A9793, 241st Leg. Sess., Reg. Sess. (N.Y. 2018), https://www.nysenate.gov/legislation/bills/2017/a9793 [https://perma.cc/RMQ9-6H48] (failed in committee); Biometric Information Privacy Act, H.B. 5019 (Mich. 2017), http://www.legislature.mi.gov/documents/2017-2018/billintroduced/House/pdf/2017-HIB-5019.pdf [https://perma.cc/274Y-QK2U]; Collection of Biometric Information, H.B. 96, 29th Leg. (Alaska 2015), https://www.akleg.gov/basis/Bill/Text/29?Hsid=HB0096A# [https://perma.cc/D4ZM-SMDE].

29 Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/847/text [https://perma.cc/MCM3-NSQH].

Online Privacy Rights Act, on December 3, 2019.[30] Both bills landed in the Committee on Commerce, Science, and Transportation.[31] Finally, in late 2019, Representatives Anna G. Eshoo and Zoe Lofgren of California introduced the Online Privacy Act.[32] Even though Congress has yet to pass a federal law, biometrics remain at the forefront of legislation.

1. Enacted State Laws & How They Define Biometric Data

This Note presents the following enacted state laws in chronological order, as this order best depicts the shift in thinking by legislatures. Between 2008 and 2017, Illinois, Texas, and Washington enacted dedicated biometric privacy laws.[33] In 2018, California amended its general privacy law to protect biometric information—a move that other states did not follow.[34]

This subsection provides a general overview of each state's biometric privacy law or proposal, including whether the statute defines biometric identifiers, requires notice and consent to collect data, and/or authorizes private rights of action against corporations for statutory violations.

a. The First Attempt at Regulating Biometric Data Collection: The Illinois Biometric Information Privacy Act

Illinois's BIPA protects biometric identifiers and biometric information.[35] Biometric identifiers are defined as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," and "do not

---

30 Consumer Online Privacy Rights Act (COPRA), S. 2968, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/2968/text [https://perma.cc/Y56D-JXYJ].

31 S. 2968; S. 847.

32 Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/house-bill/4978/text [https://perma.cc/732W-PT6K].

33 BIPA, 740 ILL. COMP. STAT. 14 (2020); CUBI, TEX. BUS. & COM. CODE ANN. § 503.001 (West 2019); Biometric Identifiers, WASH. REV. CODE. § 40.26 (2020).

34 California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798 (West 2020). Texas's CUBI comes close. It is under Title 11 Personal Identity Information, but Chapter 503, where the biometric protection sits, reads as a stand-alone law. California's law is distinct because biometric information is labeled as one category of personal information, and the protection scheme generally references all categories of personal information—not biometric information alone.

35 ILL. COMP. 14/10.

include writing samples, written signatures, [or] photographs."[36] Biometric information is considered "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier," but "does not include information derived from items or procedures excluded under the definition of biometric identifiers."[37]

Though BIPA includes guidelines on collection, retention, disclosure, and destruction, this Note will focus on collection, as it is the key to 12(b)(6) motions.[38] When collecting, or otherwise obtaining, biometric identifiers or biometric information, private entities must (1) give notice to the consumer that such data is to be collected; (2) inform the consumer in writing of the purpose and time period for which the data is being collected; and (3) receive written consent from the consumer.[39] Private entities collecting biometric identifiers or information must have a public-facing retention schedule that complies with BIPA.[40] BIPA also contains provisions barring financial profiteering

---

36 *Id.* A slew of other items are excluded from BIPA, such as:

> [H]uman biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

Id.

37 *Id.*

38 *Id.* at 14/15; *infra* Section II.A.

39 *Id.* at 14/15(b).

40 *Id.* at 14/15(a) (stating that entities must destroy the data either when the initial purpose for collection is met or "within three years of the individual's last interaction with the private entity, whichever occurs first").

from possession of biometric indicators or information, or the dissemination of such data without consent or a warrant.[41]

Uniquely, BIPA contains a right of action for private citizens.[42] The prevailing party may recover in the following instances: (1) when a private entity negligently violates BIPA; (2) when a private entity intentionally or recklessly violates BIPA; and (3) for reasonable attorneys' fees and costs, and other relief, including injunctions.[43] Because of this recovery scheme, BIPA has made Illinois a national litigation hotbed.[44] Under BIPA, plaintiffs have sued Google, Facebook, Shutterfly, TikTok, and over thirty other companies ranging from locker rentals to tanning salons in high-profile federal and state lawsuits.[45]

b. The Texas CUBI: A Restrained Approach

In 2009, Texas soon followed Illinois with Capture or Use of Biometric Identifiers, or CUBI.[46] Texas defines a biometric identifier as a

---

41 *Id.* at 14/15(c)–(d).

42 *Id.* at 14/20.

43 *Id.*

44 Charles N. Insler, *Understanding the Biometric Information Privacy Act Litigation Explosion*, 106 ILL. B.J. 34, 35 (2018).

45 *Id.*; *see*, *e.g.,* Consolidated Am. Class Action Compl. by Interim Lead Counsel for the Northern District of California for, inter alia, Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*, *In re* TikTok, Inc. Privacy Litigation, No. 1:20-cv-04723 (N.D. Ill. Aug. 14, 2020); Rivera v. Google Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017); *In re* Facebook Biometric Information Privacy Litigation, 185 F. Supp. 3d 1155 (N.D. Cal. 2016); Norberg v. Shutterfly, Inc. 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015). *In re Facebook Biometric Information Privacy Litigation* reached a critical milestone on August 19, 2020—Judge Donato of the U.S. District Court for the Northern District of California granted preliminary approval of a $650 million settlement. *In re* Facebook Biometric Information Privacy Litigation, No. 15-cv-03747-JD (N.D. Cal. Aug. 19, 2020), ECF No. 474 (order granting preliminary approval of class action settlement). Additionally, Bloomberg has reported that a settlement in principle, albeit tumultuous, has been reached in *In re TikTok, Inc. Privacy* Litigation. Malathi Nayak, *TikTok Poised for Deal to Avoid Millions in U.S. Privacy Damages*, BLOOMBERG (Aug. 19, 2020 9:54 PM), https://www.bloomberg.com/news/articles/2020-08-20/tiktok-poised-for-deal-to-avoid-millions-in-privacy-damages [https://perma.cc/J4UX-WS8L] (explaining that settlement in principal was reached and complaints were raised on the fairness of such agreement). Though this is a critical milestone for both cases, this Note does not center on the resolution or success of lawsuits under the various biometric privacy laws. This Note focuses on privacy and other underlying interests potentially influencing the statutory interpretation of the Illinois Biometric Information Privacy Act by multiple federal judges.

46 CUBI, TEX. BUS. & COM. CODE ANN. § 503.001 (West 2017).

"retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[47] Capturing of a biometric identifier for commercial purposes is forbidden without informing the individual and receiving consent for capture.[48] CUBI also subjects private companies to disclosure, security, and retention limits.[49] In Texas, only the Attorney General can bring actions to recover under CUBI.[50]

c. Washington State Joins the Biometric Privacy Bandwagon

Nearly ten years later, Washington passed its own biometric privacy law.[51] Washington defined biometric identifiers as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's retina or iris scan, fingerprint, voiceprint, DNA, or scan of hand or face geometry."[52] Unlike Illinois, this definition of biometric identifiers is much broader. However, Washington retains Illinois's exclusion of photographs.[53]

Washington's law requires notice and consent before collecting a consumer's biometric identifier for commercial purposes.[54] Additionally, without further consent, an entity cannot sell or otherwise disclose the biometric identifier, with very few exceptions.[55] The consent mechanism here is akin to Texas—the law does not specify that consent must be in writing.[56]

Also similar to Texas's law, Washington's does not contain a private right of action.[57] Notably, Washington has an exemption for biometric data collected for security purposes.[58] Additionally, a biometric identifier can be disclosed to a third party who "contractually promises that the

---

47 *Id.* § 503.001(a).

48 *Id.* § 503.001(b).

49 *Id.* § 503.001(c). These limitations mirror much of Illinois's BIPA, but because this Note focuses on collection we will not explore this part of the legislation any deeper.

50 *Id.* § 503.001(d).

51 Biometric Identifiers, WASH. REV. CODE. § 40.26 (2017).

52 *Id.* § 40.26(7)(b).

53 *Id.* § 40.26(7)(b)(i).

54 *Id.* § 40.26(1).

55 *Id.* § 40.26(2)(a).

56 *Id.* § 40.26(1)(a)-(b); John G. Browning, *The Battle Over Biometrics: A Look at the Law in Texas and Two Other States*, 81 TEX. B.J. 674, 676 (2018).

