IN THE ABSENCE OF A UNIFORM BIOMETRIC LAW: A PROPOSAL COMPARING CURRENT BIOMETRIC LAWS, ISSUES, AND FUTURE SOLUTIONS

Loraina Trujillo[1]

I. INTRODUCTION

Walking through a crowd, she pauses and looks over her shoulder. Cameras positioned high on the sides of buildings are pointed in each direction to analyze the facial structures of individuals in the flow of foot traffic from both directions. Is she being watched right now? In real-time, the cameras scan for wanted individuals and capture images to compare with police and national databases. Photographs are collected from social media sites for efficiency.

A man is called at work and told to come surrender himself at the police station. Ignoring the call, he drives home. A police car pulls into the driveway and proceeds to arrest him in front of his wife and daughters. Held overnight, he is interrogated and accused of shoplifting. He refrains from mentioning at work his two personal days were actually to cover the thirty hours spent in jail and court appearances. How far in the future are these scenarios?

It is not far at all, in fact, it is already here. On August 11, 2020, a United Kingdom Court of Appeals held the South Wales Police's use of Automated Facial Recognition ("AFR") to watch crowds in public locations to identify wanted persons was unlawful.[2] The police officers had directed the AFR at public crowds to obtain matches of suspected criminals in the crowd.[3] The AFR was used to search faces at certain events and public locations to

---

[1] J.D. Candidate, Southern Illinois University School of Law, Class of 2022. This note is dedicated to the author's parents, Loraine Brasel and Rafael Trujillo, for their love and support. The author thanks her family for their support throughout her academic career.

[2] *UK Court of Appeal Finds Automated Facial Recognition Technology Unlawful in Bridges v South Wales Police*, HUNTON ANDREWS KURTH: PRIV. & INFO. SEC. L. BLOG (Aug. 12, 2020), https://www.huntonprivacyblog.com/2020/08/12/uk-court-of-appeal-finds-automated-facial-recognition-technology-unlawful-in-bridges-v-south-wales-police/; Bridges v. The Chief Constable of South Wales Police, Case No: C1/2019/2670, Approved Judgment (Nov. 8, 2020), https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf; Dan Sabbagh, *South Wales Police Lose Landmark Facial Recognition Case*, The GUARDIAN (Aug. 11, 2020, 13:24 EDT), https://www.theguardian.com/technology/2020/aug/11/south-wales-police-lose-landmark-facial-recognition-case.

[3] *Id.* South Wales Police use of live-time facial recognition technology resulted in the arrest of sixty-one people for offenses including robbery, theft and court warrants. Sabbagh, *supra* note 2.

compare to a police database.[4] There were "fundamental deficiencies" in the AFR policies because the limitations of police's discretionary powers and permissible locations were not sufficiently defined.[5]

These privacy concerns have not been exclusive to Europe. Early in 2020, in Detroit, Michigan, two low-quality pictures were matched to Mr. Robert Julian-Borchak Williams driver's license picture.[6] The Detroit police department, using technology provided by DataWorks Plus, ran a facial recognition search and received a match.[7] However, the match was a false positive.[8] Mr. Williams' case of wrongful identification left him humiliated and his family changed.[9] Now when his daughters, ages three and seven, see police officers, they wonder if their father is going to be taken away.[10]

These cases foreshadow a future where privacy violations are commonplace or have already begun domestically and internationally. Similar situations of countries surveilling their citizens are occurring globally.[11] Authoritarian and democratic countries have incorporated the use of biometric identifiers into their government and economic policies to surveil for common objectives like law enforcement, national security, and consumer information.[12] Some countries are abusing this advancement of technology to increase supervision of their citizens.[13] Two global superpowers—the United States and China—have adopted different political ideologies, yet they occupy similar positions on the spectrum of government

---

4 *UK Court of Appeal Finds Automated Facial Recognition Technology Unlawful in Bridges v South Wales Police*, *supra* note 2.

5 *Id.*

6 Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html. Mr. Williams' case and fingerprint data would be expunged in response to this article. *Id.*

7 *Id.*

8 *Id.*

9 *Id.*

10 Drew Harwell, *Wrongfully Arrested Man Sues Detroit Police Over False Facial Recognition Match*, WASH. POST (Apr. 13, 2021, 4:18 PM EDT), https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/.

