DePaul Law Review

Volume 71
Issue 3 *Summer 2022*

Article 2

The Legal and Ethical Considerations of Facial Recognition Technology in the Business Sector

Samuel D. Hodge Jr.

THE LEGAL AND ETHICAL CONSIDERATIONS OF FACIAL RECOGNITION TECHNOLOGY IN THE BUSINESS SECTOR

Samuel D. Hodge, Jr.[1]

"The best way to enhance security is through facial recognition — it's going to be the standard very soon."
—Kesha Williams

Taylor Swift is one of the most commercially successful artists of all time, earning multiple Grammys, with a net worth of $360 million.[2] This success, however, comes with a price. For example, she endured the inappropriate actions of stalkers, home intruders, and obsessed fans.[3] No longer willing to tolerate this price of success, Swift took matters into her own hands. As fans entered the venues for her concerts, they were treated to kiosks that displayed rehearsal clips.[4] Little did they know that facial recognition cameras hidden inside the exhibits were secretly recording their faces.[5] These pictures were then sent to a "command post," where they were cross-referenced with a database containing the singer's known stalkers.[6]

While these safety measures seem extreme, they are not unique. The use of facial recognition technology at sporting events, concerts,

---

1. Samuel D. Hodge, Jr. is a Professor at Temple University, where he teaches law, anatomy, and forensics. He is also a member of the Dispute Resolution Institute in Philadelphia where he serves as a mediator and neutral arbitrator. Professor Hodge has authored over 145 articles in medical or legal journals, more than 500 non-refereed publications, and has written 10 books. The author wishes to dedicate this article to Professor Kevin Fandl who was going to co-author this article but tragically died before he could start working on it.

2. Avery Blank, *Why Taylor Swift Is So Influential (and How You Can Increase Your Influence)*, Forbes (Nov. 18, 2019), https://www.forbes.com/sites/averyblank/2019/11/18/why-taylor-swift-is-so-influential-and-how-you-can-increase-your-influence/?sh=40649f9e1020.

3. Lake Schatz, *Stalker Breaks into Taylor Swift's Rhode Island Mansion, Takes Off Shoes to Be "Polite"*, Consequence (Sept. 4, 2019), https://consequenceofsound.net/2019/09/taylor-swift-stalker-shoes-off-polite/.

4. Steve Knopper, *Why Taylor Swift Is Using Facial Recognition at Concerts*, Rolling Stone (Dec. 13, 2018), https://www.rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741/.

5. Stefan Etienne, *Taylor Swift Tracked Stalkers with Facial Recognition Tech at Her Concert*, The Verge (Dec. 12, 2018), https://www.theverge.com/2018/12/12/18137984/taylor-swift-facial-recognition-tech-concert-attendees-stalkers.

6. *Id.*

and public gatherings is common because of the security risks posed by terrorists.[7] Madison Square Garden, home to the New York Knicks and New York Rangers, employs a system to monitor visitors who enter the venue to identify those who pose a security threat.[8] Additionally, teams can use the technology to view a crowd to determine what music to play and track a fan's facial expressions when deciding what food and merchandise to sell.[9] The arena can even use facial recognition technology to identify, expel, and ban unruly spectators. Furthermore, keeping unwanted fans out of the complex improves the audience experience and protects fans from others.[10]

The type of device used is not indicative of its utility. For instance, a knife may be used as a cooking utensil or as a deadly weapon. Likewise, tools with greater utility can cause greater harm or confer more benefit.[11] Facial recognition technology is a very powerful instrument that has developed rapidly over the past decade but is far from perfect. It presents unique advantages and sobering drawbacks.[12] It also raises questions that go to the foundation of human rights safeguards like privacy and freedom of expression. These concerns heighten the responsibilities of those who create this technology and the businesses that employ it in their daily operations.[13] This Article will address the legal and ethical concerns involving facial recognition technology in a business setting. As this biometric system catapults society into unexplored terrain, the benefits that it provides must be balanced against its impact on privacy, data protection, and other consumer concerns.[14] After first explaining how the technology works, this Article will discuss the attempts by various governmental units to regulate the emerging field both in the United States and around the world. This

7. FACEFIRST, *Deliver the Ultimate VIP Fan Experience*, https://www.facefirst.com/industry/stadium-face-recognition/ (last visited Mar. 28, 2021).

8. Scooby Axson, *Report: Madison Square Garden Using Facial-Recognition Technology on Fans*, SPORTS ILLUSTRATED (Mar. 13, 2018), https://www.si.com/nba/2018/03/13/msg-facial-recognition-technology.

9. Kirsten Flicker, *The Prison of Convenience: The Need for National Regulation of Biometric Technology in Sports*, 30 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 985, 997 (2020).

10. *Id.* at 1003.

11. Brad Smith, *Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility*, MICROSOFT (July 13, 2018), https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/.

12. *Id.*

13. *See id.*

14. Mary J. Hildebrand et al., *Let's Face It: Facial Recognition Technology Involves More than Meets the Eye*, LOWENSTEIN SANDLER, LLP (Jan. 6, 2021), https://www.lowenstein.com/news-insights/publications/client-alerts/let-s-face-it-facial-recognition-technology-involves-more-than-meets-the-eye-privacy.

Article concludes by examining some of the litigation that has been initiated by consumers alleging that certain uses of facial recognition technology infringe upon their rights.

Introduction

Anonymity is no longer possible since most individuals have photo identifications and social media posts with pictures available for public viewing. Surveillance methods also continue to develop,[15] which has resulted in individuals being exposed to the greater use of facial recognition techniques without their awareness or permission. This system references equipment with the dual purpose of "connecting faces to identities," and permitting the "distribution of those identities across computer networks."[16] The software is primarily employed for "identification and access control or for identifying individuals who are under surveillance."[17] This technology is premised upon the idea that their inherent physical or behavioral characteristics can be used to correctly recognize every individual.[18]

I. Facial Recognition Technology

To the casual observer, facial recognition technology (FRT) is nothing more than a gimmick.[19] It allows consumers to unlock an iPhone with a glance and permits users to wonder how Facebook knew to tag a picture in which the person appeared with a group of friends.[20] However, the technology controlling these features has broader implications. Facial recognition is a type of physiological identifier, known as biometrics, that includes fingerprints, iris recognition, retina scanning, palm printing, voice recognition, and DNA matching.[21] Its applications are all encompassing and can be used in many aspects of police work, security screenings, and computer access.[22]

---

15. Samuel D. Hodge, Jr., *Big Brother Is Watching: Law Enforcement's Use of Digital Technology in the Twenty-First Century*, 89 U. Cin. L. Rev. 30, 57 (2020).

16. Kelly A. Gates, Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance 15 (2011).

17. Alexander S. Gillis et al., *Definition: Biometrics*, Tech Target, https://searchsecurity.techtarget.com/definition/biometrics (last visited Mar. 28, 2021).

18. *Id.*

19. Alex Najibi, *Racial Discrimination in Face Recognition Technology*, SITN (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

20. *Id.*

21. Gillis et al., *supra* note 17.

22. Najibi, *supra* note 19.

A. The Facial Recognition Market

During the past few decades, facial recognition systems have moved beyond the world of science fiction and movies. They have become a cornerstone of everyday life.[23] FRT can be employed to collect and process billions of pictures from the Web and databanks to provide a composite to the police, businesses, and individuals.[24]

FRT has many consumer and business applications, but the extent of its present use in a commercial setting is not yet fully known.[25] However, the biometric data field is exploding, "with the facial recognition market alone expected to generate a tantalizing $7 billion of revenue by 2024."[26] Apple, Samsung, Amazon, Google, and Microsoft have powered this growth, but startups and small to medium-sized tech firms also play a significant role.[27] The technology can have uses in customer services and marketing. However, its main application in the United States presently appears to be for "detecting characteristics (such as age or gender) to tailor digital advertising, rather than identifying unique individuals."[28] New developments and specific issues involving FRT continue to make headlines and prompt bans and lawsuits, demonstrating that facial recognition is a controversial topic that will be in the news for years to come.[29]

Despite members of society becoming more aware of the risks, numerous companies continue to quietly adopt facial recognition technologies. Business office spaces, mobile phones, online platforms, airports, business establishments, and shopping centers are all briskly increasing their use of sophisticated cameras linked to algorithmic software.[30] With the proliferation of devices packed with visual sensors, the ability to capture, analyze, and store human faces is expected to increase exponentially.

---

23. LEXOLOGY, *Risk and Reward: Increased Use of Facial Recognition Software* (June 30, 2020), https://www.lexology.com/library/detail.aspx?g=E3533e3e-2d29-4e6a-a66c-8fd0fd5c33c2.

24. *Id.*

25. U.S. GOV'T ACCOUNTABILITY OFFICE, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 6 (2015), https://www.gao.gov/products/gao-15-621 [hereinafter GAO, COMMERCIAL USES].