57 Biometric Identifiers § 40.26; Browning, *supra* note 56, at 674.

58 Biometric Identifiers § 40.26.

biometric identifier will not be further disclosed and will not be enrolled in a database for a commercial purpose."[59]

d. California Incorporates Biometric Data into its Blanket Personal Information Privacy Law

Most recently, California enacted the California Consumer Privacy Act of 2018 (CCPA), expanding its existing privacy framework to include protection of biometric data.[60] California now views biometric information as just one kind of personal information. To qualify as personal information, the information must identify, relate to, describe, or be reasonably capable of being linked with a particular consumer or household.[61] This definition specifically includes biometric information.[62]

California defines biometric information as "an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity."[63] California also specifically includes imagery of the iris, retina, and face that can be used to extract identifying information.[64]

The CCPA regulates how any business, within or without California, can collect, retain, or sell Californians' personal information.[65] The CCPA offers protection in several ways. First, it grants a right to access personal data.[66] If requested, a company must share all the information compiled

---

59 *Id.*

60 CCPA, CAL. CIV. CODE § 1798 (West 2020) (taking effect on January 1, 2020); *see also* Thompson Hine LLP, *State Biometric Privacy Legislation: What You Need to Know*, LEXOLOGY (Sept. 5, 2019), https://www.lexology.com/library/detail.aspx?g=ebc0e01c-45cc-4d50-959e-75434b93b250 [https://perma.cc/B57Q-8GAR].

61 CIV. § 1798.140(*o*)(1).

62 *Id.* § 1798.140(*o*)(1)(e).

63 *Id.* § 1798.140(b).

64 *Id.*

65 *California Expands Consumer Privacy Protections,* THOMPSON HINE LLP (July 9, 2018), https://www.thompsonhine.com/publications/california-expands-consumer-privacy-protections [https://perma.cc/7TLW-CAVF].

66 CIV. § 1798.100(a); Jill Cowan & Natasha Singer, *How California's New Privacy Law Affects You*, NEW YORK TIMES (Jan. 3, 2020), https://www.nytimes.com/2020/01/03/us/ccpa-california-privacy-law.html [https://perma.cc/EBJ2-NSMF].

about the consumer.[67] Second, Californians may now request deletion of their data.[68]

Additionally, Californians can opt-out of the sale of their personal information.[69] Entities must respect the consumer's decision for at least one year before requesting authorization to sell the consumer's personal information.[70] Next, entities must receive permission of a parent before selling or sharing for profit the personal information of any child less than thirteen years of age.[71] Finally, the CCPA contains a private right of action for any consumer whose "nonencrypted and nonredacted personal information . . . is subject to unauthorized access and exfiltration, theft, or disclosure" resulting from security failure.[72] The consumer right to sue is highly limited to security breaches where the breached database was not sufficiently secured.[73] California's shift to penalizing disclosure and theft, as opposed to initial collection, is in stark contrast to Illinois, where a broad right of action penalizes any violation of BIPA.[74] However, this variance is not surprising, as BIPA is law dedicated to biometric privacy only, while the CCPA is a general privacy law that includes biometric privacy. Greater protections in California should lead to less need to litigate, where Illinois's narrow protections require greater enforcement to weed out bad actors.

2. Proposed State Laws and Their Definitions

In this subsection, this Note explores the proposed state laws in alphabetical order. Most laws were proposed between 2017 and 2019, with Alaska's as the outlier, having been proposed in 2015.

This subsection will focus on (1) how the proposals defined biometric data, information, or identifiers, with particular attention to whether precursors, like photographs, are protected; (2) what onus, if

---

67 CIV. § 1798.100(a); Cowan & Singer, *supra* note 66.

68 CIV. § 1798.105(a); Cowan & Singer, *supra* note 66.

69 CIV. § 1798.120(a); Cowan & Singer, *supra* note 66.

70 CIV. § 1798.135(a)(5); Cowan & Singer, *supra* note 66.

71 CIV. § 1798.120(c); Cowan & Singer, *supra* note 66.

72 CIV. § 1798.150(a)(1).

73 *Id.*

74 BIPA, 740 ILL. COMP. STAT. § 14/20 (2020).

any, is on the collector of biometric information at time of collection; and (3) whether a private right of action exists.

a. Alaska's 2015 Effort to Protect Biometric Data Fails

Alaska's 2015 proposal limited biometric data to "fingerprints, handprints, voices, iris images, retinal images, vein scans, hand geometry, finger geometry," or other identifying physical characteristics of individuals.[75] Biometric information was merely biometric data used in a biometric system.[76] Obtaining biometric data would require clear notice and documented, revocable consent.[77] Disclosure and sale of the information would be highly limited.[78] Additionally, Alaska proposed a private right of action.[79] Alaska's law was referred to the State Affairs and Judiciary Committees in February 2015.[80]

b. Arizona Remains in "Do Pass" Limbo

The Arizona House of Representatives minority caucus voted "do pass" in February 2019 to a dedicated biometric privacy law.[81] The law would protect automatic measurements of an individual's biological characteristics like fingerprints and voiceprints, but it would not include "physical or digital photograph, . . . video or audio recording," nor any data generated from those items.[82] Collection of biometric identifiers would only be possible if (1) the collector prevents the subsequent use of the identifier for commercial purpose or (2) the collector provides notice and receives consent from the collected.[83] A right of action would be reserved for the Attorney General only.[84]

---

75 Collection of Biometric Information, H.B. 96, 29th Leg. § 18.14.090(1) (Alaska 2015), https://www.akleg.gov/basis/Bill/Text/29?Hsid=HB0096A# [https://perma.cc/D4ZM-SMDE].

76 *Id.* § 18.14.090(2).

77 *Id.* § 18.14.010.

78 *Id.* § 18.14.020.

79 *Id.* § 18.14.070.

80 4 H. JOURNAL, 29th Leg., at 142 (Alaska 2015), https://www.akleg.gov/basis/Journal/Pages/29?Chamber=H&Page=0133&pageEnd=0149#HB%2096 [https://perma.cc/NG3A-9CFU].

81 Biometric Identifiers, H.B. 2478, 44th Leg., Reg. Sess. (Ariz. 2019), https://legiscan.com/AZ/text/HB2478/id/1857901 [https://perma.cc/P8P4-8HFZ].

82 *Id.* § 44-7901.

83 *Id.* § 44-7902.

84 *Id.* § 44-7903.

c. Delaware's Bold Attempt at Broad Construction of Biometric Data

Delaware's House Bill 350, the Biometric Privacy Protection Act, was assigned to a committee in 2018.[85] Biometric identifier would be defined as:

> a biologic or behavioral characteristic that can be used to identify a specific individual, including a finger or palm print, eye retina or iris scan, voice recognition, hand or face geometry, facial imaging or recognition, gait recognition, vein recognition, or other unique biological or behavioral characteristics.[86]

Biometric information would be "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier."[87] A collector of biometric information would need to provide notice and obtain consent.[88] Enforcement would be left to the Delaware Consumer Protection Unit of the Department of Justice.[89]

d. Florida's Bicameral Shot in the Dark

Both the Florida Senate and House of Representatives presented similar biometric privacy laws in 2019.[90] Both bills were filed in February 2019 and withdrawn from consideration in May 2019.[91] Both bills define biometric identifier as "retina or iris scan, fingerprint, voice print, or scan of hand or face geometry," but exclude "[w]riting samples, written

---

85 Biometric Privacy Protection Act, H.B. 350, 149th Leg. (Del. 2018), https://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=26395&legislationTypeId=1&docTypeId=2&legislationName=HB350 [https://perma.cc/LD4K-27C3] (legislative history at: https://legis.delaware.gov/BillDetail/26395 [https://perma.cc/Q25U-6GBH]).

86 *Id.* § 1202D(1).

87 *Id.* § 1202D(2).

88 *Id.* § 1204D.

89 *Id.* § 1207D.

90 Florida Biometric Information Privacy Act, H.R. 1153, (Fla. 2019), https://www.flsenate.gov/Session/Bill/2019/1153/BillText/Filed/PDF [https://perma.cc/95NS-U84Y] [hereinafter Florida House Bill] (legislative history at: https://www.flsenate.gov/Session/Bill/2019/1153 [https://perma.cc/EN2K-TUSK]; Florida Biometric Information Privacy Act, S. 1270, (Fla. 2019), https://www.flsenate.gov/Session/Bill/2019/1270/BillText/Filed/HTML [https://perma.cc/6UQ4-EKCS] [hereinafter Florida Senate Bill].