11 *See* Paul Mozur et al., *Made in China, Exported to the World: The Surveillance State*, N.Y. TIMES (Apr. 24, 2019), https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html (describing how Chinese-made intelligent monitoring systems are being used by eighteen countries and thirty-six others have received training in topics related to public opinion guidance).

12 Justin Sherman, *The Troubling Rise of Facial Recognition Technology in Democracies*, WORLD POL. REV. (Apr. 23, 2020), https://www.worldpoliticsreview.com/articles/28707/the-troubling-rise-of-ai-facial-recognition-technology-in-democracies. Countries such as India, the United States, Russia, China, and the United Arab Emirates use facial recognition software with varying amounts of regulation on private and public entities. *Id.*

13 Olga Khazan, *Actually, Most Countries Are Increasingly Spying on Their Citizens, the UN Says*, THE ATLANTIC (June 6, 2013), https://www.theatlantic.com/international/archive/2013/06/actually-most-countries-are-increasingly-spying-on-their-citizens-the-un-says/276614/.

surveillance.[14] These superpowers are also the technological leaders in our new digital age.[15]

This note discusses the advancements of biometric identification and the current laws governing these identifications within the United States and China. Biometric identifiers are used by a broad range of technology that has the capacity to retain our most personal information. The purpose of this note will focus primarily on facial recognition technology and its data retention. To begin, this note will provide a brief background of biometric identification, relevant definitions, as well as potential dangers. The next section will present an overview of current state statutes that will demonstrate the lack of uniformity across the United States. The following section will provide a comparison with China and the extent of biometric identification methods integrated into their society. Finally, this note will conclude with a proposal to enact a federal statute, as well as an additional comment on future Supreme Court action to determine the constitutional implications of this unregulated area of technology.

There is currently an absence of federal appellate court cases raising this issue in the context of law enforcement. The dangers posed by waiting until decisions from lower court cases have been appealed are enormous. With the speed of advancements in technology, decades of waiting for a case to reach the Supreme Court could result in irreversible damage to individual privacy rights. Biometric identification technology has the potential to increase security and convenience, benefiting both the public and private industries. However, biometric identification technology must have federal regulations and procedures to ensure it is correctly implemented. The intersection between privacy laws, consumer protection laws, and the Fourth Amendment provides a complex issue for the government and courts to address.

---

[14] Ali Watkins, *How the N.Y.P.D. Is Using Post 9/11 Tools on Everyday New Yorkers*, N.Y. TIMES (Sept. 11, 2021), https://www.nytimes.com/2021/09/08/nyregion/nypd-9-11-police-surveillance.html; *see* Andrei Lungu, *The U.S.- China Clash Is About Ideology After All*, FOREIGN POLICY, https://foreignpolicy.com/2021/04/06/us-china-ideology-communism-capitalism/ (last visited Oct. 7, 2021).

[15] *See generally* Yuan Yang & Madhumita Murgia, *How China Cornered the Facial Recognition Surveillance Market*, L.A. TIMES (Dec. 9, 2019, 6:00 AM PT), https://www.latimes.com/business/story/2019-12-09/china-facial-recognition-surveillance (discussing that Chinese and American companies compete to supply surveillance technologies to governments yet Chinese companies account for nearly half the market).

II. BACKGROUND

The average person will interact with biometric technology just about every day.[16] Whether it is unlocking a phone with facial identification or a fingerprint, airport security, banking, work attendance, biometric identifiers are vital in the digital age.[17] "[F]ingerprinting, palm veins analysis, DNA sequencing, palm printing and iris recognition" are biometric authentication methods used because they contain unique markers.[18] These identifiers can take the place of passwords and be used for payments for everyday necessities such as food, rent, and banking.[19] Security upgrades race to keep up with an increasingly digital world. "Biometric information is 'inherently public,' meaning that other people can easily view and gain access to it, and 'inherently private' because every [person] possesses unique biometric identifiers."[20] The tension between the private and public aspects of biometric information and how it can be used by private companies or law enforcement creates an area of ambiguity that Congress needs to address.[21]

Images of an individual's face can be captured without their knowledge or consent.[22] How facial scans are obtained may determine whether it is considered biometric information.[23] Images can be obtained from social