26. Hildebrand et al., *supra* note 14.

27. *Id.*

28. GAO, COMMERCIAL USES, *supra* note 25, at *GAO Highlights*.

29. Nicole Sakin, *Will There Be Federal Facial Recognition in the United States?*, THE PRIVACY ADVISOR (Feb. 2021), https://iapp.org/news/a/u-s-facial-recognition-roundup/.

30. Arthur Piper, *About Face: The Risks and Challenges of Facial Recognition Technology*, RISK MGMT. MAG. (Nov. 1, 2019), https://www.rmmagazine.com/articles/article//2019/11/01/-About-Face-The-Risks-and-Challenges-of-Facial-Recognition-Technology-.

B. History of Facial Recognition Software

Woodrow Wilson Bledsoe has been dubbed the father of the technology.[31] During the 1960s, he invented a system that categorized faces by using a RAND tablet. [32] This device permitted individuals to enter "horizontal and vertical coordinates on a grid using a stylus that emitted electromagnetic pulses."[33] In turn, the user could manually enter the measured locations of different facial features such as the eyes, nose, hairline, and mouth.[34] As the technology developed, it became easier to automatically identify people because of established points of interest on the face such as the shape of the lips or distance between the eyes.[35]

By the 1990s, automated algorithms were invented.[36] Following the September 11th terrorist attacks, FRT became well recognized in the public vernacular.[37] The federal government invested in the technology and provided millions of dollars in grants to state and local governments to create databases.[38] The initial research involving FRT eventually transitioned to private sector use. "What started as government-funded research in computer sciences eventually made its way into the private sector."[39] The police have a logical interest in FRT because of the need to identify suspects, and to screen people as they pass through customs.[40] The technology is also gaining traction in the private sector.[41] For example, it can identify problem gamblers in casinos, greet visitors by name at hotels, connect individuals on dating websites, spot underage drinkers, and aid in taking attendance at schools.[42]

Companies, such as Apple, have started employing multifactor biometrics and FRT to unlock smartphones.[43] Google has even created technology that can recognize a user's voice.[44] This allows the

31. FaceFirst, *The History of Face Recognition*, https://www.facefirst.com/blog/brief-history-of-face-recognition-software/ (last visited Mar. 28, 2020).

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

37. Gates, *supra* note 16, at 1–2.

38. Hodge, *supra* note 15, at 58.

39. *Id.*

40. *Id.* at 58–59, 61.

41. Jia Jen Low, *Biometrics – The Most Secure Solutions for Banking*, Tech Q (Sept. 2, 2020), https://techhq.com/2020/09/biometrics-the-most-secure-solution-for-banking/.

42. Hodge, *supra* note 15, at 59.

43. Elizabeth McClellan, *Facial Recognition Technology: Balancing the Benefits and Concerns*, 15 J. Bus. & Tech. L. 363, 372 (2020).

44. *Id.*

company's Google Home responses to be adopted to a specific user, or the device may not respond to those it fails to recognize.[45] One of the most unusual applications arises in the medical field. Scientists have created a facial recognition program that can diagnose genetic conditions, such as Down Syndrome, by scrutinizing an ordinary picture.[46] There is simply no test to identify some disorders or illnesses.[47] FRT has proven to be of benefit by spotting some medical problems that are associated with specific facial features.[48] China even employed the technology during the COVID-19 pandemic to track the movements of individuals and stop infected citizens from traveling.[49]

C. How Facial Recognition Technology Works

"Face recognition is a skill that most people rarely think about, but it is fundamental to successful social interaction."[50] However, some people have the uncanny ability to immediately recognize a person from a distance because of certain distinguishing facial features.[51] Facial recognition technology works in a similar manner but on an algorithmic scale.[52] Many people have been exposed to the workings of the system through movies, but it is seldom portrayed correctly.[53] Each application operates differently based upon proprietary algorithms. The process is conceptually similar to matching the swirls and grooves of fingerprints but much more complicated.[54] The key to identifying a person through biometrics is to map out their facial features from a photograph or video. FRT then compares the information with a database of stored images to locate a match.[55]

---

45. *Id.*

46. *Id.* at 373.

47. *Id.*

48. *Id.*

49. *Id.*

50. Brad Duchaine, *Individual Differences in Face Recognition Ability: Impacts on Law Enforcement, Criminal Justice and National Security*, AM. PSYCHOL. ASS'N (June 25, 2015), https://www.apa.org/science/about/psa/2015/06/face-recognition.

51. *See generally* Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, 34 A. B. A. CRIM. JUST. 9, 9 (2019).

52. *Id.* at 10.

53. Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It*, N.Y. TIMES WIRECUTTER (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/.

54. SUMMA LINGUAE, *Facial Recognition Technology Explained* (Sept. 27, 2021), https://summalinguae.com/language-technology/facial-recognition-technology-explained/.

55. *Id.*

Four steps are used in this identification process.[56] The first part requires a camera to capture a face, either alone or in a crowd.[57] The image is best taken when the individual is looking directly at the camera.[58] Recent developments, however, allow slight deviations from this straight-on approach.[59] A 2D or 3D template is then created, which contains the dimensions of the person's facial characteristics, such as the space between the eyes, shape of the cheekbone, depth of the eye sockets, or length and width of the nose.[60] These markers are known as nodal points, and a face will have about eighty such identifiers.[61] These markers are then analyzed, and the software will compare the template of the person's face to those stored in a database to search for a potential match.[62] This facial breakdown is subsequently transformed into a mathematical formula.[63] The nodal points become numbers in a numerical code called a faceprint.[64] Much like the distinctive arrangement of a thumbprint, each subject has their own faceprint.[65] The last step involves analyzing the nodal points, and software will compare the template of the subject's face to those in a database to locate a match.[66]

With all of the sources available to store people's images, one might wonder how large are the databases of stored pictures? "By the time you are finished reading this sentence[,] over 20,000 images were uploaded to social media . . . ." and "by the end of this sentence, algorithms can produce an index with images of [an individual] and corresponding links."[67] Business make extensive use of these "images and social media posts . . . to create databases searchable with facial recognition software."[68] Law enforcement has used FRT for about two decades.[69] However, with so many images now on social media

56. Steve Symanovich, *What Is Facial Recognition? How Facial Recognition Works?*, NORTON (Aug. 20, 2021), https://us.norton.com/internetsecurity-iot-how-facial-recognition-softwareworks.html.

57. *Id.*

58. *Id.*

59. PANDA SECURITY, *The Complete Guide to Facial Recognition Technology* (Oct. 11, 2019), https://www.pandasecurity.com/en/mediacenter/panda-security/facial-recognition-technology/.

60. *Id.*

61. Hodge, *supra* note 15, at 59.

62. Hamann & Smith, *supra* note 51, at 10.

63. PANDA SECURITY, *supra* note 59.

64. *Id.*

65. *Id.*

66. Hodge, *supra* note 15, at 59.

67. Matthew Doktor, Comment, *Facial Recognition and The Fourth Amendment in the Wake of* Carpenter *v.* United States, 89 U. CIN. L. REV. 552, 552 (2021).

68. *Id.*

69. *Id.*

networks, this technology can disclose unprecedented detail about an individual's daily activities and associations.[70] Despite the ease in accessing the Internet and social media involvement in everyday activities, studies reveal that people are unsure "how to control that."[71]

This new technology provides many benefits, such as increasing safety and security, thwarting crimes, and decreasing human interaction.[72] It can even facilitate medical assistance.[73] FRT has become a customary aspect of airport security screening for many years, assisting in identifying criminals, terrorists, and other possible threats to airlines and passengers.[74] It necessitates fewer human resources than other forms of security measures, such as fingerprinting.[75] It also does not mandate any form of physical contact or direct human interaction.[76] Rather, the technology uses artificial intelligence to create an "automatic and seamless procedure."[77]

II. The Public's Perception of Facial Recognition Technology

FRT uses are limitless because they can quickly be married with other biometric data, such as fingerprint or retinal scanning.[78] Biometric information can also be linked to personal information of any type, such as a person's tax records, political affiliations, arrest records, and other data types.[79] However, biometric technology "presents privacy risks due to its dual nature—as a digital record of automated and remote surveillance on the one hand, and an irreplaceable and privately held password to consumers' sensitive accounts on the other."[80]

Research indicates that Americans are particularly concerned when private actors collect data about them.[81] A Pew Research Center

70. *Id.*

71. *Id.*

72. David Gargaro, *The Pros and Cons of Facial Recognition Technology: Is It really Worth Risking User Privacy in the Name of Efficiency and Security?*, IT Pro (July 20, 2021), https://www.itpro.com/security/privacy/356882/the-pros-and-cons-of-facial-recognition-technology.

73. *Id.*

74. *Id.*

75. *Id.*

76. *Id.*

77. *Id.*

78. Christopher S. Milligan, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. Cal. Interdisc. L.J. 295, 305 (1999).

79. *Id.*

80. Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 624 (2019).