91 Florida House Bill; Florida Senate Bill.

signatures, [and] photographs."[92] Biometric information is any information based on an individual's biometric identifier used to identify an individual, excluding information derived from items or procedures specifically excluded under the definition biometric identifier.[93] Private entities cannot collect biometric information or identifiers without notice and written consent.[94]

e. Massachusetts's California-esque Venture

Next on the list, Massachusetts State Senators Cynthia Stone Creem, Tommy Vitolo, Michael O. Moore, and James B. Eldridge proposed a consumer data privacy bill.[95] The bill protects personal information, which includes biometric information.[96] The bill broadly defines biometric information to include any "physiological, biological[,] or behavioral characteristics," and any imagery from which an identifier (like a faceprint) can be extracted.[97] At collection time, the collector must notify the consumer, but the bill does not require consent.[98] The bill also includes a right to request more information from the collector, a right to request deletion of the biometric information, and a right to opt out of third-party disclosures with no penalty.[99] The Massachusetts bill includes a private right of action with interesting specificity—"[a] violation of this chapter shall constitute an injury in fact."[100] The last note on the bill shows a bicameral hearing scheduled for October 2019.[101]

---

92 Florida House Bill § 501.172(2)(a); Florida Senate Bill § 501.172(2)(a).

93 Florida House Bill § 501.172(2)(b); Florida Senate Bill § 501.172(2)(b).

94 Florida House Bill § 501.172(3)(b); Florida Senate Bill § 501.172(3)(b).

95 An Act Relative to Consumer Data Privacy, S. 120, 191st Gen. Court, Reg. Sess. (Mass. 2019), https://malegislature.gov/Bills/191/S120/Senate/Bill/Text [https://perma.cc/P5T5-832Q] (legislative history at: https://malegislature.gov/Bills/191/SD341 [https://perma.cc/PGG9-QGTB]).

96 *Id.* § m(1)

97 *Id.* § 1(b).

98 *See id.* § 2(a).

99 *Id.* §§ 3, 5, 6, 7.

100 *Id.* § 9(a).

101 *Id.*

f. Michigan Follows in Nearby Illinois's Footsteps

In September 2017, a Michigan legislator introduced the Biometric Information Privacy Act to the Michigan House of Representatives.[102] Michigan's definition of biometric identifiers followed a familiar pattern of including retina or iris scans, fingerprints, voiceprints, and face or hand geometry, but excluding photographs, written samples, or written signatures.[103] Biometric information's definition is also familiar: any information, regardless of procurement method, used to identify an individual, excluding data derived from items banned under biometric identifiers' definition.[104] Michigan also requires notice and written consent before collection of biometric data.[105] Additionally, Michigan embraces a private right of action for any negligent violation of the Act.[106]

g. Yankees Strikeout Again: How New York Missed its Chance

Finally, New York State attempted to pass its own biometric privacy law.[107] That bill was referred to the Consumer Affairs and Protection Committee in February of 2018.[108] The New York proposal defines biometric identifiers and information identically to Illinois, Florida, and Michigan.[109] The following are considered biometric identifiers: "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[110] The proposal shuts out writing samples, written signatures, and

---

102 Biometric Information Privacy Act, H.R. 5019 (Mich. 2017), http://www.legislature.mi.gov/documents/2017-2018/billintroduced/House/pdf/2017-HIB-5019.pdf [https://perma.cc/274Y-QK2U].

103 *Id.* § 3(a).

104 *Id.* § 3(b).

105 *Id.* § 5(3).

106 *Id.* § 7.

107 Biometric Privacy Act, Assemb. Bill A9793, 241st Leg. Sess., Reg. Sess. (N.Y. 2018), https://www.nysenate.gov/legislation/bills/2017/a9793 [https://perma.cc/RMQ9-6H48] (failed in committee). In 2019, even New York City considered biometric privacy laws. Three bills were considered requiring businesses to notify consumers when biometrics were used, requiring "real property owners to register the use of any biometric . . . devices," and preventing landlords from requiring tents to use "keyless entry technology to enter their apartment buildings or units." *See* Annie McDonough, *New York City Council Contemplates Banning Biometric Tech*, CITY & STATE N.Y. (Oct. 8, 2019), https://www.cityandstateny.com/articles/policy/technology/new-york-city-council-contemplates-banning-biometric-tech.html [https://perma.cc/22P8-XS75].

108 Biometric Privacy Act.

109 *See infra* Section I.B.

110 Biometric Privacy Act § 676-A.

photographs.[111] The definition of biometric information bars information derived from the shut-out items.[112] New York would also require notice and written consent for collection.[113] Noticeably, New York proposes a private right of action.[114]

3. The Federal Legislature's Attempt to Regulate and Define Biometric Data

In 2019, two bills on biometric privacy were presented to the United States Senate. First, Senator Roy Blunt of Montana introduced the Commercial Facial Recognition Privacy Act of 2019.[115] As the title denotes, this bill focuses on facial recognition technology only. Facial recognition technology, pursuant to Senator Blunt's proposal, is technology that "analyzes facial features in still or video images" and is used to either "assign a unique, persistent identifier" or for "unique personal identification of a specific individual."[116]

The proposal bars collection of facial recognition data unless there is notice and consent.[117] The proposal has a special carve out for "facial recognition data [that determines] whether an end user has given affirmative consent if the controller immediately and permanently destroys the facial recognition data after determining that the end user has not given affirmative consent."[118] However, this exception does not authorize "mass scanning of faces in spaces where end users do not have a reasonable expectation that facial recognition technology is being used on them."[119] This carve out would directly implicate persons such as Taylor Swift, who have used facial recognition technology on mass

---

111 *Id.*

112 *Id.*

113 *Id. §§ 676-A(5), B(2)(c).*

114 *Id.* § 676-C.

115 Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/847/text [https://perma.cc/MCM3-NSQH].

116 *Id.* § 2(5).

117 *Id.* § 3.

118 *Id.* § 3(e)(1)(b).

119 *Id.* § 3(e)(3).

crowds at concert venues, where attendees may potentially not reasonably expect that such technology may be used on them.[120]

While Senator Blunt's proposal implicates Taylor Swift's actions, it leaves a loophole for other actors.[121] The proposal makes an exemption for a "product or service designed for personal file management or photo or video sorting or storage if the facial recognition technology is not used for unique personal identification of a specific individual."[122] For example, companies like Ever advertise themselves as cloud-saving applications, but they are actually exploiting users' photographs to strengthen and market Ever's facial recognition AI.[123] Even IBM is partaking in this practice; IBM uses photos from Flickr to enhance its facial recognition algorithms.[124] Thus, Senator Blunt's bill explicitly creates an opportunity for companies like Ever and IBM to continue their questionable practices, even though there would be a federal facial recognition law on the books. As of this writing, the Senator's bill remains in committee.[125]

Senator Maria Cantwell of Washington's December 2019 bill, Consumer Online Privacy Rights Act (COPRA) also remains in committee.[126] Contrasted with Senator Blunt's bill, Senator Cantwell proposes a "foundational data privacy rights" act to "create strong oversight mechanisms, and establish meaningful enforcement."[127] COPRA uses a familiar definition for biometric information: "data generated from the measurement or specific technological processing of an individual's biological, physical, or physiological characteristics," and excludes "writing samples, written signatures, photographs," and more.[128]

---

120 *See infra* Section II.C.3.

121 S. 847.

122 *Id.*

123 Olivia Solon & Cyrus Farivar, *Millions of People Uploaded Photos to the Ever App. Then the Company Used Them to Develop Facial Recognition Tools.*, CNBC (May 9, 2019, 1:07 PM), https://www.cnbc.com/2019/05/09/ever-developed-facial-recognition-tools-using-photos-uploaded-to-app.html [https://perma.cc/X2M5-WBPC].

124 *IBM Used Flickr Photos for Facial-Recognition Project*, BBC NEWS (Mar. 13, 2019), https://www.bbc.com/news/technology-47555216 [https://perma.cc/JH7H-HVQQ].

125 Commercial Facial Recognition Privacy Act of 2019.

126 COPRA, S. 2968, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/2968/text [https://perma.cc/8DSA-ZM73].

127 *Id.*

128 *Id.* § 2(3).

Senator Cantwell introduces several new rights: a right to access and transparency, a right to delete, a right to correct inaccuracies, a right to controls, a right to data minimization, and a right to data security.[129] The Senator has characterized the bill as "Miranda Rights" for the digital age.[130] The Senator proposes the creation of a new bureau within the Federal Trade Commission to enforce the law.[131] Additionally, the bill preserves the right for states to create their privacy laws and enforce them.[132]

Lastly, Representatives Anna G. Eshoo and Zoe Lofgren of California introduced the Online Privacy Act in late 2019, a radical proposal petitioning for the creation of a new Digital Privacy Agency to enforce the sweeping privacy bill's consumer rights.[133] The bill does not explicitly protect biometric information, but protects any personal information "maintained by [certain corporations] that is linked or reasonably linkable to a specific individual."[134] The proposal would create nine new rights for consumers: the right to access, correct, or delete data, as well as the right to portability, human review of automated decisions, individual autonomy, notice, consent, and impermanence.[135]

II. ANALYSIS

A. *How Courts Broadly Interpret What Qualifies as Biometric Information Pursuant to Biometric Privacy Statutes*

After examining fourteen laws and bills, three major types of legislation emerge concerning the protection of photographs, which are

---

129 *Id.* §§ 102–06.