---

16 John Trader, *5 Ways Biometric Technology Impacts Our Everyday Life: A Statistical Representation*, M2SYS: BLOG (Dec. 26, 2015), https://www.m2sys.com/blog/access-control/5-ways-biometric-technology-impacts-our-everyday-life/; *See generally The Top 9 Common Uses of Biometrics in Everyday Life*, *Publications & Media*, NEC (July 7, 2020), https://www.nec.co.nz/market-leadership/publications-media/the-top-9-common-uses-of-biometrics-in-everyday-life/ (explaining that day-to-day life includes the usage of fingerprint, facial recognition, voice and iris recognition for airport security, law enforcement, mobile access and authentication, banking, home assistants, building access, schools, public transport, and blood banks).

17 Sharon Nakar & Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 BOS. U. J. SCI. & TECH. L. 88 (2017); *see The Top 9 Common Uses of Biometrics in Everyday Life*, *supra* note 16.

18 Nakar & Greenbaum, *supra* note 17, at 94; *UK Court of Appeal Finds Automated Facial Recognition Technology Unlawful in Bridges v South Wales Police*, *supra* note 2; *see* Sabbagh, *supra* note 2.

19 *See How to Use Apple Pay*, APPLE, https://support.apple.com/en-us/HT201239 (last visited Sept. 24, 2021).

20 Blake Benson, *Fingerprint Not Recognized: Why the United States Needs to Protect Biometric Privacy*, 19 N.C. J.L. & TECH. 161, 171 (2018).

21 *Id.*

22 LAW ENFORCEMENT IMAGING TECHNOLOGY TASK FORCE, LAW ENFORCEMENT FACIAL RECOGNITION USE CASE CATALOG 4 (Integrated Justice Information Systems Institute 2019), https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Law_Enforcement_Facial_Recognition_Use_Case_Catalog.pdf. Images can be taken unknowingly by cameras or security cameras. *Id.* Images can be taken with consent at first but may be retained in a database or used by outside agencies. *Id.*

23 Natasha Kohne & Kamran Salour, *Biometric Privacy Litigation: Is Unique Personal Identifying Information Obtained from a Photograph Biometric Information?*, 25 ANTITRUST L. SECTIONS COMPETITION 2 (2016). Under Illinois Biometric Information Privacy Act, the definition of "biometric identifier and biometric information" does not include photographs. *Id.* at 5. Whether

media and the internet, but the government also has access to official pictures from the Department of Motor Vehicles ("DMV").[24] Whether or not collected images can be retained indefinitely, or only for a short time, is yet to be established.[25] There are no uniform guidelines for what is lawful.[26] States that have enacted biometric data statutes are regulating commercial and private entities, not law enforcement.[27]

The United States does not have a federal statute addressing the boundaries of biometric identification usage.[28] With the increasing advancements in technology, regulations are needed to ensure citizens' rights are protected. When Illinois enacted its biometric security statute, the legislature included their findings that there is a heightened risk using biometric information because the characteristics are so biologically unique.[29] Therefore, an individual's biometric information needs protection and strong enforcement of that protection.[30]

Facial recognition is used by different industries such as corporations, law enforcement, consumer data collection, corporations like Apple, Inc., and online apps such as Instagram, Facebook and Shutterfly.[31] Multiple lawsuits have been filed against websites allegedly collecting biometric data without consent.[32] The federal government also uses biometric identifiers for various national security objectives.[33] The most common uses of facial recognition technology are by airport security, immigration, and law enforcement.[34] The United States has a troubling history of the federal

---

deriving an individual's faceprint from photographs online constitutes biometric data may depend on what state they are in. *Id.* at 18.

24 Thomas Germain, *Federal Agencies Use DMV Photos for Facial Recognition. Here's What You Need to Know*, CONSUMERREPORTS (July 8, 2019), https://www.consumerreports.org/privacy/federal-agencies-use-dmv-photos-for-facial-recognition-a1704098825/.

25 *Id*. at 6.

26 Chloe Stepney, *Actual Harm Means it is Too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law*, 40 LOY. L.A. ENT. L. REV. 51, 56-59 (2019) ("[P]rivacy standards are established for specific industries and situations."). There is no federal law regulating the collection or use of biometric information. *Id.*

27 FRANK NOLAN, IMPLICATION OF US LAWS ON COLLECTION, STORAGE, AND USE OF BIOMETRIC INFORMATION 7 (2020), https://us.eversheds-sutherland.com/portalresource/Biometrics%20whitepaper_July%202020.pdf.

28 Stepney, *supra* note 26.

29 740 ILL. COMP. STAT. 14/5(c) (2008).

30 *Id*.

31 LAW ENFORCEMENT IMAGING TECHNOLOGY TASK FORCE, *supra* note 22, at 3.

32 Aaron Holmes, *Instagram Could Face Up to $500 Billion in Fines in Class-Action Lawsuit Alleging It Illegally Harvested Biometric Data*, INSIDER (Aug. 12, 2020, 9:48 AM), https://www.businessinsider.com; *See generally* Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017); Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019); Hazlitt v. Apple, Inc., 500 F. Supp. 3d 738 (S.D. Ill. 2020); Rivera v. Google, Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017).

33 Office of Biometric Identity Management, *Biometrics*, DEP'T HOMELAND SEC. (June 9, 2021), https://www.dhs.gov/biometrics.

34 *Id*.

government abusing surveillance technology.[35] Dissidents have historically been targets of government campaigns to discredit, demoralize, and demonize organizations that are deemed contrary to the American way of life.[36]

During the summer of 2020, police body cameras were used to capture images of protestors.[37] Surveillance has been used to watch protestors as activism for racial justice has increased.[38] In January of 2021, after agitators entered the Capitol, usage of Clearview AI increased to identify any participants directly involved.[39] Clearview AI is a company that has created a facial recognition app with a database comprised of images from internet websites like Facebook or YouTube and has been licensed to law enforcement and private companies.[40] The Federal Bureau of Investigation ("FBI") requested assistance from state and local police departments familiar with Clearview AI's system to identify participants.[41] The federal government's indirect use of a third-party company that obtains images from various platforms may lead to increased usage should the searches yield a positive outcome.[42]

Although facial recognition software has many positive uses, Congress should enact a statute to regulate the technology before any worst-case scenarios come to fruition. Advanced surveillance technology to search an individual's face, or to retain it for future use in a search database, presents the issue of whether these searches are unreasonable under the Fourth Amendment.

---

35 David P. Hadley, *America's "Big Brother": A Century of U.S. Domestic Surveillance*, ORIGINS: CURRENT EVENTS IN HIST. PERSP. (Dec. 2013), http://origins.osu.edu/article/americas-big-brother-century-us-domestic-surveillance; Kashmir Hill, *The Secretive Company That Might End Privacy as We Know it*, N.Y. TIMES (Mar. 18, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

36 *Id.*

37 Malkia Devich-Cyril, *Defund Facial Recognition*, THE ATLANTIC (July 5, 2020), https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/.

38 *Id.*

39 Kashmir Hill, *The Facial Recognition App Clearview Sees a Spike in Use After the Capitol Attack*, N.Y. TIMES (Jan. 31, 2021), https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html; Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1, 4 (2020). This app has been licensed to law enforcement and private companies. *Id.* at 4-5.

40 Hill, *supra* note 39.

41 *Id.*

42 *Id.*

A. Brief History of Biometric Identifier Usage

Biometric identifiers can be divided into two categories: physiological and behavioral.[43]

In the twentieth century, federal and state governments have been using both categories of technology to record, wiretap, follow, and access data to monitor persons of interest.[44] The federal government can, and has, demonstrated it will overstep privacy boundaries.[45] From *Olmstead*[46] to *Carpenter*,[47] multiple landmark cases have set the current parameters for what is constitutional under the Fourth Amendment and the right to privacy.[48] The government is allowed to obtain information from a third-party because "an individual has no reasonable expectation of privacy in that [voluntarily conveyed] information."[49] In *Carpenter*, the Court set new boundaries on the third-party doctrine by holding "cell phone users possess a reasonable expectation of privacy in the cell-site location information history associated with their cell phones."[50] Whether a future Supreme Court case could apply a doctrine similar to *Carpenter* to third-party databases compiling images that individuals upload to internet accounts remains to be decided. Images such as profile pictures are voluntarily uploaded to media platforms. However, some social media users take reasonable measures to protect their privacy and prevent others from using their information.[51] Social media platforms provide options to limit what other users can see about an individual's profile, photos, friends, or posts.[52] Some platforms provide an

---

43 Jason B. