You Have the Right to Remain Private: Safeguarding Biometric Identifiers in Civil and Criminal Contexts

Sarah Hunt-Blackwell*

I. INTRODUCTION

Technology, with all its conveniences and advancements, affords us a world reminiscent of an episode of *The Jetsons*. We can see and speak to people across the world, send emails and review documents, and capture and share our most cherished moments all through handheld devices. We can tell household robots to play our favorite song or control the temperature in the room. Ease and access are at our fingertips in ways they never were before, making technology seem like the answer to our first-world woes. Unfortunately, the flip side of the proverbial coin reveals more sinister effects of the technologies we have come to rely on. Our smartphones' capabilities require us to store our face and fingerprints on the devices, and household robots are wholly ineffective without the ability to recognize our voices.

---

* © 2022 Sarah Hunt-Blackwell, Senior Business Editor, Volume 24, *Tulane Journal of Technology and Intellectual Property*, J.D. candidate 2022, Tulane University Law School; B.A. 2016, Communication Studies, Vanderbilt University. The author would like to thank her parents, Shelley and Byron, for their unconditional love and encouragement, her close friends for their support, and the members of the *Tulane Journal of Technology and Intellectual Property* for their dedicated work.

Since identifiers like our faces, fingers, and voices are used on personal devices in our personal lives, there isn't much to worry about, right? It is easy to diminish the privacy threats surrounding technology use because, after all, what are the chances that our identifiers will be taken, stored, and used against us? Ask Nijer Parks, a New Jersey resident, or Michael Oliver, a citizen of Detroit, both of whom were wrongfully arrested based on images that were captured and stored in a database of over three billion photos.[1]

Voice, face, palm, and iris or retinal recognition encompass the field of biometric technology.[2] Our individual, unique features are the identifiers our devices utilize for operation.[3] They are also the identifiers that private businesses and government agencies use to gather information about consumers and constituents.[4] And, in the cases of Nijer Parks and Michael Oliver, biometric identifiers become the basis for criminal investigations that lead to filed charges and arrests.[5] Despite growing prominence and expanding capabilities, only a handful of states have legislation that regulates the acquisition, use, and distribution of biometric identifiers.[6] There is no federal legislation regarding biometric technology.

This Comment compares the effectiveness of existing biometric privacy statutes and explores the need for federal law that protects tech users' right to privacy and safeguards against criminal injustice. Part II addresses privacy regulations in four states and analyzes pending litigation. Part III examines the use of biometrics in criminal cases. Specifically, this section highlights misidentification and its disproportionate impact on the Black community. Lastly, Part IV assesses the elements needed for a successful federal solution using the backdrop of a proposed 2020 Senate bill.

---

1. Donie O'Sullivan, *This Man Says He's Stockpiling Billions of Our Photos*, CNN (Feb. 10, 2020), http://www.cnn.com/2020/02/10/tech/clearview-ai-ceo-hoan-ton-that/index.html.

2. *Types of Biometrics*, BIOMETRICS INST.,http://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/.

3. *See* JOESPH N. PATO & LYNETTE I. MILLETT, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES, 85-115 (2010).

4. *See id.*

5. Compl. & Demand for Trial by Jury, at 4-5, Parks v. McCormack, No. PAS-L-003672-20 (N.J. Super. L. Nov. 25, 2020); Compl. & Jury Demand, at 3-4, Oliver v. Bussa, No. 20-011495 (Mich. Cir. Ct. Sep. 4, 2020).

6. Molly K. McGinley et al., *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, 9 NAT'L L. REV. 84 (Mar. 25, 2019).

II. ANALYSIS OF EXISTING PRIVACY REGULATIONS

A. BIPA: The Biometric Trailblazer

The Illinois Biometric Information Privacy Act (BIPA) was enacted in 2008 as the United States' first statutory regulation on the acquisition and use of biometric identifiers.[7] The law came in response to the growing use of biometrics in financial transactions in Illinois, particularly in the city of Chicago.[8] In 2008, the term "biometrics" was nearly unheard of outside of technology circles, so the foresight of the Illinois legislature to create this statutory regulation was groundbreaking. Even then, the legislature understood the importance of preserving privacy in the mysterious and evolving field of biometric technology.[9] As the legislative intent indicates, biometric identifiers are unchangeable and uniquely specific.[10] No two identities are the same and accessing individual identifiers through this technology could open the floodgates of fraud, identity theft, and general misuse.[11]

In addition to financial underpinnings, BIPA came at a time where technology began its rapid advancement. The year 2008 saw the release of the first MacBook Air, which was only one year removed from the first-generation iPhone.[12] While technological device usage of biometrics did not yet exist, the statute was composed to allow for growth in technology and protection of Illinois residents along the way.[13] BIPA, which is fairly short, directly addresses the "[r]etention; collection; disclosure; [and] destruction" of biometric identifiers.[14] It defines biometric identifiers as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[15]

The first provision of the statute requires private entities possessing biometric identifiers to create a "written policy" that outlines the retention and destruction framework of any collected biometric

---

7. *See generally* Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/1-99 (2008); *see also* Natalie A. Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, 10 NAT'L L. REV. 15 (Jan. 15, 2020), http://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.