81. *Id.*

study demonstrated that members of society care about the security of their personal information and being free from surveillance.[82] The findings revealed that sixty-three percent of those surveyed believed it is essential to be able to "go around in public without always being identified."[83] Consumer feelings about biometrics highlight particular discomfort with the use of the technology in business locations. For instance, people are more disturbed with biometric use in malls and open public places than in an area like an airport, which is thought to be more secure.[84]

According to extensive research conducted by scholars at the University of Texas at Austin, more than half of those questioned were "very comfortable" with fingerprint scanning biometrics but only about a third were "very comfortable" with any other biometric type.[85] More importantly, most were unsure about facial recognition technology, with thirteen percent being "not at all comfortable," with its use being a full ten percent higher than any other form of biometrics.[86] GetApp, an online resource for businesses interested in software as a service, found "69 percent of consumers say they aren't comfortable with businesses using facial recognition for retail purchases, 76 percent aren't comfortable with it for emotion analysis, and 77 percent aren't comfortable with it for personalized advertising."[87] These negative perceptions stem from consumer apprehensions about the precision of the new technology and the potential misuse of the information.[88]

III. Consumer Applications of Facial Recognition Technology

Despite these negative consumer attitudes, facial recognition in the business sector is increasing. It is labeled "as an important tool in the toolbox of 'the future of shopping'" with retailers constantly experi-

82. *Id.* at 625.

83. *Id.* (quoting Mary Madden & Lee Rainie, *Americans' Views About Data Collection and Security*, Pew Res. Ctr. (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-views-about-data-collection-and-security/).

84. *Id*. at 626.

85. UT News, *New Survey on Biometric Technology Shows Consumers Are OK with Some Forms and Wary of Others* (May 3, 2018), https://news.utexas.edu/2018/05/03/new-survey-on-consumer-attitudes-toward-biometric-technology.

86. Leonard Klie, *Consumers Fear Facial Recognition*, Destination CRM (Mar. 26, 2020), https://www.destinationcrm.com/Articles/CRM-Insights/Insight/Consumers-Fear-Facial-Recognition-139934.aspx.

87. *Id.*

88. *Id.*

menting with new applications.[89] The facial recognition market was pegged at $3.72 billion in 2020, but is expected to be worth $11.62 billion by 2026.[90] Governments have been allocating substantial resources to FRT, with the United States and China leading the way.[91] Start-ups from China have invested $1.6 billion in the technology.[92] Intel and Tencent (a Chinese internet company) are working collaboratively on products that use artificial intelligence and facial recognition to "gain new insights about their customers to both elevate the users' experience and drive business transformation."[93]

Facial recognition can significantly benefit the retail industry by detecting shoplifters in real-time. It recognizes prior thieves and matches them through the shoplifter database.[94] A security team could then be dispatched to take appropriate action when a match is seen.[95] FRT can create a personalized shopping experience by recognizing the customer based upon demographics, such as age, sex, and prior buying patterns, and offering goods and products suitable to their purchasing preferences.[96] It can allow merchants to manage their employees more efficiently. The system can maintain worker attendance records, restrict improper entry to restricted parts of the premises, and promote faster check-ins and check-outs.[97] For instance, the technology can dissuade a co-worker from time-stamping another's attendance or timesheets because each person must pass a face-scanning unit to check-in and out of work.[98] Employee efficiency can be improved by observing real-time interactions and recording workers' contact with shoppers, thereby identifying critical improvement areas.[99] Some businesses have started using the technology to monitor the spread of

89. Wright, *supra* note 80, at 638.

90. MORDOR INTELLIGENCE, *Facial Recognition Market - Growth, Trends, COVID-19 Impact, and Forecasts (2022 - 2027)*, https://www.mordorintelligence.com/industry-reports/facial-recognition-market (last visited Mar. 31, 2021).

91. *See id.*

92. Wright, *supra* note 80, at 635 (quoting Jonathan Chadwick, *Tencent Teams Up with Intel for Retail Surveillance Camera and "AI Box"*, COMPUTER BUS. REV. (Nov. 2, 2018), https://techmonitor.ai/technology/emerging-technology/ai-box).

93. *Id.*

94. Vihar Soni, *Facial Recognition in Retail – Enhance In-Store Customer Experience and Improve Retailer Operations*, E INFOCHIPS (Aug. 11, 2020), https://www.einfochips.com/blog/facial-recognition-in-retail-enhance-in-store-customer-experience-and-improve-retailer-operations.

95. *Id.*

96. *Id.*

97. *Id.*

98. Hodge, *supra* note 15, at 61.

99. *See* Soni, *supra* note 94.

COVID-19 — by recognizing people who have had an interaction with someone displaying symptoms of the virus.[100]

One of the more creative applications is Amazon's new Go Stores.[101] Cameras will capture shoppers' images as they walk around the market and send the feed to some type of "central processing unit."[102] The software will immediately identify the customer and merchandise being picked up or held.[103] Selected items will automatically be added to the person's "virtual shopping cart."[104] When finished, the customer leaves the market, and the purchases will be charged to the customer's credit card.[105]

In some circles, however, commercial privacy and other concerns related to specific FRT applications may have slowed the adoption of FRT in some businesses.[106] The 2019 Biometrics Institute Annual Survey reported that "74 percent of respondents agreed that privacy concerns are holding back the market for biometrics."[107] For instance, delegates from one industry association noted that some retail establishments do not want to alienate their customers by employing facial recognition tools. One FRT vendor even expressed dismay because the firm had suffered a lower market for retail clients "that may be due to negative customer perceptions of the technology."[108]

IV. Ethical Issues with Facial Recognition Technology

FRT is an outgrowth of computer vision from the 1960s.[109] The system is premised upon machine learning and advanced mathematical processes.[110] Algorithms are pervasive in the computer age, but when it comes to facial recognition, algorithmic biases occurred within the cipher because the system was not properly exposed to a diverse database.[111] This weakness has caused injustices when surveilled indi-

100. U.S. Gov't Accountability Office, Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses 1 (2020), https://www.gao.gov/assets/gao-20-522.pdf [hereinafter GAO, Privacy & Accuracy].

101. Devin Coldewey, *Inside Amazon's Surveillance-Powered, No-Checkout Convenience Store*, TechCrunch (Jan. 21, 2018), https://techcrunch.com/2018/01/21/inside-amazons-surveillance-powered-no-checkout-convenience-store/.

102. *Id.*

103. *Id.*

104. *Id.*

105. *Id.*

106. *Id.*

107. GAO, Privacy & Accuracy, *supra* note 100, at 10.

108. *Id.*

109. *Id.*

110. Vivian D. Wesson, *Why Facial Recognition Technology Is Flawed*, 92 N.Y. St. B.A. J., Aug. 2020, at 21 (2020).

111. *Id.*

viduals look for work or seek loans. Some have even been misidentified as the perpetrator of a crime.[112] To be more specific, the technology's development required deep learning, where the software achieved its mapping capabilities and identification methods by practicing on substantial data collections.[113] A large number of these information sets were not sufficiently diverse.[114] The databases contained a disproportionate number of middle-aged Caucasian males.[115] This lack of diversity thus causes errors when plotting and pairing faces of people of color, women, and the elderly.[116] Racial disparity is particularly problematic, especially in the United States, where African Americans are incarcerated disproportionately.[117] This database flaw can exacerbate the color differential and cause an increased number of misidentifications due to incorrect matches.[118] For example, one study reported an error rate of about thirty-one percent when identifying women with dark skin.[119]

These factors have prompted a re-examination of the technology, thereby stimulating further discussions about discrimination in the use of the technology.[120] For instance, some of the tech giants implemented safeguards to reduce bias "by altering testing cohorts and refining data collection on specific demographics."[121] A Gender Shades[122] re-audit corroborated a reduction in error rates among Black females and investigated more algorithms such as Amazon's Rekognition, discussed later in this Article.[123] This study also revealed "racial bias against darker-skinned women (31% error in gender classification)."[124] The Gender Shades re-audit affirmed a previous analy-

112. *Id.*

113. Jake Bechtel, *Two Major Concerns About the Ethics of Facial Recognition in Public Safety*, DESIGN WORLD (Mar. 14, 2019), https://www.designworldonline.com/two-major-concerns-about-the-ethics-of-facial-recognition-in-public-safety/.

114. *Id.*

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.*

119. Hodge, *supra* note 15, at 62 (citing NEW HUMANIST, *The Limits of Facial Recognition Technology* (Feb. 18, 2019), https://newhumanist.org.uk/articles/5419/the-limits-of-facial-recognition-technology).

120. Najibi, *supra* note 19.

121. *Id.*

122. This term refers to the discrepancies identified by scientists "in classification of gender and skin tone by facial recognition technology indicating algorithmic bias." Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classi?cation*, RACE, RES, & POL'Y PORTAL, https://rrapp.hks.harvard.edu/algorithmic-bias-in-facial-recognition-technology-on-the-basis-of-gender-and-skin-tone/ (last visited Apr. 17, 2022).

123. Najibi, *supra* note 19.

124. *Id.*

sis of Rekognition's "face-matching capability by the American Civil Liberties Union (ACLU), in which 28 members of Congress, disproportionately people of color, were incorrectly matched with mugshots" of suspected criminals.[125]

Another inherent weakness of FRT is that people's faces change over time, which can trick the software into misidentifying an individual based upon an earlier image. Even alterations in appearance that occur daily, such as hairstyle and facial expressions, can cause misidentifications.[126] The picture's quality even reduces the success of FRT since it influences the utility of facial-recognition algorithms.[127] This is a fundamental problem with video scanning since the image's quality is not as good as a digital camera.[128] "The comparative dimensions of the face with the image size also influence how well the face will be identified," and "[t]herefore, small image sizes cause facial recognition difficulties."[129]

Ethical concerns can also arise in matters of "necessity, complicity, impartiality, bias, accountability, and oversight."[130] For instance, FRT runs the risk of being misused in its implementation. Its capacity and abilities can be viewed as a justification to increase surveillance at an event or at a site where it was not previously employed, evoking the reproach that "big brother" is watching.[131] There is also a risk of facial identity fraud.[132] The ability to not wait in line to pay for a purchase because of a cashier-less store is exciting, but the technology raises security concerns.[133] Contemplate a case involving twins who look very much alike but have different financial resources.[134] The wrong person may be charged for the purchase.[135] This type of misidentification is real, making "purchase validation through facial recognition a very grey area in terms of security."[136]

---

125. *Id.*

126. Hamann & Smith, *supra* note 51, at 10.

127. Jeffrey Edgell & Andrew Trimpe, *4 Limitations of Facial Recognition Technology*, FEDTECH (Nov. 22, 2013), https://fedtechmagazine.com/article/2013/11/4-limitations-facial-recognition-technology.

128. *Id.*

129. Hodge, *supra* note 15, at 62.

130. Bechtel, *supra* note 113.

131. Yaroslav Kuflinski, *How Ethical Is Facial Recognition Technology?*, TOWARDS DATA SCIENCE (Apr. 11, 2019), https://towardsdatascience.com/how-ethical-is-facial-recognition-technology-8104db2cb81b.

132. *Id.*

133. *Id.*

134. *Id.*

135. *Id.*

136. *Id.*

In the retail world, advertisers are data rich. Instead of searching through many sources, retailers can use facial recognition technology to learn about consumer buying behaviors.[137] They will be able to form opinions about likes and dislikes based upon the facial expressions of consumers.[138] Advertisers can estimate the demographics of those walking by billboards to customize their messages, and they can ascertain how long a consumer viewed an advertisement.[139] These methods raise privacy concerns but also present distress over stereotypes. For instance, a person might be exposed to an ad based upon the viewer's skin color or be shown a restaurant promotion grounded upon ethnicity.[140] As the technology continues to develop, marketers will predict with greater accuracy more sensitive information about a person such as a name, interests, and credit scores by taking their picture and using the recognition software to link the picture to the consumer's social media accounts and homepages.[141]

Some companies have recognized the technology's flaws and have stopped selling facial recognition software to law enforcement.[142] As the Black Lives Matter marches erupted across the country, IBM, Amazon, and Microsoft are some of the vendors who halted sales of FRT to the police and urged the government to regulate the technology.[143] Some organizations, academics, and politicians warn that continued government use of FRT presents substantial dangers to democracy. [144] This risk occurs by tolerating observations in public areas and greatly enlarging law enforcement's capabilities to identify and track individuals covertly.[145] Some algorithms even have trouble identifying people of color, a shortcoming which raises "fears that [FRT's] use harms minority communities."[146]

While most of the attention regarding the disadvantages and civil liberty concerns involving FRT has been directed to law enforcement use, there is also apprehension of its application to the private sector. The safeguards provided by the Constitution may not have the same consumer protections in the retail, medical, and banking markets; in-

137. MINETTE DRUMWRIGHT, ETHICAL ISSUES IN COMMUNICATION PROFESSIONS: NEW AGENDAS IN COMMUNICATION 242 (2013).

138. *Id.*

139. *Id.* at 242, 245.

140. *Id.* at 246.

141. *Id.* at 247.

142. Julia Horowitz, *Tech Companies Are Still Helping Police Scan Your Face*, CNN (July 3, 2020), https://www.cnn.com/2020/07/03/tech/facial-recognition-police/index.html.

143. *Id.*

144. *Id.*

145. *Id.*

146. *Id.*

dividuals still enjoy common law and statutory protections such as the right to privacy.[147]

A variety of industry and privacy organizations have suggested or are developing voluntary privacy strategies for commercial use of the technology.[148] Proposed best practices differ, "but most call for disclosing the technology's use and obtaining consent before using it to identify someone from anonymous images."[149]

V. Laws Regulating Facial Recognition Technology

A. Common Law

Privacy is part of the fabric of United States law and is a fundamental right.[150] The common law origins of the right to privacy were articulated in the 1890s in a law review article that analyzed a series of cases over a century which identified "a general right to privacy."[151] In *Griswold v. Connecticut*, the Supreme Court noted that the right of privacy is "older than the Bill of Rights—older than our political parties, [and] older than our school system."[152] The Court then linked the right to privacy to a "penumbra" of Amendments even though the concept is not explicitly provided in the Constitution.[153]

B. Federal Level

It is common knowledge that technology outpaces the law, so it is not surprising that there is little federal regulation of biometric privacy.[154] This is troublesome because questions persist about the accuracy and built-in biases in these systems.[155] A few industry-driven

147. *See id.*

148. GAO, Commercial Uses, *supra* note 25.

149. *Id.*

150. 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, 363 (2019).

151. Patel v. Facebook, Inc., 932 F.3d 1264, 1271 (9th Cir. 2019) (citing Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 198 (1890)).

152. Griswold v. Connecticut, 381 U.S. 479, 486 (1965).

153. Stewart, *supra* note 150, at 363.

154. Natasha Kohne & Kamran Salour, Biometric Privacy Litigation: Is Unique Personally Identifying Information Obtained from a Photograph Biometric Information? 2 (2017), https://www.akingump.com/a/web/61629/1Biometric-Privacy-Litigation.pdf.

155. Hodge, *supra* note 15, at 66. FBI facial recognition systems are regulated chiefly by two laws: the Privacy Act of 1974, 5 U.S.C. § 552a and the E-Government Act of 2002, P.L. 107-347. These laws require that the FBI conduct Privacy Impact Assessments (PIAs) of its biometric initiatives and that it use Fair Information Practices Principles (FIPPS); *see* CloudFare, *What Are the Fair Information Practice Principles? FIPPs*, https://www.cloudflare.com/learning/privacy/what-are-fair-information-practices-fipps/ (last visited Apr. 25, 2022). FIPPs highlight the need for transparency, consent, limited use, data quality, data minimization, security, and ac-

regulations pertain to biometric identification data within the financial, healthcare, commercial, and educational sectors.[156] For example, the Federal Trade Commission Act gives the agency the power to maintain enforcement action against commercial entities that engage in unfair or deceptive trade practices involving biometric data.[157]

The Health Insurance Portability and Accountability Act (HIPAA) requires healthcare providers to safeguard the protected health information (PHI) of patients.[158] PHI is defined as "individually identifiable health information . . . [t]ransmitted or maintained in any . . . form or medium" by a covered entity or its business associates.[159] Facial images are classified as protected health information and safeguarded if they are tied directly to a patient.[160] The privacy of student records is protected by the Family Educational Rights and Privacy Act.[161] This law covers any institution that obtains money under a program of the U.S. Department of Education.[162] The statute requires a school to acquire written permission from the parent or eligible student before releasing any information from a student's educational records.[163]

"Headline-grabbing" cases involving FRT, such as the January 6, 2020, capital riots, have caught the attention of members of Congress.[164] "Both law enforcement professionals and amateur sleuths turned to facial recognition to identify insurrectionists."[165] Legislators have also taken notice of the firms that no longer license the technology to law enforcement because of the legal questions presented by its use.[166] These events and a flurry of class-action lawsuits against image suppliers have spurred several legislators to propose facial recognition

countability when working with personal identifiable information. *Id.* PIAs review how personal identifiable information is controlled in electronic systems and ascertain the danger of collecting, keeping, and distrusting this material. *Id.*

156. Stewart, *supra* note 150, at 355–56, 358.

157. Hildebrand et al., *supra* note 14.

158. 45 C.F.R. §§ 160, 164 (1996).

159. *Id.* § 160.103.

160. Roger Shindell, *HIPAA Privacy & Security Compliance: Managing the Use of Photographs and Videos in the Wound Clinic*, TODAY'S WOUND CLINIC (July 2016), https://www.todayswoundclinic.com/blog/hipaa-privacy-security-compliance-managing-use-photographs-and-videos-wound-clinic.

161. 20 U.S.C. § 1232g (2013); 34 C.F.R. § 99.1 (1996).

162. U.S. DEP'T. OF EDUC., *Family Educational Rights and Privacy Act (FERPA)*, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (last visited Apr. 3, 2021).

163. *Id.*

164. Nicole Sakin, *Will There Be Federal Facial Recognition Regulation in the US?*, IAPP (Feb. 11, 2021), https://iapp.org/news/a/u-s-facial-recognition-roundup/.

165. *Id*.

166. *Id.*

policies and regulations.[167] For instance, the U.S. House Committee on Oversight and Reform has conducted multiple hearings to examine the risks presented by both government and commercial use of FRT.[168]

It is worth mentioning that the enterprises that are at the forefront of FRT development software are pressuring Congress to regulate the field.[169] Paramount in these efforts is Amazon. The company's policy team has crafted legislation that it wants Congress to adopt.[170] It wants to solidify "Rekognition," a facial recognition tool developed by Amazon. This desire causes some to question the company's motivation as being an act of protecting the firm's self-interest.[171] Amazon wants an "open, honest, and earnest dialogue among all parties involved to ensure that the technology is applied appropriately and is continuously enhanced."[172] Interestingly, Rekognition's FAQ page notes that pictures and videos may be "stored and used for any of Amazon's machine learning or artificial intelligence technologies unless the consumer affirmatively opts out."[173]

C. State Response

States are happy to fill the void caused by the lack of federal legislation involving this technology, and 2020 was a banner year for the passage of privacy statutes.[174] According to the National Conference of State Legislators, twenty-two states have enacted legislation on facial recognition technology.[175] Almost half of these jurisdictions debated incorporating biometric data in their definitions of personal information as part of their privacy legislation packages.[176] The result is that these laws are varied in scope and remedy across states. Some allow a private cause of action, and others only empower a state offi-

167. *Id.*

168. Angelique Carson, *Lawmakers (Continue To) Grapple with How to Regulate Facial Recognition*, IAPP (Jan. 16, 2020), https://iapp.org/news/a/lawmakers-continue-to-grapple-with-how-to-regulate-facial-recognition/.

169. Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STANFORD TECH. L. REV. 1, 37 (2020).

170. *Id.*

171. *Id.*

172. *Id.* (quoting Michael Puke, *Some Thoughts of Facial Recognition Legislation*, AMAZON WEB SERVICES MACHINE LEARNING BLOG (Feb. 7, 2019), https://perma.cc/C6PE-Y3VD).

173. *Id.* at 37–38.

174. Pam Greenberg, *Spotlight: Facial Recognition Gaining Measured Acceptance*, NAT'L CONF. ST. LEGISLATORS (Sept. 18, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/facial-recognition-gaining-measured-acceptance-magazine2020.aspx.

175. *Id.*

176. *Id.*

cial to enforce the law.[177] Some state statutes are narrowly focused on a specific issue, such as using the technology by law enforcement.[178] The following is a representative sample of these laws.

1. Illinois

Illinois was the first state to regulate biometric information with the passage of the Biometric Information Privacy Act (BIPA).[179] The goal of this statute is to ensure transparency between private entities and consumers.[180] Therefore, the law "sets up significant restrictions on how private companies obtain and use an individual's biometric data."[181] Businesses that collect information will have to inform consumers that their biometric profiles will be gathered.[182] They must also justify the collection; explain the amount of time the information is to be collected, retained, and used; fashion a written policy that provides a retention schedule; and secure written authorization before obtaining biometric information or sharing the biometric data with another entity.[183]

The statute creates a private cause of action, permitting individuals to file a claim for a violation of the law, and the penalties are substantial.[184] Any entity that negligently violates BIPA is subject to liquated damages of $1,000 or actual damages, whichever is greater.[185] If the violation is intentional or reckless, the penalty increases to liquidated damages of $5,000 or actual damages, whichever is larger.[186] Added to these sums is an award of "reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses."[187]

2. Texas

Texas followed suit and enacted the Capture or Use of Biometric Identifier Act.[188] This law prohibits obtaining a person's "biometric identifiers for commercial purposes" unless the collecting entity noti-

177. *Id.*
178. *Id.*
179. 740 ILL. COMP. STAT. 14 (2008); *see also* ACLU ILL., *Biometric Information Privacy Act (BIPA)*, https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa (last visited Apr. 25, 2022).
180. ACLU ILL., *supra* note 179.
181. Hodge, *supra* note 15, at 65.
182. *Id*.
183. *Id.*
184. 740 ILL. COMP. STAT. 14/20.
185. *See id.* § 1.
186. *Id.*
187. *Id.*
188. TEX. BUS. & COM. CODE ANN. § 503.001 (2021).

fies the individual and obtains that person's consent.[189] Texas also restricts "the sale or disclosure of an individual's biometric identifiers except under specific conditions."[190] However, the statute only protects biometric identifiers.[191] It does not cover data that is transformed into a template or code, nor does it require a written release.[192] Unlike Illinois law, the legislation does not create a private cause of action.[193] It merely gives the Attorney General the authority to bring suit to enforce the statute along with a penalty up to $25,000 per violation.[194]

3. Washington

Washington was the third state to enact legislation when it passed the Biometric Data Statute in 2017.[195] This comprehensive law defines a biometric identifier as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."[196] However, it excludes a physical or digital photograph collected or stored for healthcare treatment or operations under HIPAA.[197] No one may "enroll" a biometric identifier in a database for a commercial use without providing prior notice, securing consent, or offering a way to thwart the subsequent utilization of a biometric identifier for commercial purposes.[198] Unlike the statutes of Illinois and Texas, this law contains an exception for those entities who collect, capture, or store biometric identifiers for "security purpose[s]."[199] This legislation, however, provides no private remedy, and only Washington's Attorney General can enforce the mandates.[200]

---

189. Hodge, *supra* note 15, at 66.

190. *Id.*

191. *Id.*

192. John G. Browning, *The Battle Over Biometrics*, TEX. B.J., Oct.2018, at 674, 676, https://www.texasbar.com/AM/Template.cfm?ection=Content_Folders&ContentID=42128&Template=/CM/ContentDisplay.cfm.

193. *Id.* at 674, 676; TEX. BUS. & COM. CODE ANN. § 503.001(d).

194. Browning, *supra* note 192, at 674, 676; TEX. BUS. & COM. CODE ANN. § 503.001(d).

195. WASH. REV. CODE ANN. § 19.375.010 (West 2017).

196. *Id.* § 19.375.010(1).

197. *Id.*

198. HUNTON ANDREW KURTH LLP, *Washington Becomes Third State to Enact Biometric Privacy Law* (June 1, 2017), https://www.huntonprivacyblog.com/2017/06/01/washington-becomes-third-state-enact-biometric-privacy-law/.

199. *Id.*

200. *Id.*

4. New York

New York amended its existing data law in 2019 when it passed the Stop Hacks and Improve Electronic Data Security Act (SHIELD).[201] The law requires businesses to safeguard New York residents' "private information" and enlarges the state's security breach notification mandates.[202] SHIELD notes that any company that stores the private information of its residents, such as biometrics and driver's license information, must "develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information."[203] Unlike Illinois, the legislation does not create a private remedy.[204] Instead, it empowers the state's Attorney General to uphold the mandates.[205]

5. California

The California law regulating biometric data is known as the California Privacy Act.[206] It provides new privacy rights for consumers, such as being informed about the personal material a business gathers about them, how it is used, and the ability to eliminate personal information collected.[207] The penalty for non-compliance depends on the offense—unintentional civil penalties start at $2,500 per violation;[208] the fine for an intentional violation can be as much as $7,500 per incident.[209]

6. Arkansas

Arkansas amended its Personal Information Protection Act to include biometric data in the definition of "personal information."[210] Biometric data is information created by "automatic measurements

201. N.Y. GEN. BUS. LAW § 899-bb (West 2020).

202. Hodge, *supra* note 15, at 65.

203. Philip Gordon & Jennifer Taiwo, *The New York SHIELD Act: What Employers Need to Know*, SHRM (Aug. 28, 2019), https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/new-york-shield-act.aspx.

204. *Id.*

205. *Id.*

206. *See* CAL. DEP'T. OF JUSTICE, *California Consumer Privacy Act (CCPA)*, https://oag.ca.gov/privacy/ccpa (last visited Apr. 25, 2022).

207. *Id.*

208. Arlo Gilbert, *California Consumer Privacy Act (CCPA) Compliance Guide: Everything You Need to Know About the New Data Privacy Law*, OSANO (Sept. 29, 2020), https://www.osano.com/articles/ccpa-guide.

209. *Id.*

210. ARK. CODE ANN. § 4-110-103(7) (West 2019).

on an individual's biological characteristics."[211] The law provides that in the event of a security breach that involves the data of more than 1,000 people, the Attorney General must be notified.[212] A breach of security does not include the "good faith acquisition of personal information by an employee or agent" of that entity for "legitimate purposes" if the data is "not otherwise used or subject to further unauthorized disclosure."[213]

7. Maryland

Maryland prohibits an employer from using a facial recognition service to create a facial template during a job interview unless the applicant consents.[214] A facial recognition service means technology that evaluates facial characteristics and is used for the identification or persistent tracking of individuals in still or video images.[215] To be valid, the written consent must include the applicant's name, the interview date, the person's permission to use facial recognition during the interview, and an acknowledgement that the applicant has read the waiver.[216]

8. Massachusetts

Massachusetts law covering FRT is directed to law enforcement agencies using FRT and requires them to seek written permission before performing a database search.[217] A facial recognition search is defined as a "computer search using facial recognition to attempt to identify an unidentified person by comparing an image containing the face of the unidentified person to a set of images of identified persons; provided, however, that a set of images shall not include moving images or video data."[218] A search can be done under court approval, or without an order to identify a corpse, or if the law enforcement agency reasonably believes that an emergency involving a substantial

211. Adam Faria, *Arkansas Amends Its Personal Information Protection Act*, CLA CONNECT (May 7, 2019), https://blogs.claconnect.com/residentialmortgage/arkansas-amends-its-personal-information-protection-act/.

212. *Id.*

213. ARK. CODE ANN. § 4-110-103(1)(B).

214. MD. CODE ANN., LAB. & EMPL. § 3-717-b (West 2020).

215. *Id.* § 3-717-a(1).

216. Adam Forman & Nathaniel Glasser, *New Maryland Law Requires Applicant Consent Prior to Using Facial Recognition Technology in Job Interviews*, JD SUPRA (July 10, 2020), https://www.jdsupra.com/legalnews/new-maryland-law-requires-applicant-50746.

217. MASS. GEN. LAWS ch. 6 § 220 (2021).

218. *Id.*

risk of harm to another mandates the performance of a facial recognition search without delay.[219]

9. New Hampshire

New Hampshire is the first state to ban facial recognition technology used by the Department of Motor Vehicles.[220] The law prohibits this agency from using FRT concerning taking or retaining photographs and digital images.[221]

10. Virginia

In 2021, the Virginia state legislature enacted one of the most restrictive prohibitions in the country on FRT.[222] The law forbids all local law enforcement agencies and campus police from buying or employing FRT unless expressly allowed by the state legislature.[223]

11. Other States

Other jurisdictions that have proposed or enacted some form of legislation on facial recognition include Delaware, Michigan, North Carolina, Wisconsin, Kentucky, Arizona, Louisiana, Iowa, Nebraska, New Mexico, South Dakota, Colorado, and Wyoming.[224]

12. Cities

San Francisco, Boston, and Portland, Oregon are some of the cities that have taken matters into their own hands by passing ordinances that prohibit FRT.[225] Most of these initiatives are limited to police use.[226] Portland's law, however, is the most expansive.[227] It prohibits

219. *Id.*

220. N.H. REV. STAT. ANN. § 263:40-b (2014).

221. Kim Miller, *Facial Recognition: Current Uses, Concerns, and State Action*, MULTISTATE (Feb. 19, 2020), https://www.multistate.us/insider/2020/2/19/facial-recognition-current-uses-concerns-and-state-action.

222. Denise Lavoie, *Virginia Lawmakers Ban Police Use of Facial Recognition*, U.S. NEWS (Mar. 29, 2021), https://www.usnews.com/news/politics/articles/2021-03-29/virginia-lawmakers-ban-police-use-of-facial-recognition.

223. *Id.*

224. Greenberg, *supra* note 174.

225. Peggy Keene, *So Far, Three U.S. Cities Have Banned Facial Recognition Software*, KLEMCHUK, LLP (Oct. 8, 2020), https://www.klemchuk.com/ip-law-trends/cities-ban-facial-recognition-software-in-public; *see also* Julie Carr Smyth, *States Push Back Against Use of Facial Recognition by Police*, ABC NEWS (May 5, 2021), https://abcnews.go.com/Politics/wireStory/states-push-back-facial-recognition-police-77510175.

226. AMNESTY INT'L, *Ban Dangerous Facial Recognition Technology That Amplifies Racist Policing* (Jan. 26, 2021), https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing.

227. Keene, *supra* note 225.

the use of facial recognition software in "places of public accommodation,"[228] which is defined as businesses that are commonly open to the public or come within the ambit of one of the twelve categories defined under the Americans with Disability Act.[229] This software prohibition will affect private enterprises because it bans such use in areas that include restaurants, daycares, movie theaters, recreation centers, and doctors' offices.[230]

D. Other Countries

Many other nations have enacted data privacy laws to manage information that can identify or be used to recognize individuals. Currently, more than eighty countries have passed such legislation.[231] The European Union (EU) created the General Data Protection Regulation (GDPR) in 2018, one of the world's most rigid privacy protection laws.[232] Its goal is to safeguard individuals "in the EU from unlawful data collection or processing."[233] The law operates to enlarge consent mandates, offer enhanced user rights, and mandates a privacy strategy that is written in a manner that is easy to understand.[234] The law bans any artificial intelligence techniques that exploit vulnerable groups, use subconscious methods, or score people's social behavior.[235] The use of FRT and other "real-time remote biometric identification systems" by the police is also banned unless employed to "prevent a terror attack, find missing children or tackle other public security emergencies."[236] The reach of the law extends beyond member countries.[237] Regardless of where an entity is located, any business that sells to or has EU customers is subject to the GDPR.[238] Belgium and Luxembourg are two of only three countries globally to "officially oppose the use of facial recognition technology."[239]

---

228. *Id.*

229. 42 U.S.C. §§ 12101–12213 (2018).

230. Keene, *supra* note 225.

231. Myranda Westbrook, *Global Privacy Concerns of Facial Recognition Big Data*, U. TENN. CHATTANOOGA SCHOLAR 12 (Dec. 2020), https://scholar.utc.edu/cgi/viewcontent.cgi?article=1299&context=Honors-theses.

232. *Id.* at 13.

233. *Id.*

234. *Id.*

235. Natalia Drozdiak, *Facial Recognition, Other 'Risky' AI Set for Constraints in EU*, BLOOMBERG (Apr. 21, 2021), https://www.bloomberg.com/news/articles/2021-04-21/facial-recognition-other-risky-ai-set-for-constraints-in-eu.

236. *Id.*

237. Westbrook, *supra* note 231, at 14.

238. *Id.*

239. Iman Ghosh, *Mapped: The State of Facial Recognition Around the World*, VISUAL CAPITALIST (May 22, 2020), https://www.visualcapitalist.com/facial-recognition-world-map/.

Most facial recognition technology in South America is focused on reducing crime.[240] It permitted law enforcement officials in Brazil to apprehend Interpol's second most wanted criminal.[241] Brazil has plans to establish a biometric database of its citizens. [242] However, some citizens are apprehensive that this development could also act as a way to "prevent dissent against the current political order."[243]

Canada permits the collection and sharing of facial images for identification purposes regardless of consent and lacks satisfactory legal remedies, including the ability to challenge decisions made with this technology.[244] The country's privacy laws, designed to guard against mass surveillance, presently have no "real enforcement power and adequate safeguards to protect facial [identification] information."[245] A vulnerability in Canadian law is that its biometric data safeguards for facial information is poorly defined.[246] Canada's Privacy Act, the country's privacy legislation regulating the federal government, fails to explicitly address "facial and biometric information as subsets of personal information worthy of special protection."[247] The legislation thus fails to offer proper protections against the substantial risks related to the collection, use, and disclosure of some of its citizen's most sensitive personal information.[248]

China has been at the forefront in the development and use of FRT.[249] It is employed for "government and corporate surveillance of citizens and employees, to toilet-paper dispensers in public bathrooms."[250] The nation has even created a "cloud camera system which uses artificial intelligence and can detect thousands of faces at one time and 'generate their facial data for the cloud, while locating a particular target in an instant.'"[251] Largely unchecked by regulations, the

240. *Id.*

241. *Id.*

242. *Id.*

243. *Id.*

244. Yuan Stevens & Sonja Solomun, *Facial Recognition Technology Speeds Ahead as Canada's Privacy Law Lags Behind*, OTTAWA CITIZEN (Mar. 1, 2021), https://ottawacitizen.com/opinion/stevens-and-solomun-facial-recognition-technology-speeds-ahead-as-canadas-privacy-law-lags-behind.

245. *Id.*

246. *Id.*

247. *Id.*

248. *Id.*

249. Rowe, *supra* note 169, at 19–20.

250. *Id.*

251. *Id.* at 23 (quoting Jane Li, *China's Facial-Recognition Giant Says It Can Crack Masked Faces During Coronavirus*, QUARTZ (Feb. 18, 2020), https://perma.cc/TEV2-EFMY).

government "could conceivably utilize [FRT] everywhere: [in the] streets, subway stations, airports, and border check points."[252]

The Personal Information Security Specifications, a data privacy regulation, may protect the information collected from facial recognition surveillance systems in China.[253] The regulation requires personal information be collected for "legal, justified, necessary, and specific purposes."[254] The rule generally necessitates consent, and the information must be safeguarded.[255] However, scholars have commented that there is minor enforcement and "biometric data is frequently collected without consent or sufficient data security protections, particularly during the COVID-19 pandemic."[256]

There is also no explicit definition of "personal facial information" under Chinese law.[257] Instead, it is encompassed by the broader concept of "personal identifiable information."[258] More specifically, the country's facial recognition law is covered by the Cybersecurity Law of the People's Republic of China.[259] The law provides legal requirements on "network operators by stating the requirements for the collection, use, and protection of personally identifiable information (PII), which includes biometric data."[260] "However, biometric information is not the central focus of the law, and [the technology] is not discussed beyond the definition section."[261] The law does contain a "Personal Information Security Specification."[262] This Specification encompasses "data protection with a higher degree of granularity, but it is nonbinding."[263] The law sets forth guidelines on data handling and protection to prevent illegal collection, abuse, and data access.[264] Despite the failure of the Specification to set forth penalties, it is recognized as establishing best practices and acts as a central reference for governmental agencies.[265]

---

252. *Id.*

253. *Id.* at 19.

254. *Id.* at 20 (quoting Mingli Shi et al., *Translation: China's Personal Information Security Specification*, NEW AM. (Feb. 8, 2019), https://perma.cc/2W6V-LALE).

255. *Id.*

256. *Id.*

257. Seungha Lee, *Coming into Focus: China's Facial Recognition Regulations*, CTR. FOR STRATEGIC & INT'L STUD. (May 4, 2020), https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations.

258. *Id.*

259. *Id.*

260. *Id.*

261. *Id.*

262. *Id.*

263. *Id.*

264. *Id.*

265. *Id.*

VI. LITIGATION

Most of the litigation involving facial recognition technology arises in a criminal law context. The government tries to keep any mention of the technology's use out of the courtroom.[266] Defendants in criminal matters claim that FRT violates several of their constitutional rights.[267] This trend is changing as civil lawsuits are becoming commonplace.[268] The foundation of these lawsuits, in many cases, involves the statutes that allow a private cause of action.[269]

Many proceedings are filed as class actions, but the plaintiffs face several challenges, such as standing and the constitutionality of the statutes. The defendants rely heavily upon the Supreme Court ruling in *Spokeo v. Robins*[270] to maintain that the claimants have not adequately asserted an injury to have standing.[271] The *Spokeo* case arose under the Fair Credit Reporting Act of 1970 and alleged that a website operator published inaccurate information about the plaintiff.[272] The case centered on whether the customer had standing to maintain his claim under Article III of the Constitution.[273]

The Supreme Court noted that "the injury-in-fact requirement requires a plaintiff to allege an injury that is both 'concrete *and* particularized.'"[274] A "plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision."[275] The injury must harm the plaintiff in a personal and individual manner that is concrete.[276] This requirement does not mean that an aggrieved party automatically fulfills the injury-in-fact mandate whenever a statute provides a person with a statutory right and aims to permit that person to sue to enforce that privilege.[277] A plaintiff cannot merely allege a bare procedural violation disassociated from

266. Hodge, *supra* note 15, at 69–70.

267. *Id.*

268. *Id.*

269. *Id.*

270. Spokeo v. Robins, 578 U.S. 330 (2016).

271. Stewart, *supra* note 150, at 373–74.

272. *Spokeo*, 578 U.S. at 331.

273. *Id.*

274. *Id*. at 334 (quoting Friends of the Earth, Inc. v. Laidlaw Env't Servs. (TOC), Inc., 582 U.S. 167, 180–81 (2000).

275. *Id.* at 338.

276. *Id.*

277. *Id.* at 341.

any actual harm.[278] Instead, the pleading must allege and satisfy the injury-in-fact requirement of Article III.[279]

Many FRT lawsuits are based upon BIPA, which was enacted in 2008 but went largely unnoticed until 2015.[280] At this time, several Illinois citizens sued Facebook, claiming that the social media company's "Tag Suggestions" accumulated, stored, and used face prints in violation of BIPA.[281] For example, In re *Facebook Biometric Information Privacy Litigation* involved a suit against Facebook based upon BIPA.[282] The plaintiffs asserted that Facebook "unlawfully collected and stored biometric data derived from their faces."[283] The matter arose from the defendant's "Tag Suggestions" feature when a consumer identifies by name other Facebook users who appear in the pictures uploaded to the platform.[284] The complaint alleged that this action allowed Facebook to accumulate users' biometric data without consent in violation of BIPA.[285] The defendant moved to dismiss the complaint claiming that it failed to state a claim under the Act.[286]

The court denied the requested relief and ruled that the complaint was sufficient under the plain language of BIPA.[287] The plaintiffs averred that Facebook scans user-uploaded photographs to generate a "unique digital representation of the face . . . based on geometric relationship of their facial features."[288] The statute is an informed consent law dealing with the collection, storage, and use of personal biometric identifiers and information when biometrics is just starting to be broadly used.[289] Trying to classify this objective within a specific in-person data collection process has no backing in the words and construction of the law.[290] It is also adverse to its far-reaching purpose of safeguarding privacy given emerging biometric technology.[291]

The case against Facebook was the impetus for the filing of additional lawsuits against various social media companies.[292] During the

278. *Spokeo*, 578 U.S. at 341.
279. *Id.* at 338.
280. *See generally* KOHNE & SALOUR, *supra* note 154.
281. *Id.*
282. *In re* Facebook Biometric Info. Privacy Litig., 185 F.Supp.3d 1155, 1158 (N.D. Cal. 2016).
283. *Id.*
284. *Id.*
285. *Id.* at 1159.
286. *Id.*
287. *Id.*
288. In re *Facebook*, 185 F.Supp.3d at 1171.
289. *Id*. at 1172.
290. *Id.*
291. *Id.*
292. *See generally* KOHNE & SALOUR, *supra* note 154.

same year, another Illinois court considered *McCullough v. Smarte Carte, Inc.* based upon the Illinois privacy law.[293] The case involves a form of biometric data other than facial photographs but is instructive.[294] Smarte Carte does business in Illinois, where it provides lockers that use the renter's fingerprint as a "key."[295] The plaintiff rented a locker on several occasions at Union Station in Chicago.[296] The lawsuit claimed that Smarte Carte did not inform renters and obtain their written consent to collect or store their fingerprints, in violation of BIPA.[297] The defendant moved to dismiss, claiming that the court lacked subject matter jurisdiction, and alleging that the plaintiff failed to assert that she incurred an injury to satisfy the requirements of standing.[298]

The plaintiff averred that Smarte Carte violated the statute by failing to obtain consent and tell her that it would keep her fingerprints and for what time period, if any, following the rental period.[299] These are technical violations of BIPA, but the court determined that the plaintiff failed to allege any harm that resulted from the violation.[300] The plaintiff knew when she first used the locker that her fingerprint information would have to be stored until she repossessed the items from the storage unit.[301] Even without a prior agreement to retain, the court found it hard to understand how this retaining of information could constitute an actual harm.[302] The plaintiff also lacked standing because of the failure to show proof of an actual injury to recover statutory damages like those provided under BIPA. [303] The plaintiff's bare procedural violation cannot satisfy the constitutional requirements of standing. [304] While this attempt to collect damages failed, it was one of the first volleys to maintain a private cause of action against a business. It signaled the potential legal risks of using artificial intelligence.[305]

---

293. McCollough v. Smarte Carte, Inc., No. 16C 03777, 2016 WL 4077108, at *3 (N.D. Ill. Aug. 1, 2016).

294. *Id.*

295. *Id.* at *1.

296. *Id.*

297. *Id.*

298. *Id.* at *2.

299. *McCollough*, 2016 WL 4077108, at *3.

300. *Id.*

301. *Id.*

302. *Id.* at *3.

303. *Id.*

304. *Id.* at *4.

305. *See* Debra Bernard et al., *New Biometrics Lawsuits Signal Potential Legal Risks in AI*, JD SUPRA (Feb. 5, 2020), https://www.jdsupra.com/legalnews/new-biometrics-lawsuits-signal-32517/.

One year later, the opposite result was achieved. In *Dixon v. Washington and Jane Smith Community—Beverly*, the court was asked to decide whether BIPA was violated when an employer required its workers to clock in and out to record their work time by scanning their fingerprints onto a biometric timekeeping device.[306] The defendant moved to dismiss the BIPA claim because the worker had not "alleged an injury sufficient to make her a person 'aggrieved' under the Act."[307]

The court noted that the state passed the biometric law out of apprehension about the mounting use of biometric identifiers and information in financial transactions and security screening methods.[308] For this reason, the legislature's desire to fashion a legal right to privacy in personal biometric data and to safeguard the ability to control one's biometric information is "evident from its statement of legislative findings and intent as well as from the substantive requirements of the Act."[309] The law creates a private cause of action to allow "[a]ny person aggrieved by a violation of [the] Act" to enforce her rights under the legislation.[310] The plaintiff alleged that her employer revealed her fingerprint scan to the defendant without telling her or securing her consent.[311] Thus, this claimed violation of the right to privacy over one's biometric data is sufficient to constitute an injury.[312]

Monroy v. Shutterfly, Inc. involved a claim directly related to facial recognition technology.[313] The plaintiffs sued Shutterfly for "collecting and using their facial geometry without their consent in violation of Illinois' Biometric Information Privacy Act."[314] Shutterfly moved to dismiss the lawsuit by asserting that BIPA did not apply to facial geometry obtained from photos and that the plaintiffs failed to allege actual damages.[315] Based upon an analysis of the statutory definitions, the court opined that a facial scan did not constitute "biometric information"[316] but was a "biometric identifier."[317]

306. Dixon v. Washington and Jane Smith Community—Beverly, No. 17 C 8033, 2018 WL 2445292, at *1 (N.D. Ill. May 31, 2018).