130 Lauren Feiner, *Senate Democrats Reveal New Digital Privacy Bill That Would Strengthen the FTC's Enforcement Powers Over Tech Companies,* CNBC (Nov. 26, 2019, 9:57 AM), https://www.cnbc.com/2019/11/26/senate-democrats-reveal-new-copra-digital-privacy-bill.html [https://perma.cc/7QLX-XG8T].

131 S. 2968 § 301(a).

132 *Id.* § 301(b).

133 Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/house-bill/4978/text [https://perma.cc/732W-PT6K].

134 *Id.* As the representatives are from California, it is no surprise that their proposal mirrors California's blanket privacy approach to protecting biometric data. *See supra* Section I.B.1.d.

135 H.R. 4978.

precursors to biometric data that many companies are accused of exploiting. The following table summarizes the three major types of legislation with respect to photographs.

Type 1	Explicitly *excludes* photographs.	Illinois, Washington, Arizona, Florida, Michigan, New York, U.S. Senator Cantwell's bill.
Type 2	*Includes* photographs.	California, Delaware, Massachusetts, U.S. Representatives Eshoo & Lofgren, U.S. Senator Blunt.
Type 3	Biometric data protection is narrowly described and/or the statute is silent on the matter.	Texas & Alaska.

Critically, the nation's leading law, Illinois's BIPA and its private right of action, falls under Type 1. Under a plain text reading, BIPA does not cover photographs nor any information derived from photographs.[136] Yet, time and again, when faced with this question, courts allow lawsuits to proceed.[137] The facial recognition lawsuits follow a common pattern; the defendant is accused of taking the following steps without plaintiff's consent per BIPA: (1) scanning a photograph of plaintiff's face; (2) extracting plaintiff's unique facial geometry from the photograph; (3) using the extracted data to create a face print; and (4) comparing the plaintiff's faceprint to an existing database for purposes of identifying the plaintiff.[138]

Norberg v. Shutterfly, filed in the United States District Court for the Northern District of Illinois, is considered the first judicial interpretation of BIPA.[139] Norberg alleged that Shutterfly, a photo-service company allowing users to store their photos online, unlawfully extracted

---

136 Kohne & Salour, *supra* note 7, at 155.

137 *See* Rivera v. Google, 238 F. Supp. 3d 1088 (N.D. Ill. 2017); *In re* Facebook Biometric Information Privacy Litigation, 185 F. Supp. 3d 1155 (N.D. Cal. 2016); Norberg v. Shutterfly, 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).

138 Kohne & Salour, *supra* note 7, at 155.

139 *Norberg*, 152 F. Supp. 3d at 1106 ("The BIPA was enacted in 2008, and to this date, the Court is unaware of any judicial interpretation of the statute."); Kohne & Salour, *supra* note 7, at 156; Ian Taylor Logan, Comment, *For Sale: Window to the Soul Eye Tracking As the Impetus for Federal Biometric Data Protection*, 123 PENN ST. L. REV. 779, 795 (2019); Lauren Stewart, Note, *Big Data* Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security, 60 B.C. L. REV. 349, 371–72 (2019) (explaining the sudden boom of class action lawsuits under BIPA in 2015, 2016, and 2017).

Norberg's facial geometry from a photograph uploaded to Shutterfly.[140] Shutterfly moved to dismiss for failure to state a claim under BIPA because BIPA explicitly excludes photographs. The court denied Shutterfly's motion.[141] Judge Norgle focused on Shutterfly's possession of Norberg's facial geometry—not the facial geometry's extraction from a photograph.[142] The court's brief, barely three-page opinion does not elaborate on why Judge Norgle chose to sidestep the photograph extraction issue.[143] Nevertheless, Norberg makes for an incredibly sympathetic plaintiff. Norberg was never a user of Shutterfly and never received notice or supplied consent for use of his biometric identifier.[144] In fact, Norberg stated that his friend uploaded and tagged a photo of him that found its way into Shutterfly's database.[145] In the end, Norberg and Shutterfly settled.[146] So, whether this theory would have succeeded later in the litigation is a mystery.

The following year, the Northern District of California saw another BIPA case with another motion to dismiss for failure to state a claim because BIPA's plain text excludes photographs and biometric data derived therefrom.[147] Three separate putative class actions were filed against Facebook in the Northern District of Illinois.[148] The three suits by Adam Pezen, Carlo Licata, and Nimesh Patel, respectively, were consolidated and transferred to the Northern District of California.[149]

In the class action, plaintiffs argued that Facebook's "Tag Suggestions" feature violated BIPA.[150] Facebook's "Tag Suggestions" is a feature that allegedly scans photographs uploaded to Facebook, extracts facial biometric data from the photographs, uses the data to identify

---

140 Kohne & Salour, *supra* note 7, at 156.

141 *Norberg*, 152 F. Supp. 3d at 1105.

142 *Id.* at 1106.

143 *See generally id.* at 1104–06.

144 *Id.* at 1106.

145 Kim Janssen, *Facial Recognition Lawsuit Against Shutterfly Can Go Ahead, Judge Rules*, CHI. TRIB. (Jan. 13, 2016, 8:56 AM), https://www.chicagotribune.com/business/ct-shutterfly-lawsuit-0113-biz-20160112-story.html [https://perma.cc/9WFZ-2SXM].

146 Kohne & Salour, *supra* note 7, at 157.

147 *See In re* Facebook Biometric Information Privacy Litigation, 185 F. Supp. 3d 1155 (N.D. Cal. 2016).

148 *Id.*; Kohne & Salour, *supra* note 7, at 157.

149 *In re Facebook*, 185 F. Supp. 3d 1155; Kohne & Salour, *supra* note 7, at 157.

150 *In re Facebook*, 185 F. Supp. 3d 1155; Kohne & Salour, *supra* note 7, at 157.

persons in future uploaded photos, and does all this without consent.[151] This feature encourages users to "tag" their friends in uploaded images, thus making Facebook more interactive and engaging.

Like Shutterfly, Facebook argued that "Tag Suggestions" was not subject to BIPA because BIPA excludes photographs and information derived from photographs—the plaintiffs' complaint here is an issue of photographs.[152] The California court did not buy into this argument, and radically departed from the *Norberg v. Shutterfly* theory.[153] Judge Donato interpreted "photographs" as *physical* photographs only, and not "digitized images stored as a computer file and uploaded to the [i]nternet."[154] Judge Donato argued that, reading the provisions of BIPA together, the Illinois legislature attempted to address emerging biometric technology while excluding physical identifiers that are "more qualitative and non-digital in nature."[155]

The opinion makes one thing certain: BIPA, on its face, would not apply to these facts. Thus, if the court were to include Facebook's "Tag Suggestions" program into BIPA's purview, it would have to do so via an exception. Characterizing the word "photographs" to mean tangible paper-and-ink allows the court to rope Facebook into BIPA's grasp.

One year later, *Rivera v. Google* was filed in the United States District Court for the Northern District of Illinois.[156] While Judge Chang came to the same result as Judges Norgle and Donato, Judge Chang attacked the photograph extraction issue from a new angle. When Google argued against the results in the Northern District of California, Judge Chang held that as advances in technology drove the Illinois legislature to pass BIPA in the first place, it is improbable that BIPA was meant to limit how biometric identifiers are measured.[157] Judge Chang poignantly asked, "Who knows how iris scans, retina scans, fingerprints, voiceprints, and scans of faces and hands will be taken in the future?"[158] Judge Chang's

---

151 *In re Facebook*, 185 F. Supp. 3d 1155; Kohne & Salour, *supra* note 7, at 157.

152 *In re Facebook*, 185 F. Supp. 3d 1155; Kohne & Salour, *supra* note 7, at 157.

153 *In re Facebook*, 185 F. Supp. 3d 1155; Kohne & Salour, *supra* note 7, at 157.

154 *In re Facebook*, 185 F. Supp. 3d at 1171.

155 *Id.*

156 Rivera v. Google, 238 F. Supp. 3d 1088 (N.D. Ill. 2017).

157 *Id.* at 1095–96.

158 *Id.* at 1096.

Katzmann-esque approach—looking to legislative history even when the statute is plain on its face—is thought-provoking.[159]

BIPA itself was enacted in 2008.[160] In 2008, Global Positioning Systems (GPS) became universal, Android phones hit the market, and Apple premiered the first "App Store."[161] Meanwhile, the first BIPA adjudication came in 2015. That seven-year gap represents a monumental leap in technology.[162] It is irrational to keep static a 2008 law and use it to regulate technological problems of today—the law must adapt. Furthermore, the Illinois legislature itself admitted that the "full ramifications" of biometrics are unknown.[163] In this light, Judge Chang's argument is sensible, but fully ignoring the statutory text still begs for a weightier reason.

What value judgments may have persuaded Judges Norgle and Donato to skirt the plain text reading of BIPA so that photographs receive some litigable protections? Perhaps the value of one's privacy led these judges to find creative ways to circumvent BIPA's plain text language.

B. *The United States Supreme Court Has Continually Expounded*

159 ROBERT A. KATZMANN, JUDGING STATUTES 29 (Oxford Univ. Press ed. 2014) ("At times, even when the statute is plain on its face, the judge may find legislative history helpful in reinforcing the court's understanding of the words. If, for example, the result suggested by the plain language seems absurd, then a broader inquiry, including consideration of legislative history, may be in order."). Katzmann's presentation of the "purposivism" approach is also often associated with Henry M. Hart and Albert M. Sacks. *See* FRANK. B. CROSS, THE THEORY AND PRACTICE OF STATUTORY INTERPRETATION 60 (Standard Univ. Press ed. 2009). Nevertheless, Judge Chang's look to legislative purpose keys into the *how* and *why* the Illinois legislature decided to pass BIPA, another idea that is not without support. *See* VICTORIA NOURSE, MISREADING LAW, MISREADING DEMOCRACY 135–36 (Harvard Univ. Press ed. 2016).

160 *See* BIPA, 740 ILL. COMP. STAT. 14 (2020).

161 Priya Ganapati, *Top Technology Breakthroughs of 2008*, WIRED (Dec. 25, 2008, 9:00 PM), https://www.wired.com/2008/12/top-technology-breakthroughs-of-2008 [https://perma.cc/K6R6-AB65].

162 *See id.*; Eric Walters, *The 10 Best Technology Advances of 2015*, PASTE (Dec. 22, 2015, 10:00 AM), https://www.pastemagazine.com/articles/2015/12/the-10-best-technology-advances-of-2015.html [https://perma.cc/R7YA-FDJL].

163 BIPA § 14/5(f).

Concerns for Privacy Interests

Louis Brandeis and Samuel Warren were not the originators of privacy, but they gave it legs in *The Right to Privacy* by framing it as an evolving right to be let alone.[164] The Justices chronicle a right to protection in person and property that led to the development of the law of battery and assault, nuisance, slander and libel, alienation of a partner's affection, and intellectual property.[165] Interestingly, it is often retold that the heart of the article was Justice Warren's marriage to a senator's daughter and the personal invasions the couple suffered at the hands of journalists and their newer, faster photography cameras.[166] Warren was highly concerned with new technology that allowed for wrongs to be committed without any knowledge of the injured party.[167]

Similar to Justices Brandeis and Warren, our generation is experiencing a technological shift. Sure, facial recognition data is not a

---

164 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) ("The right to life has come to mean the right to enjoy life, —the right to be let alone . . . ."). The article by the Justices truly did break the mold. *See, e.g.*, Benjamin E. Bratman, *Brandeis and Warren's "The Right to Privacy and the Birth of the Right to Privacy"*, 69 TENN. L. REV. 623, 623–25 (2002). In 1934, the American Law Institute published a nebulous definition of privacy in the first Restatement of Torts: "A person who unreasonably and seriously interferes with another's interest in not having his affairs known to others or his likeness exhibited to the public is liable to the other." RESTATEMENT (FIRST) OF TORTS § 867 Interference with Privacy (1939). Almost one hundred years after Warren and Brandeis, William Prosser formulated privacy into four distinct torts: (a) an unreasonable intrusion upon the plaintiff's seclusion, (b) the appropriation of the plaintiff's name or likeness, (c) unreasonably giving publicity to the plaintiff's private life, and (d) publicizing the plaintiff in a false light. RESTATEMENT (SECOND) OF TORTS § 652A General Principle (1977). Today, Prosser's formulation prevails in the common law. *See* G. EDWARD WHITE, TORT LAW IN AMERICA: AN INTELLECTUAL HISTORY 176 (2003). However, there is plenty of academic debate on the viability of Prosser's privacy torts in the modern era. *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805 (2010); Scott Jon Shagin, *The Prosser Privacy Torts in a Digital Age*, 251 N.J. LAW., MAG. 9 (2008).

165 Warren & Brandeis, *supra* note 164, at 193–95.

166 *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960); *see also* Joshua J. Kaufman, *The Invention that Resulted in the Rights of Privacy and Publicity*, VENABLE LLP (Sep. 24, 2014), https://www.venable.com/insights/publications/2014/09/the-invention-that-resulted-in-the-rights-of-priva [https://perma.cc/H85R-4NNC] ("What prompted Warren and Brandeis to write their *Law Review* article? Did it appear out of thin air? What threat motivated these gentlemen to feel a need to articulate this new doctrine and protection? It was the development of a nefarious, threatening and dangerous device, the *hand-held camera*.").

167 Warren & Brandeis, *supra* note 164, at 211.

traditional picture, but it is capturing our unique faces in cutting-edge fashion. That is what makes their perspective in *The Right to Privacy* particularly applicable to facial recognition. Looking back to Brandeis and Warren highlights the timeless desires of all persons—privacy, or being free from intrusion into one's acts and decisions.[168]

1. Privacy Interests and the Fourth Amendment

Justice Brandeis reiterated his strong feelings for the right to be let alone in his dissent from 1928's *Olmstead v. United States* decision.[169] *Olmstead* presented a Fourth Amendment question—whether evidence obtained sans warrant through wiretapping was constitutionally inadmissible in court.[170] The majority found no constitutional violation because the Fourth Amendment applied to physical searches of one's home, person, papers, and effects.[171] Brandeis offered a lengthy dissent.[172] The Justice argued that legislation is the reaction to negative experiences by the people-at-large, but that legislation should not remain stagnant through time.[173] Legislation should, instead, grow with the times for any new "conditions and purposes" to which its purpose would seek to legislate.[174] Moreover, the Framers themselves recognized the importance of the right to be let alone.[175] So much so that the Framers protected individuals from the government's intrusion upon that right through the Fourth Amendment.[176]

---

168 *Privacy*, BLACK'S LAW DICTIONARY (11th ed. 2019).

169 Olmstead v. United States, 277 U.S. 438, 471–85 (1928) (Brandeis, J., dissenting).

170 *Id.* at 438–71 (majority opinion); *see also* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

171 *Olmstead*, 277 U.S. at 463–64.

172 *Id.* at 471–85 (Brandeis, J., dissenting).

173 *Id.* at 472 ("Legislation, both statutory and constitutional, is enacted, it is true, from an experience of evils, but its general language should, therefore, be necessarily confined to the form that evil had theretofore taken.") (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

174 *Id.* at 472–73.

175 *Id.* at 478.

176 *Id.*

Justice Holmes also dissented in *Olmstead* stating that courts are likely to misstep when dissecting statutory language narrowly where the language expounds on a policy greater than the text itself.[177] Justices Brandeis and Holmes's ideas that statutes, when protecting our critical privacy interests, must be construed broadly or risk error remains true because technology continually outpaces our courts. Thus, narrow construction leaves citizens without remedy.

The evolution of Fourth Amendment privacy, as *The Right to Privacy* predicted, continued to evolve as our society evolved as well.[178] Though initially the Fourth Amendment was focused on property rights, *Katz v. United States* enlarged the Amendment's scope by stating that its power does not "turn upon the presence or absence of a physical intrusion."[179] This enlarging of scope is key because a test based on traditional trespass proves wholly inadequate and irrelevant for evaluating an invasion of privacy committed with zero physical intrusion, such as the surreptitious collection of facial recognition data.[180]

Be that as it may, the Supreme Court took troubling positions post-*Katz* in regards to public versus private space surveillance: searches that occurred in public were constitutional, contrasted with private area searches, which were labeled unconstitutional.[181] This distinction between public and private areas matters because photographs used to extract facial recognition data often exist in a public space, i.e., the internet.[182]

This concern was addressed in both *Jones* and *Carpenter*.[183] When Antoine Jones, a District of Columbia nightclub owner, was suspected of trafficking narcotics, the Federal Bureau of Investigation (FBI) and

---

177 *Id.* at 485 (Holmes, J., dissenting).

178 *See* Warren & Brandeis, *supra* note 164, at 193–94.

179 United States v. Jones, 565 U.S. 400, 414 (2012) (Sotomayor, J., concurring) (quoting Katz v. United States, 389 U.S. 347, 353 (1967)).

180 *See id.* at 414–15.

181 Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 508–09 (2012). Notably, Justice Stewart writes for the Court that the "Fourth Amendment protects people, not places," but this sentiment proves untrue for some time. Katz v. United States, 389 U.S. 347, 351 (1967).

182 The internet is surely a different type of public environment than *Katz*'s public phone booth. *See Katz*, 389 U.S. at 348. However, it exhibits all the factors of public places, such as how anyone is free to be there at any time, albeit with some criminal law restrictions.

183 *See Jones*, 565 U.S. 400; Carpenter v. United States, 138 S. Ct. 2206 (2018).

Metropolitan Police Department installed a GPS tracking device on the car Mr. Jones used.[184] The Supreme Court, in a Justice Scalia opinion, found that the government's installation of the GPS device constituted a "search" under the Fourth Amendment's protection for "effects."[185]

The hijacking of Mr. Jones's vehicle via the GPS device invaded his privacy interests.[186] GPS monitoring created exacting records of the person's public life, thereby painting a portrait of the person's family life, political alignment, professional work, religious practices, and sexual orientation.[187] In her concurrence, Justice Sotomayor remained concerned about the potential for long-term mining of this data, and the cost and labor effectiveness that GPS monitoring affords law enforcement agencies.[188] Justice Sotomayor also expressed concern that awareness of this phenomenon will chill freedoms of association and expression because of the susceptibility of abuse by the government when mining this data.[189] Nevertheless, the Court left it unanswered whether surveillance over a weeks-long period through electronic means, without any accompanying trespass, would be an unconstitutional search or invasion of privacy.[190]

This issue is at the heart of *Carpenter*.[191] Here, the Court held that collection of one's cell site location information (CSLI) provides a comprehensive chronicle of the user's past movements constituting a

---

184 *Jones*, 565 U.S. at 402–03.

185 *Id.* at 404. Note that Justice Scalia is applying a trespassory test to find the GPS device unconstitutional—this is contrary to the reasonable expectation of privacy test created in *Katz*. *See Katz*, 389 U.S. 347; *see also* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

186 *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

187 *Id.* Justice Sotomayor also cites a Court of Appeals of New York case that discusses the disclosures made via electronic surveillance. *See* People v. Weaver, 909 N.E.2d 1195, 1199 (2009) ("Disclosed in the [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.").

188 *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring).

189 *Id.* at 416.

190 *Id.* at 412, 417–18.

191 Carpenter v. United States, 138 S. Ct. 2206 (2018).

search under the Fourth Amendment.[192] CSLI is generated because cellphones constantly scan for the best signals (closest cell sites), and connection to the signal creates a time-stamped record.[193] Like facial recognition data collected by Facebook, *Carpenter*'s "personal location information maintained by a third party" via CSLI "does not fit neatly under existing precedents."[194]

How could our cellphones theoretically compare to Facebook? Every time a friend posts a photo of you, often saying where the photo was taken and why, Facebook could potentially record a "hit" for your face.[195] That is, Facebook could potentially keep a record each time its facial recognition system thought it identified you, as well as how many of those times your friends confirmed that the algorithm worked by tagging you. Collection of those data points, like collection of CSLI, could give precise information about your personal life.[196] After all, if you did not post the photo to your Facebook, perhaps there is a reason—a privacy concern—that you sought to avoid. The *Carpenter* decision reminds us that sophistication of certain technologies, their accuracy, and their ubiquity are key factors when considering their potential to create a sum of information that enters the realm of constitutional search.[197]

When weighing solutions to the issues we face today regarding our privacy and its connection to technology, Justice Alito's concurrence in *Riley* offers food for thought.[198] Two persons are arrested: Person A has a paper copy in their pockets of their monthly phone bill listing incriminating phone calls and a physical copy of an incriminating picture, and Person B has a cellphone in their pocket with the same incriminating phone log and incriminating photos saved to their cellphone.[199] Under the *Riley* holding, Person A's evidence will be seized without a warrant, but Person B's evidence is out.[200] This discrepancy is a

---

192 *Id.* at 2211.

193 *Id.*

194 *Id.* at 2214.

195 I have not found any evidence that Facebook actually does this, but it does not seem so implausible as to require exclusion from this argument.

196 Facial recognition systems are getting more and more accurate. *Infra* Section II.C.3.

197 *Carpenter*, 138 S. Ct. at 2218–19.

198 Riley v. California, 573 U.S. 373, 403–08 (2014) (Alito, J., concurring).

199 *Id.*

200 *Id.*

clear inequity in the administrability of the law. However, Justice Alito sees no other way to protect Person B's phone, storing sensitive, personal information, because developing nuanced rules would take years, and the speed of technological advancement will not stop for a court to decide how to deal with technology during arrests.[201] We are faced with the same decisions and problems in the biometric sphere, and Justice Alito provides clear footing for protecting privacy.

2. *Griswold*'s Affirmation of a Privacy Interest

In the famous *Griswold v. Connecticut* suit, the Supreme Court examined whether a fundamental interest of a right to privacy, a right to be let alone, would be enough to overcome state legislation. The answer is yes.[202]

Justice Douglas, writing for the *Griswold* Court, presents a series of cases in which certain rights, such as freedom of association and the right to educate a child as the parent sees fit, are not enumerated in the Bill of Rights, but are nevertheless protected by it.[203] To Justice Douglas, the results of these cases indicate that the Amendments have "penumbras, formed by emanations from those guarantees that help give them life and substance."[204] Those penumbras are "zones of privacy" extending from the guarantees of the Bill of Rights.[205] For Justice Douglas, this theory justifies finding Connecticut's law forbidding use of contraceptives

---

201 *Id.* I can only posit that judicial sensitivity to these issues is motivated by the simple fact that they too have smartphones full of banal things they would rather not share. For example, would a Supreme Court Justice want photos of their children available all over the internet? Or text messages that clearly depict a trusted confidant? Or their call logs to each other to be dissected by TMZ?

202 *See generally* Griswold v. Connecticut, 381 U.S. 479 (1965).

203 *Id.* at 481–84; *see also* Poe v. Ullman, 367 U.S. 497, 515–22 (1961) (Douglas, J., dissenting). Note that in *Griswold*, Justice Douglas delivers a plurality opinion; Justice Goldberg, the Chief Justice, and Justice Brennan submit a concurrence; Justice Harlan enters his own concurrence; Justice White also concurs; and Justices Black and Stewart dissent individually and in support of each other. *See generally Griswold*, 381 U.S. 479.

204 *Griswold*, 381 U.S. at 484 ("The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance.").

205 *Id.* ("Various guarantees create zones of privacy.").

unconstitutional.[206] Regulation of contraception in a marital bed intrudes upon a zone of privacy older than the Bill of Rights, according to Douglas.[207] In a concurring opinion,[208] Justice Goldberg finds this zone of privacy within the Ninth Amendment via incorporation through the Fourteenth Amendment.[209] Justice Harlan also concurs, but grounds the privacy interest in the Fourteenth Amendment alone, finding the "zones of privacy" theory unnecessary.[210] No matter where the privacy interest is found, the baseline is that a privacy interest exists.

C. *Offering Further Support for Broad Construction of Biometric Privacy Laws Via Least-Cost-Avoider Theory, Lack of Incentives to Regulate, and Rapid Growth and Ubiquity of Biometric Technology*

1. Least-Cost-Avoider Theory Supports Corporations Taking Greater Responsibility When Collecting Biometric Data

Law and economics scholars use the least-cost-avoider theory to create efficient rules for liability purposes.[211] This theory asks one to consider which party is better suited to take ex ante precautions, and

206 *Id.* at 485–86.

207 *Id.*

208 Justice Goldberg was joined by the Chief Justice and Justice Brennan. *Id.* at 486 (Goldberg, J., concurring).

209 *Id.* at 486–95; *see also* U.S. CONST. amend. IX ("The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."); U.S. CONST. amend. XIV, § 1 ("All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.").

210 *Griswold*, 381 U.S. at 500 (Harlan, J., concurring) ("While the relevant inquiry may be aided by resort to one or more of the provisions of the Bill of Rights, it is not dependent on them or any of their radiations. The Due Process Clause of the Fourteenth Amendment stands, in my opinion, on its own bottom.").

211 George M. Cohen, *The Negligence-Opportunism Tradeoff in Contract Law*, 20 HOFSTRA L. REV. 941, 945–47 (1992).

assigns the liability to the better-suited party.[212] A finding of liability creates incentives for parties in similar situations to take precaution in their own dealings.[213] To recap, this theory simply examines which party could avoid harm at the cheapest price.[214] The fact that in biometric collection the commercial entity has far greater knowledge of the security and privacy risks than the individual end-user of Facebook, Google, or Shutterfly does should be a dispositive factor in assigning liability to those entities.[215] Though the least-cost-avoider theory stems from accident law, it can provide some policy basis for placing a greater onus on commercial collectors of biometric information.[216]

2. Lack of Incentives to Regulate in a Booming Market

Information is power in the roaring biometrics business.[217] The global market for biometric systems is estimated to reach fifty billion dollars by 2025.[218] In testimony before a Senate subcommittee, Professor

---

212 *Id.* Mr. Cohen is summarizing Guido Calabresi, one of the popular proponents of Law and Economics. *See* GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS (1970).

213 Cohen, *supra* note 211.

214 Stephen G. Gilles, *Negligence, Strict Liability, and the Cheapest Cost-Avoider*, 78 VA. L. REV. 1291, 1308 (1992).

215 *Id.* at 1307.

216 Least-cost-avoider theory found its footing in accident law thanks to law and economics scholars. Cohen, *supra* note 211, at 944–45; *see also* Guido Calabresi, *The Decision for Accidents: An Approach to Nonfault Allocation of Costs*, 78 HARV. L. REV. 713 (1965); Guido Calabresi, *Some Thoughts on Risk Distribution and the Law of Torts*, 70 YALE L.J. 499 (1961).

217 *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy Tech. and the Law of the S. Comm. on the Judiciary*, 112th Cong. (2012) [hereinafter *Acquisti Statement*] (prepared statement of Alessandro Acquisti, Associate Professor, Heinz College and Cylab, Carnegie Mellon University, Pittsburgh, Pennsylvania).

218 *See* GRAND VIEW RESEARCH, INC., BIOMETRICS TECHNOLOGY MARKET ANALYSIS REPORT BY END-USE (GOVERNMENT, BANKING & FINANCE, TRANSPORT/LOGISTICS, DEFENSE & SECURITY), BY APPLICATION (AFIS, IRIS, NON-AFIS), AND SEGMENT FORECASTS, 2018–2025 (2018); *Biometrics Technology Market Size Worth $59.31 Billion by 2025: Grand View Research, Inc.*, PR NEWSWIRE (Apr. 18, 2019), https://www.prnewswire.com/news-releases/biometrics-technology-market-size-worth-59-31-billion-by-2025-grand-view-research-inc-300834463.html [https://perma.cc/8CYX-7254]; Chris Burt, *Biometrics Market to Approach $52 Billion by 2023 as Facial Recognition and Banking AI Expand*, BIOMETRICUPDATE.COM (Apr. 12, 2019), https://www.biometricupdate.com/201904/biometrics-market-to-approach-52-billion-by-2023-as-facial-recognition-and-banking-ai-expand [https://perma.cc/CQE4-3SXJ].

Alessandro Acquisti of Carnegie Mellon University gave two reasons for why the biometrics industry will not self-regulate.[219] First, facial biometric data is valuable.[220] Because of the permanence and ubiquity of facial identification, there is a race to be the first to provide effective, accurate facial recognition services to others.[221] Tough competition is a breeding ground for poor choices in the name of greed.[222]

Secondly, the biometric market currently indicates that firms are willing to engage in more invasive facial recognition.[223] Professor Acquisti posits that the facial recognition applications we see now are "bridgeheads" created to coax consumers into accepting increasingly far-reaching applications.[224] Professor Acquisti uses Facebook as an example.[225] Facebook has constantly tweaked its user privacy settings and defaults inching consumers closer to disclosing and sharing vastly more data.[226] In this situation, information is used to influence the Facebook user in ways that Facebook can monetize via advertisement revenue.[227] Professor Acquisti's concerns about the power of information and how greed can affect our data security and privacy are central to the notion that the biometrics industry will not self-regulate.[228]

---

219 *See Acquisti Statement*, *supra* note 217.

220 *Id.*

221 *Id.*

222 *Id.*

223 *Id.*

224 *Id.* ("Current users of face recognition are limited not just by computational costs but by fear of consumer backlash. These initial applications that we see, however, could be considered as 'bridgeheads.' In a way, they are designed to habituate us into accepting progressively more expansive services.").

225 *Id.*

226 *Id.*

227 *See id.* ("In the 21st century, the wealth of data accumulated about individuals and the staggering progress of behavioral research in using the data to influence individual behavior make it so that control over personal information implies power over the person."); *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy Tech. and the Law of the S. Comm. on the Judiciary*, 112th Cong. (2012) (prepared statement of Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection, Federal Trade Commission, Washington, D.C.) ("Companies can also determine demographic characteristics of a face such as age and gender to deliver targeted ads in real time in retail spaces.").

228 Even if it did, it is highly unlikely that the market will do so in such an expansive way as our state laws have. *See supra* Section II.B.

3. Rapid Growth and Ubiquity of Biometrics

Professor Acquisti's concerns are not unfounded. In the last decade, growth in biometric technology has moved at a breakneck pace. The United States Department of Commerce's National Institute of Standards and Technology (NIST) has reported that the most accurate facial recognition algorithms can find matching faces in databases containing twelve million individuals—with an error rate below 0.2%.[229] NIST completed a similar study in 2014, and found facial recognition error rates ranging from 4.1% to 66.9% depending on the scenario.[230] NIST highlighted the "massive gains" in facial recognition accuracy achieved in only five years.[231]

NIST's experiments used 127 facial recognition algorithms from "commercial face recognition suppliers and one university."[232] NIST used photographs ranging from high to low quality, and used the algorithms to (1) extract facial recognition data from the photographs and (2) compare the newly extracted data to a database of tweleve million faces.[233] In essence, NIST used a photograph to produce facial geometry datapoints to test their algorithms' powers of extraction and matching accuracy.[234] As innocuous as photographs are, the unchecked power of commercial biometric recognition turns these items into ultra-sensitive datapoints. Have you considered how many websites keep a public-facing photograph of you? Most people in 2020 have multiple social media accounts, such as Facebook, Twitter, Instagram, Snapchat, LinkedIn, WhatsApp, Slack, GroupMe, TikTok, Reddit, Tumblr, Google+, and

---

229 PATRICK GROTHER, MEI NGAN, & KAYEE HANAOKA, U.S. DEP'T OF COM., NAT'L INST. OF STANDARDS & TECH., ONGOING FACE RECOGNITION VENDOR TEST (FRVT) PART 2: IDENTIFICATION 2 (2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf [https://perma.cc/9BAP-HAWV].

230 PATRICK GROTHER & MEI NGAN, U.S. DEP'T OF COM., NAT'L INST. OF STANDARDS & TECH., FACE RECOGNITION VENDOR TEST (FRVT): PERFORMANCE OF FACE IDENTIFICATION ALGORITHMS 3 (2014), https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf [https://perma.cc/4CW3-9ZB7].

231 GROTHER ET AL., *supra* note 229, at 2.

232 *Id.*

233 *Id.* NIST also used three smaller databases of "3.2 million webcam images; 2.5 million photojournalism and amateur photographer photos; and 90 thousand faces cropped from surveillance-style video clips." *Id.*

234 *See id.*

more.[235] This list does not even consider websites, like Flickr or Shutterfly, used to store photos remotely.

Again, this technology is not foreign. We interact with it every day—from mobile phones to entertainment venues to workplaces, airports, and more. You might be reading this from your cellphone that was unlocked by authentication of your fingerprint image or facial image. You may have even purchased the coffee you are drinking by authenticating your identity to your cellphone via fingerprint or facial image. Since 2013, Apple's extremely popular iPhone has included Touch ID, an electronic fingerprint recognition system.[236] Starting in 2017, Apple included Face ID, advanced facial recognition technology, in iPhones.[237] Apple's facial recognition technology is everywhere—the company sold more than 217 million iPhones in 2018 alone.[238]

Facial recognition is not reserved for iPhones, as entertainers have used it to scan arena crowds for security purposes. Ten-time Grammy Award winner Taylor Swift did just that at a May 2018 concert.[239] Swift

---

235 Andrew Perrin & Monica Anderson, *Share of U.S. Adults Using Social Media, Including Facebook, Is Mostly Unchanged Since 2018*, PEW RES. CTR. (Apr. 10, 2019), https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018 [https://perma.cc/UN5L-E328]; Rachel Lerman, *'45 Days of Ambiguity': What a U.S. TikTok Ban could mean for Users and Employees*, WASHINGTON POST (Aug. 17, 2020 2:25 PM), https://www.washingtonpost.com/technology/2020/08/17/tiktok-ban-us-faq [https://perma.cc/NWS4-3UPN] (noting that TikTok has 100 million users in the United States).

236 *Apple Announces iPhone 5s—The Most Forward-Thinking Smartphone in the World*, APPLE NEWSROOM (Sept. 10, 2013), https://www.apple.com/newsroom/2013/09/10Apple-Announces-iPhone-5s-The-Most-Forward-Thinking-Smartphone-in-the-World [https://perma.cc/5QH4-FDPV].

237 *The Future Is Here: iPhone X*, APPLE NEWSROOM (Sept. 12, 2017), https://www.apple.com/newsroom/2017/09/the-future-is-here-iphone-x [https://perma.cc/9WBM-T9S4]; Mark Gurman, *What's New in the iPhone X*, BLOOMBERG (Aug. 22, 2017), https://www.bloomberg.com/graphics/2017-apple-iphone8 [https://perma.cc/CC2D-KT6M]; Brett Molina, *New iPhones Might be Able to Recognize Your Face*, USA TODAY (Aug. 28, 2017, 10:53 AM), https://www.usatoday.com/story/tech/talkingtech/2017/08/28/new-iphones-might-able-recognize-your-face/607272001 [https://perma.cc/K4YQ-PLPV]; Luke Dormehl, *iPhone 8's Amazing Facial Recognition is Super Quick, Works in the Dark*, CULT OF MAC (Aug. 21, 2017, 7:25 AM), https://www.cultofmac.com/498426/iphone-8s-amazing-facial-recognition-super-quick-works-dark [https://perma.cc/5JNP-LE7J].

238 Apple Inc., Annual Report (Form 10-K) (Nov. 5, 2018).

239 *See Artist: Taylor Swift*, RECORDING ACADEMY GRAMMY AWARDS, https://www.grammy.com/grammys/artists/taylor-swift [https://perma.cc/H2QF-7RQL] (last visited Jan. 6, 2019); *see, e.g.*, *The Future of Entertainment*, ROLLING STONE (Dec. 10, 2018, 4:53 PM),

and her team hid facial recognition cameras inside a kiosk where concertgoers would stop to look at a highlight reel of her recent performances.[240] Swift's team used the collected data to identify her known stalkers in the crowd.[241] Ms. Swift is not the only one who believes biometrics have a place at large event venues. Entertainment behemoth Live Nation Entertainment recently invested in Blink Identity.[242] Blink Identity is a new facial recognition startup that claims to identify people walking by in a moment's notice—without those people having to look straight into a camera.[243] The use of this technology matters because Live Nation Entertainment connects over 580 million fans to concerts in nearly forty-six countries.[244] The possibility that biometric technology could be deployed against so many potentially unwitting persons across the globe is highly concerning.

Other large venues are also tapping into biometric technology. Clear, a New York City-based company, claims to have three million members using biometric authentication—instead of government IDs or event tickets—to gain access to more than forty airports, arenas, and stadiums across the country.[245] Workplaces are even using the new technology to prevent fraudulent clock-ins. Buddy punching, or clocking

---

https://www.rollingstone.com/culture/culture-lists/future-entertainment-technology-music-tv-movies-760659/facial-recognition-concert-security-760696 [https://perma.cc/L9QY-XMQJ]; Stefan Etienne, *Taylor Swift Tracked Stalkers with Facial Recognition Tech at Her Concert*, THE VERGE (Dec. 12, 2018, 3:04 PM), https://www.theverge.com/2018/12/12/18137984/taylor-swift-facial-recognition-tech-concert-attendees-stalkers [https://perma.cc/B2PL-MNY6]; Madison Malone Kircher, *Look What You Made Taylor Swift Do: Use Facial-Recognition Technology*, NEW YORK (Dec. 12, 2018), http://nymag.com/intelligencer/2018/12/taylor-swift-scanned-audience-using-facial-recognition-tech.html [https://perma.cc/P4DD-2DRU].

240 ROLLING STONE, *supra* note 239.

241 *Id.*

242 *See* Lake Schatz, *Ticketmaster Invests in Facial Recognition Technology Company*, CONSEQUENCE OF SOUND (May 8, 2018, 5:16 PM), https://consequenceofsound.net/2018/05/ticketmaster-invests-in-a-facial-recognition-technology-company [https://perma.cc/9YLH-AXWW].

243 *Id.*; Jacob Kastrenakes, *Ticketmaster Could Replace Tickets with Facial Recognition*, THE VERGE (May 7, 2018, 6:41 PM), https://www.theverge.com/2018/5/7/17329196/ticketmaster-facial-recognition-tickets-investment-blink-identity [https://perma.cc/J533-M2YB].

244 *See* Live Nation Entm't, Inc., Annual Report (Form 10-K) (Feb. 27, 2020).

245 *2019 Disruptor 50 Full Coverage: 22. Clear*, CNBC (May 15, 2019, 5:55 AM), https://www.cnbc.com/2019/05/14/clear-2019-disruptor-50.html [https://perma.cc/4L9J-3EY7]. Whether Clear is acting in place of the government and could be held to the Fourth Amendment is a question for another day.

in on behalf of a fellow employee, costs U.S. employers more than $373 million every year.[246] Private companies have stepped in to provide a biometric solution. One company, Workwell Technologies, offers biometric timekeeping services that track over a million employees.[247] Apple, Taylor Swift, Clear, and Workwell have something in common. They are exploiting the growing biometrics market with little concern for individual privacy.

4. Greater Protection of Biometric Data is Not Unheard of: *Bearder v. State*

Finally, a Minnesota case about the definition of genetic information is a thought-provoking comparison for our biometric data collection issue. In *Bearder v. State*, the parents of twenty-five children whose blood was collected for Minnesota's newborn screening program alleged that Minnesota shared the children's blood samples for non-program testing in violation of the Minnesota genetic privacy law.[248] The newborn screening program tested for congenital diseases, and typically used seventy percent of the blood sample.[249] Minnesota retained the leftover sample indefinitely unless new parents requested destruction.[250] By 2008, there were nearly one million samples in storage dating back over ten years.[251] Over 50,000 samples were used in studies beyond the newborn screening program. In 2006, the Minnesota legislature amended the Minnesota Government Data Practices Act to include regulation of

---

246 *What is Buddy Punching and How to Prevent It: Why Buddy Punching Costs U.S. Employers $373 Million a Year and What You Can Do About It*, TSHEETS, https://www.tsheets.com/resources/prevent-buddy-punching [https://perma.cc/VUD6-P57J].

247 Te-Ping Chen, *Workers Push Back as Companies Gather Fingerprints and Retina Scans: Lawsuits Challenge Firms Over How Biometric Data Gets Collected and Stored*, WALL STREET J. (Mar. 27, 2019 10:52 AM), https://www.wsj.com/articles/workers-push-back-as-companies-gather-fingerprints-and-retina-scans-11553698332 [https://perma.cc/3RKD-ALVZ].

248 Bearder v. State, 806 N.W.2d 766 (Minn. 2011). The collection of DNA by third parties and its repercussions for all genetically related parties is explored by fellow *Cardozo Law Review* member Jesse Kitnick. Jesse Kitnick, Note, *Killer's Code: Familial DNA Searches Through Third-Party Databases under Carpenter*, 41 CARDOZO L. REV. 855 (2019).

249 *Bearder*, 806 N.W.2d at 770.

250 *Id.*

251 *Id.* at 770–71.

genetic information.[252] The parents argued that this genetic privacy law requires the State to obtain consent before disseminating newborn blood samples beyond the initial newborn screening program's purposes.[253] The State disputed this argument, asserting that the blood samples were not protected genetic information under the law.[254]

The Supreme Court of Minnesota first looks to the statutory language. The statute has two definitions for genetic information, and the court focuses on the second one.[255] The second definition reads "'Genetic Information' also means medical or biological information collected from an individual about a particular genetic condition that is or might be used to provide medical care to that individual or the individual's family members."[256] The court finds it "self-evident" that biological information includes blood samples.[257] The court highlights that DNA is the key because its presence in the blood samples is the information that brings the sample within the ambit of the genetic privacy law.[258] Thus, the State must procure written, informed consent to further disseminate the blood samples beyond the scope of the newborn screening program.[259] In summary, the Supreme Court of Minnesota held that a precursor to genetic data (DNA), a blood sample, is considered genetic information, and is protected with the same fervor as a blood test result.

The *Bearder* case tells us that protection of a precursor to unique information at the same level as the unique information itself is not unprecedented. Blood samples and photographs are admittedly very different items. Everyone has visited a doctor's office and had a blood sample drawn, cut their finger on a piece of paper, and scraped their knees playing as a child. That blood is an item exclusive to our persons and contains valuable information is not a difficult concept to grasp. Applying that concept to photographs is difficult. Yet, technology is advancing faster than we understand. Today, our photographs are not just keepsake

252 *Id.* at 771.

253 *Id.*

254 *Id.*

255 The first definition of genetic information protects "the privacy of the test results, and not the specimen or source of the information." *Id.* at 772–73.

256 *Id.*

257 *Id.*

258 *Id.* at 773.

259 *Id.* at 774.

memories. Photographs can be used to extract unique, identifying information that, if compromised, cannot be remedied.[260]

CONCLUSION

Judges Norgle, Donato, and Chang initially appear to eschew the plain text of BIPA, but the story does not end there.[261] The totality of the surrounding circumstances paints a clear picture: there are many interests at play.[262] These interests—constitutional privacy, least-cost-avoider theory, lack of incentive to self-regulate, and rapid growth and ubiquity of the biometric technology—may not suffice on their own, but, when taken together, leave judges with only one decision.[263] These interests tip the scale in favor of unwitting consumers upon whom facial recognition is used to fill commercial coffers and influence consumer decision-making.

BIPA is already a touchstone in biometrics legislation, but it can also be a guide for judicial interpretation. BIPA should stand as precedent for broad judicial construction when legislatures are outpaced by technology. Even if this construction leads to inequitable results, there may not be any practical alternative.[264] The interests of justice and privacy require the courts to provide a remedy when commercial entities overstep their boundaries in an effort to monetize our most sensitive feature: our faces.

---

260 *See*, *e.g.*, BIPA, 740 ILL. COMP. STAT. 14/5(c) (2008).

261 *Supra* Section II.A.

262 *Supra* Part II.

263 *Supra* Part II.

264 *See* Riley v. California, 573 U.S. 373, 407 (2014).