8. 740 ILL. COMP. STAT. 14/5(a)-(b).

9. *Id.* 14/5(f).

10. *Id.* 14/5(c).

11. *See id.*

12. Samuel Gibbs, *40 Years of Apple—In Pictures*, GUARDIAN (Apr. 1, 2016, 3:15 PM), http://www.theguardian.com/technology/gallery/2016/apr/01/40-years-of-apple-in-pictures.

13. *See* 740 ILL. COMP. STAT. 14/5.

14. *Id.* 14/15.

15. *Id.* 14/10.

information.[16] Transparency was critical in the development of this law, even more so than regulating the actual process of acquiring the information. There was also the insinuation that biometric information should not be stored indefinitely.[17] The destruction scheme requirement suggests that not only did the legislature anticipate short-term, temporary use of biometric information, but that it was also seemingly encouraged.[18]

The regulatory structure of the statute is simple: acquisition of biometric information is prohibited without a private entity first providing written notice or receiving written consent from the individual; a private entity must share the purpose and duration of use; biometric information may not be sold, leased, or traded; disclosure or redisclosure of the information is prohibited, barring select exceptions; and biometric information must be handled with reasonable care and in the same or heightened manner as the entity handles other private information.[19] Again, transparency is key. BIPA places the onus of biometric integrity on the private entity and ensures that individuals can actively choose whether to have their information shared.

Perhaps the most revolutionary aspect of BIPA is the right of action provision, which awards damages up to $5,000 per violation to "[a]ny person aggrieved by a violation of this Act. . . ."[20] BIPA allows individuals to pursue claims under both negligence and recklessness.[21] The Illinois legislature was firm in defending biometric safety and guaranteeing that proof of infringement would result in remedy.[22] To reiterate, the foresight here is monumental. BIPA was written broadly enough to evolve with the industry but narrowly enough to enumerate guidelines for policy and recovery.[23] Fourteen years later, BIPA is not as comprehensive with regard to third-party liability, private entity retaliation against individuals, or exclusion of minors from biometric databases.[24] However, BIPA still provides the most protection, requires the most transparency, and is the only existing statute that allows for a

16. *Id.* 14/15(a).
17. *See id.*
18. *See id.*
19. *See id.* 14/15(b)-(e).
20. 740 ILL. COMP. STAT. 14/20.
21. *Id.* 14/20(1)-(2).
22. *See id.*
23. *See* 740 ILL. COMP. STAT. 14/5, 14/20.
24. *See infra* 27-40 and accompanying text.

private right of action.[25] The statutes that followed in Texas, Washington, and California have BIPA to thank for pioneering such critical legislation.

B. Regulatory Developments

The year after BIPA was enacted, Texas became the next state to implement a biometric privacy statute.[26] The Capture or Use of Biometric Identifier Act of 2009 similarly requires private entities to notify or receive consent from individuals before acquiring their biometric information.[27] Also intended for protection in commercial settings, the Texas statute differs from BIPA in two noteworthy ways. First, there is no requirement for the private entity to reveal the purpose and duration of use.[28] Second, and most concerning, are the exceptions permitted for the sale, lease, and disclosure of biometric information.[29] Individuals can only consent to these actions for purposes of identification in the event of "disappearance or death."[30] Additionally, disclosure of biometric information does not require consent or notice if it is disclosed to law enforcement "for a law enforcement purpose in response to a warrant. . . ."[31]

The law enforcement component of the statute is significant because it is vague and grants law enforcement agencies *carte blanche* access to biometric information under the guise of a warrant.[32] There is no explanation of the type of warrant to which the statute refers.[33] An arrest warrant? A search warrant? Failing to specify the types of warrants—as well as the aforementioned "law enforcement purposes"—leaves the door wide open for law enforcement agencies to assert subjective, inconsistent interpretations of the law.[34]