307. *Id.* at *3.

308. *Id.* at *8; 740 ILL. COMP. STAT. 14/5 (2008).

309. *Dixon*, 2018 WL 2445292, at *9; *see* 740 ILL. COMP. STAT. 14/5.

310. *Dixon*, 2018 WL 2445292, at *9 (quoting 740 ILL. COMP. STAT. 14/20).

311. *Id.* at *12.

312. *Id.*

313. Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846, at *1 (N.D. Ill. Sept. 15, 2017).

314. Hodge, *supra* note 15, at 77–78.

315. *Monroy*, WL 4099846, at *2.

316. *Id.* at *3.

317. *See id.*

A facial scan is listed in the definition of "biometric identifier,"[318] and restricting these scans to those secured in person was not supported by the law's purpose of "protecting privacy in the face of emerging biometric technology."[319] As for Shutterfly's second defense, the court concluded that BIPA does not mandate proof of actual damages to state a claim.[320] This conclusion is supported by other statutes that have permitted recovery without a showing of actual harm.[321]

The most well-known case involving facial recognition technology is *Patel v. Facebook, Inc.*[322] Several Facebook users instituted a suit against Facebook, alleging that the social media giant utilized facial recognition technology without following the mandates of BIPA.[323] The litigation concerned Facebook's feature, "Tag Suggestions." If activated, the company may use FRT to determine if the user's friends are featured in pictures uploaded by that user.[324] If an image is downloaded, a program will examine the picture to determine if it contains known individuals' faces.[325] If known people are found in the image, the software identifies the geometric nodal points that create a facial signature.[326] The signature is then compared with other images in Facebook's database.[327] If a match is discovered, the company notifies the user to tag the person in the image.[328]

The defendant filed a motion to dismiss the lawsuit for lack of standing because the plaintiffs had not asserted an identifiable injury.[329] This motion was denied, and an appeal was taken of that ruling.[330] In upholding this ruling, and certifying the litigation as a class action, the Ninth Circuit Court of Appeals concluded that "an invasion of an individual's biometric privacy rights 'has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.'"[331] As soon as the social

318. *Id.* at *2.

319. *Id.* at *5 (quoting *In re* Facebook Biometric Info. Privacy Litig, 185 F.Supp.3d 1155, 1172 (N.D. Cal. 2016)).

320. *Id.* at *9.

321. *Monroy*, WL 4099846, at *9.

322. Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).

323. *Id.* at 1267.

324. *Id.* at 1268.

325. *Id.* at 1268.

326. *Id.*

327. *Id.*

328. *Patel*, 932 F.3d at 1268.

329. *Id*. at 1269–70.

330. *Id.*

331. *Id.* at 1273 (quoting Spokeo, Inc. v. Robins, 587 U.S. 330, 341 (2016)).

media giant generates a facial template of that individual, the possible applications are boundless.[332] Facebook can use the data to tag the consumer in millions of pictures uploaded to the defendant's site every day and ascertain if their Facebook friends are also located in the image.[333] The Ninth Circuit opined that Facebook's accumulation, use, and storage of customer's facial templates is the exact injury anticipated by BIPA.[334] Facebook appealed this adverse ruling to the United States Supreme Court, but the Court denied the writ.[335]

A few weeks later, the case was settled for $550 million.[336] The trial judge, however, rejected this resolution as being inadequate, and the matter was eventually resolved for $650 million making it one of the biggest privacy-related settlements in history.[337] Counsel fees were approved at $97.5 million, which was to be deducted from the settlement pool.[338] The terms of the agreement also required Facebook to turn the facial recognition setting off as the default option and to remove face templates unless it obtained express permission from the user.[339] Individuals who turned facial recognition on or signed up after September 23, 2019, were not covered by the agreement.[340]

This resolution contains several lessons in biometric privacy. Plaintiffs' attorneys now have every incentive to utilize BIPA as the next class action bonanza because of the award's size and low threshold for proving liability that is offered by Illinois's privacy law.[341] The award will become a yardstick to value other similar cases, increasing settlement values and causing it to become much more difficult for smaller defendants to dispose of BIPA cases for a reasonable figure.[342]

This settlement also highlights a developing circuit court split regarding these claims. The Ninth Circuit allows plaintiffs to satisfy Article III standing issues by averring a violation of BIPA distinct from

---

332. *See id.*

333. *Id.*

334. *Patel*, 932 F.3d at 1275.

335. *Id.* at 1264, *cert. denied*, 140 S. Ct. 937 (2020).

336. Thomas Germain, *Facebook Settles $550 Million Facial Recognition Lawsuit*, CONSUMER REPS. (Jan. 30, 2020), https://www.consumerreports.org/lawsuits-settlements/facebook-settles-facial-recognition-lawsuit/.

337. Nicholas Iovino, *Judge Approves Historic $650M Facebook Privacy Settlement*, COURTHOUSE NEWS SERV. (Feb. 26, 2021), https://www.courthousenews.com/judge-approves-historic-650m-facebook-privacy-settlement/?amp=1.

338. *Id.*

339. *Id.*

340. *Id.*

341. *Id.*

342. *Id.*

any actual injury.[343] Courts in different Circuits, however, have remanded BIPA lawsuits for failure to demonstrate actual harm.[344] Questions about other defenses to BIPA claims remain open, such as the applicable statute of limitations. The law in question fails to set forth a statute of limitations, but Illinois has a one-year time period for "publication of matters violating the right of privacy."[345] Nevertheless, this settlement is a wake-up call. Businesses should not only be cautious with their biometric procedures, but they must also stay abreast of developments in this quickly developing area of jurisprudence. It is also not just large tech firms that should be alert. Even small entities have been sued over alleged BIPA violations in recent years.[346]

CONCLUSION

As FRT hurls society into unexplored waters, the benefits that it provides must be balanced against its impact on privacy, data protection, and other consumer concerns.[347] FRT can be used to obtain and process an untold numbers of pictures from the internet and databanks to offer a composite to the police, businesses, and individuals.[348] New developments involving this technology, increased government regulations, and litigation demonstrate that facial recognition is a controversial topic that will continue to be in the news for many years.[349]

Ethical issues have and will surface in matters of "necessity, complicity, impartiality, bias, accountability, and oversight."[350] For instance, the technology presents the real risk of being misapplied in its implementation. Its abilities can be seen as a justification to increase surveillance at a function or at a location where it was not previously used, suggesting that "big brother" is watching.[351] Most of the focus about the drawbacks and civil liberty concerns involving FRT has been devoted to law enforcement use. However, they have equal ap-

343. Nick Kahlon & Eli Litoff, *Lessons from Facebook's Record $550 Million Biometric Settlement*, ILL. ST. B. ASS'N (Mar. 2020), https://www.isba.org/sections/bench/newsletter/2020/03/lessonsfromfacebooksrecord550millio (last visited Apr. 6, 2021).

344. *Id.*; *see, e.g.*, Hunter v. Automated Health Sys., Inc., No. 19 C 2529, 2020 WL 833180 (N.D. Ill. Feb. 20, 2020).

345. Kahlon & Litoff, *supra* note 343 (quoting 735 ILL. COMP. STAT. 5/13–201 (1982)).

346. *Id.*

347. Hildebrand et al., *supra* note 14.

348. LEXOLOGY, *supra* note 23.

349. Nicole Sakin, *Will There Be Federal Facial Recognition in the United States?*, PRIVACY ADVISOR (Feb. 11, 2021), https://iapp.org/news/a/u-s-facial-recognition-roundup/.

350. Bechtel, *supra* note 113.

351. Kuflinski, *supra* note 131.

plication to the business sector.[352] While the safeguards provided by the Constitution may not have the same consumer protections in the retail, medical, and banking markets, individuals still enjoy common law and statutory protections such as the right to privacy.[353]

It is a well-known phenomenon that technology outpaces the law. Therefore, it is not surprising that there is little federal regulation of biometric privacy.[354] However, some states have attempted to fill this void, and 2020 was a banner year for the passage of privacy statutes.[355] Twenty-two states have enacted legislation on FRT,[356] and this number should only increase with time. These laws differ in scale and remedy. Some allow a private cause of action, and others only empower a state official to enforce the law.[357]

FRT will continue to expand in the business sector as new uses are discovered. How the various governmental units will regulate this technology in the future remains to be seen. What is certain is that the *Patel* settlement has caught the attention of all interested parties who will assert competing pressures on the legislators to intervene one way or another.

352. *See generally* Horowitz, *supra* note 142.
353. *See id.*
354. KOHNE & SALOUR, *supra* note 154, at 2.
355. Greenberg, *supra* note 174.
356. *Id.*
357. *Id.*