Further, assuming an arrest warrant falls under the purview of this exception, law enforcement agencies have the ability to identify and seize individuals in a way that they would not otherwise have. Imagine

---

25. *See* 740 ILL. COMP. STAT. 14.
26. *See generally* Capture or Use of Biometric Identifier Act, TEX. BUS. & COM. CODE § 503.001 (2009).
27. *Id.* § 503.001(b)(1)-(2).
28. *See id.*
29. *Id.* § 503.001(c)(1).
30. *Id.* § 503.001(c)(1)(A).
31. *Id.* § 503.001(c)(1)(D).
32. *Id.*
33. *Id.*
34. *Id.*

an instance where an arrest warrant is issued in Texas for a man who has never been in contact with law enforcement. His identity is not in the agency's dossier, so officers do not know what the man looks like. Before the advent of biometric technology, the officers would have to identify the man based on general descriptions and investigative techniques.[35] Now, the officers can simply solicit an image of the man's face without his consent.[36]

Washington state's biometric legislation, the Washington Biometric Privacy Act of 2017, raises comparable issues.[37] The statute allows for the sale, lease, and disclosure of biometric information in preparation for litigation or in response to participation in the judicial process.[38] Here, does litigation preparation reference discovery? And what, exactly, constitutes participation in the judicial process? Participation as a plaintiff or defendant? Participation as a witness? If the inference is that the exception covers all the above, again, the provision is a free for all, of sorts. Conversely, if there are scenarios that do not apply, the statute fails to make any clear distinction.

Like BIPA, though, Washington's statute requires that private entities receive notice or consent before acquiring individuals' biometric information.[39] The statute is also the first to address third-party liability, allowing the disclosure of information to third parties who "contractually promise" not to redisclose the information.[40] Earlier in 2021, Washington senators introduced a general privacy act, the Washington Privacy Act of 2021 (WPA), which protects the state's residents from non-commercial privacy infringements.[41] The 2021 bill's language regarding law enforcement compliance is much clearer than the language of the 2017 bill.[42] It thoroughly outlines the ways personal information can be used in civil and criminal contexts, lists the types of offenses for which the

35. *See* Stephen Mayhew, *History of Biometrics*, BIOMETRIC UPDATE (Feb. 1, 2018), http://www.biometricupdate.com/201802/history-of-biometrics-2.

36. *See id.*

37. *See generally* Biometric Identifiers Act, WASH. REV. CODE §§ 19.375.010–19.375.900 (2017).

38. *Id.* § 19.375.020(3)(f).

39. *Id.* § 19.375.020(1).

40. *Cf. id.* § 19.375.020(3)(e), *with* TEX. BUS. & COM. CODE ANN. § 503.001 (2009), *and* 740 ILL. COMP. STAT. 14/15 (2008).

41. David Stauss, *2021 Washington Privacy Act Released*, JDSUPRA (Jan. 11, 2021), http://www.jdsupra.com/legalnews/2021-washington-privacy-act-released-2010940/.

42. *Cf.* S.B. 5062, 67th Leg., Reg. Sess. §§ 110, 202(2) (Wash. 2021), *with* WASH. REV. CODE § 19.375.040(3) (2017).

information could be used, and delineates which parts of the judicial process to which the information applies.[43]

Other components of WPA deviate from the Washington Biometric Privacy Act in that they change the process by which residents exercise their rights against private entities.[44] Instead of a prior consent or notice requirement, WPA permits "controllers" to take biometric information first and Washington residents can later submit information requests to determine what information the controller has obtained.[45]However, the controller must publish a privacy policy that informs individuals about the categories and purpose of the information it acquires, the process for submitting information requests, and the types of information the controller shares with third parties.[46]

WPA is structured similarly to the California Consumer Privacy Act of 2018 (CCPA).[47] Intended for commercial purposes, the CCPA also takes a post-acquisition approach that allows California consumers to identify whether or not their information has been collected through submission of a request.[48] Businesses must maintain and update a privacy policy that notifies consumers of the request submission process as well as the categories of information gathered in the preceding twelve months.[49] The CCPA is the first of the privacy statutes to prohibit retaliation against consumers who "opt-out" of information acquisition.[50] Proposed updates to the bill in 2020 considerably alter the statutory language.[51]

From BIPA in 2008 to the CCPA in 2018, the societal prominence of biometric technology is evident from the expansion of statutory regulations.[52] What began as consumer privacy protection in financial transactions has burgeoned into privacy management that prioritizes corporate access to biometric information.[53] Each of the existing statutes

43. S.B. 5062, 67th Leg., Reg. Sess. § 110 (Wash. 2021).
44. *Id.* § 104.
45. *Id.*
46. *Id.* §§ 107(i)-(iv).
47. *See generally* CAL. CIV. CODE §§ 1798.100-.199 (2020).
48. *Id.* § 1798.100(c).
49. *Id.* § 1798.130(a)(5).
50. *Id.* § 1798.125(a)(1).
51. *Cf. id.* §§ 1798.100-.199 (2020), *with* California Privacy Rights Act, Proposition 24 (Cal. 2020) (codified at CAL. CIV. CODE §§ 1798.100-.199 (Nov. 3, 2020)) (effective Jan. 1, 2023).
52. *See* CAL. CIV. CODE §§ 1798.100-.199 (2020).
53. *Id.* § 1798.140(L)(2).

are similar, but their variances make compliance especially difficult for national and international companies.[54]

Table 1: Existing State Biometric Privacy Legislation

	BIPA	TX	*WA	*CCPA
Prior notice or consent to acquisition required	X	X	X	
Required notice of purpose and length of acquisition	X			Purpose
Sell, lease, trade, or profit of information prohibited	X	Limitations	Limitations	Limitations
Consent to disclosure/ redisclosure	X		X	
Destruction of information	3 years	1 year		
Private right of action	X		Included in WPA 2021	
Protection against retaliation				X

**Updates to the law are pending.*

C. BIPA In Action: Clearview AI Cases

Clearview AI is a company that not many people know about, but many people have been affected by its operation.[55] Unbeknownst to the approximately 233 million social media users in the United States, Clearview AI has been pulling individuals' photos from their personal social media accounts and storing the photos in a database—a process called "scraping."[56] Clearview AI is not only scraping images from social

54. *Cf.* CAL. CIV. CODE §§ 1798.100-.199 (2020), *with* California Privacy Rights Act of 2020, Proposition 24 (Cal. 2020) (codified at CAL. CIV. CODE §§ 1798.100-.199 (2020) (effective Jan. 1, 2023).

55. Chris Burt, *Clearview AI CEO Claims First Amendment Protects Scraping of Public Biometric Data*, BIOMETRIC UPDATE (Feb. 5, 2020), http://www.biometricupdate.com/202002/clearview-ai-ceo-claims-first-amendment-protects-scraping-of-public-biometric-data.

56. *Number of Social Network Users in the United States from 2017 to 2026*, STATISTA (Aug. 5, 2021), http://www.statista.com/statistics/278409/number-of-social-network-users-in-the-

media, but it also scours the internet for any articles or other digital media content that includes individuals' photos.[57] During a controversial exposé in 2020, Clearview AI founder Hoan Ton-That revealed that the company has a database of more than 3 billion photos of people that they have obtained without those individuals' knowledge or consent — a fact that is quite disturbing.[58] Even more disturbing is the fact that Clearview AI sells the database to law enforcement agencies across the country for criminal identification purposes.[59] More than 600 law enforcement agencies currently access the database, either through paid contracts or free trials, including the Chicago Police Department.[60] As of last year, an "opt-out" option allowing individuals to exclude their photos from the Clearview AI database was not available.[61]

After Clearview AI's work was revealed, the major social media platforms—Twitter, Facebook and Instagram—sent cease and desist letters to the company, claiming that its practice violated their respective Terms of Service (ToS).[62] Additionally, numerous class action lawsuits were filed.[63] Clearview AI is now embroiled in at least seven class actions, the first of which, *Mutnick v. Clearview AI, Inc. et al*, was filed in Illinois under BIPA.[64] In the complaint, plaintiff David Mutnick asserts that Clearview AI operates as "massive surveillance state" that is "laying the groundwork for a 'dystopian future.'"[65]

Under BIPA, Mutnick's complaint alleges recklessness and negligence.[66] Mutnick, along with the other class members, seeks injunctive relief as well as the monetary damages of up to $5,000 as outlined by the law.[67] The complaint alleges that Clearview AI violates BIPA for failure to provide notice or receive consent before acquiring biometric identifiers, and/or selling and disclosing such biometric information, and for the absence of a written policy detailing retention

---

united-states/ (last visited Oct. 7, 2021); *see* O'Sullivan, *supra* note 1; *see also* Burt, *supra* note 55.

57. O'Sullivan, *supra* note 1.

58. *See id.*

59. *See id.*

60. Burt, *supra* note 55.

61. *Id.*

62. O'Sullivan, *supra* note 1.

63. *See* Lauren Kitces, *Lessons from a Failed Intervention*, 10 NAT'L L. REV. 184, (July 2, 2020).

64. Class Action Compl., at 4, Mutnick v. Clearview AI, Inc., Case No. 20 C 0512, 0846 (N.D. Ill. Aug. 12, 2020); *see also* Kitces, *supra* note 63.

65. Class Action Compl., *supra* note 64, at 2.

66. *See id.* at 23-26.

67. *See id.* at 23-27.

and destruction guidelines.[68] Of the five BIPA provisions, Mutnick alleges that Clearview AI violates the first four.[69] Because Clearview AI does not provide an opt-out option and the overall processes maintained by the company are ambiguous, plaintiffs do not even have enough information to justifiably assert BIPA's fifth provision, which is the reasonable care standard and protection of confidentiality.[70] Although proof of harm is not required to proceed with BIPA violation claims, Mutnick and the class members contend they have "suffer[ed] injury, [and] ascertainable losses of money and property" as a result of Clearview AI's actions.[71]

While litigation is still in process, *Mutnick* is a landmark case, and its effects will be undoubtedly colossal. If decided in favor of Clearview AI, the court will afford legal grounds for the unauthorized capture of biometric information as well as its subsequent sale and disclosure.[72] If the ruling comes down for Mutnick and the class members, Clearview AI's entire operation will be severely compromised.[73] In defense of his company, Ton-That asserts a First Amendment right to the acquisition of public biometric information.[74] Ton-That claims Clearview AI merely creates a Google-like search engine, and with substantial business and financial interests involved, the court could very well establish legal standing for the company.[75] However, the company's mission also implicates public safety interests by equipping law enforcement agencies with a technologically advanced identification tool. Here, it could be determined that the means justify the end.[76] That justification, of course, assumes the technology is accurate and effective.

68. *See id.* at 17-29.
69. *See id.* at 7-12.
70. 740 ILL. COMP. STAT. 14/15(e).
71. Class Action Compl., *supra* note 64, at 23; Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1204 (Ill. 2019) ("Proof of actual damages is not required in order to recover.").
72. *See* Class Action Compl., *supra* note 64, at 29-30.
73. *See id.* at 3-4.
74. Burt, *supra* note 55.
75. *Id.*
76. *See id.*

III. BIOMETRICS IN CRIMINAL ACTIONS

A. Dire Consequences of Misidentification

Discriminatory misidentification is not a new phenomenon in the United States.[77] Eyewitness misidentification historically skews against Black people, and reliance on facial recognition technology only perpetuates this longstanding issue.[78] In a society that already incriminates and arrests Black people at alarmingly higher rates than that of white counterparts, technological flaws in police identification databases have far-reaching—even deadly—consequences.[79] Police departments are understandably "tight-lipped" about their investigative resources, each of which are subject to genuine human error. But neither freedom nor justice should be impaired as a result of known, obvious flaws in criminal identification processes.

In February 2019, Nijer Parks, a Black man from Patterson, NJ, was arrested for a crime he did not commit in Woodbridge, NJ; almost thirty miles from his residence in Patterson.[80] The Woodbridge Police Department (WPD) used facial recognition software provided by Clearview AI to conclude that Parks was involved in an alleged assault by vehicle in January 2019.[81] After becoming aware of a warrant issued for his arrest, Parks was certain that the identification error would be resolved once he shared his credible alibi and explained that he did not have a driver's license or own a vehicle.[82] Instead, Parks was arrested and jailed for more than two weeks.[83] Parks appeared in court twice, and on both occasions professed the impossibility of his involvement in the crime.[84] The Woodbridge police officers remained adamant about Parks' guilt throughout the proceedings despite a lack of matching DNA, fingerprints, or other evidence linking him to the crime.[85]

---

77. *See* Matthew Clarke, *Racism and Wrongful Convictions*, CRIM. LEGAL NEWS (May 15, 2020), http://www.criminallegalnews.org/news/2020/may/15/racism-and-wrongful-convictions/.

78. *See id.*

79. *See id.*

80. Compl. & Demand for Trial by Jury, *supra* note 5, at 2-3; *Distance from Woodbridge, NJ to Patterson, NJ*, DISTANCE BETWEEN CITIES, http://www.distance-cities.com (search origin field for "Woodbridge, NY" and search destination field for "Patterson, NJ").

81. Compl. & Demand for Trial by Jury, *supra* note 5, at 2-3.

82. *Id.* at 3.

83. *Id.* at 4-5.

84. *See id.* at 1-5.

85. *Id.* at 4-5.

Parks brought suit against the Woodbridge mayor, chief of police, involved police officers, Middlesex Department of Corrections, and the Middlesex county prosecutor.[86] Among the claims were excessive force, false arrest, and false imprisonment.[87] The complaint criticized the WPD's sole dependence on the "faulty and illegal" facial recognition software used in furtherance of Parks' indictment.[88] Parks avers that the actions against him were rooted in racism and committed with willful malice and reckless disregard.[89]

A Detroit man, Michael Oliver, had a similar experience after he was charged with larceny by a Detroit Police Department (DPD) investigator.[90] Here, a defendant in the case worked as a teacher and was recording an altercation when someone snatched and threw his phone in May 2019.[91] The defendant retrieved his phone and, because he was recording at the time that his phone was taken, was able to obtain an image of the person from the recorded video.[92] The defendant shared the image with DPD, who then ran the image through the department's facial recognition software, Data Works Plus.[93] The software produced a false match with Oliver's image.[94] The DPD investigator issued a warrant for Oliver's arrest and concluded the investigation without conducting any further research or witness interviews.[95]

Oliver was arrested in July 2019 when he was stopped by police while driving to work.[96] Charges against Oliver were ultimately dropped, but he pursued claims against the investigator and the City of Detroit under 42 U.S.C. § 1983 and the Fourteenth Amendment Equal Protection Clause.[97] The complaint goes into great detail about DPD's use of a "flawed identification process" with knowledge that the technology is inaccurate and often misidentifies people of color.[98] Further, the complaint condemns reliance on the technology in general given its "substantial error rate among black and brown persons of ethnicity which

86. *Id.* at 1.
87. *See id.* at 6-16.
88. *Id.* at 4.
89. *Id.* at 6.
90. Compl. & Jury Demand, *supra* note 5, at 5.
91. *Id.* at 3.
92. *Id.*
93. *Id.* at 4.
94. *Id.*
95. *Id.* at 4.
96. *Id.* at 5.
97. *See id.* at 6-16.
98. *Id.* at 8.

would lead to the wrongful arrest and incarceration of people in that ethnic demographic."[99]

Another unnerving instance of misidentification in Detroit involved Robert Williams in January 2018.[100] The father of two was arrested at his home in front of his wife and young daughters on charges of first-degree theft.[101] At the police station, Williams was interrogated and held in custody for thirty hours.[102] Williams repeatedly explained that the suspect's image, pulled from video surveillance that "matched" Williams's photo in the facial recognition database, was not him.[103] DPD was forced to dismiss the charges because a previously identified eyewitness, who confirmed Williams as the suspect, was not present at the scene of the crime.[104]

Fortunately for these three men, their police encounters did not lead to injury or death, as is the case for many Black men in America.[105] Unfortunately, biometric privacy laws do not exist in New Jersey or Michigan, so their only recourse was to find applicable state law for police misconduct, pursue federal causes of action, or "chalk it up" to mistake and continue living life with the hopes that the ordeal will be a one-time mishap, as in Williams's case.[106] Despite the absence of state legislation, cases of misidentification, false arrest, and false imprisonment should not be overlooked. Parks, Oliver, and Williams are real people who have suffered horrific consequences as a result of technological error.[107]

It is one thing to use a face scan to unlock a phone, but it is something entirely different to charge and arrest people solely because face scanning software claims to have paired two images with each other. DPD's police chief attributed Williams's wrongful arrest to "poor

---

99. *Id.* at 9-10.

100. Sarah Rahal & Mark Hicks, *Detroit Police Work to Expunge the Record of a Man Wrongfully Accused with Facial Recognition*, DETROIT NEWS (June 26, 2020, 12:35 AM), http://www.detroitnews.com/story/news/local/detroit-city/2020/06/26/detroit-police-clear-record-man-wrongfully-accused-facial-recognition-software/3259651001/.

101. *Id.*

102. *Id.*

103. *Id.*

104. *Id.*

105. *See* Brita Belli, *Racial Disparity in Police Shootings Unchanged over 5 Years*, YALE NEWS (Oct. 27, 2020), http://news.yale.edu/2020/10/27/racial-disparity-police-shootings-unchanged-over-5-years.

106. *See* Compl. & Demand for Trial by Jury, *supra* note 5; *see also* Compl. & Jury Demand, *supra* note 90; Rahal & Hicks, *supra* note 100.

107. *See* Compl. & Demand for Trial by Jury, *supra* note 5; *see also* Compl. & Jury Demand, *supra* note 90; Rahal & Hicks, *supra* note 100.

investigative work" on the part of the detectives rather than a legitimate mistake with the facial recognition software.[108] However, the two are inextricably linked. If the singular tool used to identify a suspect fails to yield accurate results, any subsequent investigation of the misidentified person is "poor" because it is unfounded and baseless.[109] Additionally, failure to substantiate the identification results is not merely "poor investigative work," it is unjust and reprehensible.[110]

B. Federal Involvement

Local police departments are not the only law enforcement agencies that implement facial recognition technology in their investigative practices.[111] The country's highest federal criminal agencies—the Department of Justice (DOJ), the Department of Homeland Security (DHS), and their subsidiaries—have hundreds of millions of "unique identities" stored in the Next Generation Identification (NGI) system, Facial Analysis, Comparison, and Evaluation (FACE) Services Unit, and the Automated Biometric Identification System (IDENT).[112]

In October 2019, the national chapter of the American Civil Liberties Union (ACLU) and the ACLU of Massachusetts filed an injunction against the DOJ, FBI, and the Drug Enforcement Administration (DEA) for the agencies' failure to submit their "policies, contracts and other records" relating to their use of facial recognition technology.[113] Requested under the Freedom of Information Act (FOIA) in January 2019, the ACLU and the ACLU of Massachusetts asserted the right of the public to be informed on the agencies' acquisition, use, maintenance, and safeguard measures regarding the technology.[114] The

---

108. Rahal & Hicks, *supra* note 100.

109. *Id.*

110. *Id.*

111. *See Criminal Justice Information Services (CJIS)*, FBI, http://www.fbi.gov/services/cjis.

112. *See Fingerprints and Other Biometrics*, FBI, http://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics; *see also* Prest, *Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Phase II System*, FBI (July 9, 2018), http://www.fbi.gov/file-repository/pia-face-phase-2-system.pdf; *see also Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)*, U.S. DEP'T HOMELAND SEC. (Dec. 7, 2012), http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-06252013.pdf.

113. Compl., at 1, ACLU v. U.S. Dep't of Just., No. 1:19-CV-12242 (D. Mass., Oct. 31, 2019).

114. *Id.* at 1-2.

complaint addressed how inaccuracies can lead to a heightened risk of false arrests, particularly with people of color.[115]

C. Big Tech Involvement

In the wake of racial justice demonstrations around the country during the summer of 2020, businesses were forced to come to terms with racist policing and the ways in which their business operations exacerbate racial injustices.[116] Major technology companies like IBM, Microsoft, and Amazon were among those corporations.[117] The time had come to finally address their practice of selling facial recognition software to law enforcement agencies across the country.[118] IBM was the first of the companies to announce its decision to end the sale of "general purpose" facial recognition technology.[119] Following suit, Amazon announced a temporary halt for one year and Microsoft announced an indefinite ban on selling facial recognition technology until a national law is passed that regulates its use.[120]

Cases of misidentification at the local level coupled with the federal government's reluctance to disclose its facial recognition technology practices create serious concerns about transparency and reliability.[121] As civilians, we are very much left in the dark about where our images are pulled from, which images are pulled, what entities pulls them, where our pulled images are stored, and whether the images are shared with other entities or individuals. Moreover, facial recognition software itself is a mystery. How do the software algorithms operate? What, if any, standards exist to ensure that misidentification is nonexistent, or at the very least, kept at a minimum? How can local and federal agencies be held accountable for privacy infringement if no published standards exist? Obviously, facial recognition technology raises more questions than answers. That is why federal legislation is the most logical next step.

---

115. *Id.* at 2.

116. Isobel Asher Hamilton, *Outrage over Police Brutality has Finally Convinced Amazon, Microsoft, and IBM to Rule out Selling Facial Recognition Tech to Law Enforcement. Here's What's Going on.*, BUS. INSIDER (June 13, 2020 4:01 AM), http://www.businessinsider.com/amazon-microsoft-ibm-halt-selling-facial-recognition-to-police-2020-6.

117. *Id.*

118. *Id.*

119. *Id.*

120. *Id.*

121. *See* Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where it Falls Short*, N.Y. TIMES (Jan. 12, 2020), http://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

IV. MAKING THE CASE FOR FEDERAL LEGISLATION

Without federal legislation on biometric information gathering and biometric technology use, privacy concerns, procedural inconsistencies, and wrongful arrests will only persist. As the ACLU mentions in its complaint against the DOJ, biometrics are increasing in popularity and use, yet there is still much that we do not know about the technology itself and its implementation.[122] Studies cite the accuracy of biometric identification while omitting the fact that most biometric algorithms are modeled after the faces of white men.[123] This methodology provides more guaranteed reliability for white Americans but leaves Black Americans victim to yet another state-sanctioned disparity.

Civilly, BIPA is the only statute that allows for a private right of action in cases of biometric privacy infringement.[124] The remaining three statutes reserve the right of action to the Attorney General.[125] Criminally, victims of misidentification and wrongful arrests can bring suit under generally applicable state laws or file §1983 or Fourteenth Amendment claims.[126] These measures are unequivocally inadequate because they address biometric issues *after* a situation occurs.[127] Federal legislation is needed to proactively safeguard citizens' personal information and prevent wrongful arrests.

In 2020, United States Senators Jeff Merkley and Bernie Sanders introduced the National Biometric Information Privacy Act.[128] Mirrored very closely after BIPA, the bill requires prior notice or consent of biometric information acquisition, consent for the sale, lease, trade, or disclosure of the information, destruction of the information if it is no longer being reasonably used after one year of first acquisition, and it allows for both private rights of action as well as claims filed by attorneys general on behalf of the people.[129]

---

122. Compl., *supra* note 113, at 2.

123. Pam Greenberg, *Spotlight | Facial Recognition Gaining Measured Acceptance*, NAT'L CONF. ST. LEG. (Sept. 18, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/facial-recognition-gaining-measured-acceptance-magazine2020.aspx; Hamilton, *supra* note 116.

124. 740 ILL. COMP. STAT. 14/20.

125. *See* TEX. BUS. & COM. CODE § 503.001(d) (2009); WASH. REV. CODE § 19.375.030(2) (2021); CAL. CIV. CODE § 1798.135(c) (2020).

126. Compl. & Jury Demand, *supra* note 5, at 6-7.

127. *Id.* at 5 (emphasis added).

128. S. 4400, 116th Cong. (2020).

129. *Id.* §§ 2, 4.

Table 2: Provisions of the National Biometric Information Privacy Act of 2020

	National Biometric Privacy Act of 2020
Required notice of acquisition before capture	X
Required notice of purpose and length of acquisition	X
Subject consents to acquisition	X
Sell, lease, trade, or profit of information prohibited	X
Subject's consent to disclosure/redisclosure of information	X
Destruction of information	1 year
Private right of action	X
Protection against retaliation	

Disappointingly, the bill does not propose any anti-retaliatory measures to protect citizens who exercise their right to exclude their information from being collected.[130] Additionally, because the bill was written from the context of commercial interactions, the bill permits disclosure of biometric information to federal, state, and local law enforcement agencies in response to "a valid warrant or subpoena issued by a court of competent jurisdiction . . . ."[131] The retaliation omission and law enforcement exception are two of the most important biometric technology considerations.

Consumers need measures in place that will prevent corporations from raising prices or otherwise administering deviant treatment to those who do not want to share their information. Passing federal legislation that lacks this provision would be a glaring disservice. In contrast, federal legislation that makes retaliation unlawful could create a covered class of people against whom violations would receive heightened

130. *See generally id.*
131. *Id.* § 3.

judicial scrutiny.[132] Courts analyze constitutionality using one of three tests: rational basis, intermediate scrutiny, or strict scrutiny; with strict scrutiny being reserved for incidents involving discrimination against minorities and other groups.[133] Considering the existing disparate treatment of Black people with biometric information, strict scrutiny review of retaliatory actions is not outside the realm of possibilities.[134]

Passing a law enforcement exception in the federal bill is disconcerting because it would legitimize law enforcement's unauthorized access to biometric information. It is established that Black people are disproportionately misidentified by facial recognition software, so permitting law enforcement agencies to obtain biometric information from private corporations is a glaring injustice.[135]

Biometric technology is indicative of how far our society has come technologically, but it also sheds light on the ways that technological advancements continue to perpetuate violations of basic rights. State legislation has started us on our way toward a society that is more protective of the few things in our lives that will never change: our faces, voices, eyes, and fingerprints.[136] While we continue discovering biometrics' capabilities and functions, now is the time to implement federal legislation that will keep us safe and maintain our right to stay private.

---

132. *See generally* 42 U.S.C. § 12203(a) (prohibiting retaliation and coercion against individuals opposing practices made unlawful in the context of equal opportunity among individuals with disabilities).

133. Kenji Yoshino, *Covering*, 111 YALE L.J. 769, 876 (2002) (discussing the levels of scrutiny courts apply).

134. *See id.*

135. *See* Hamilton, *supra* note 116.

136. *See* 740 ILL. COMP. STAT. 14/1-14/99.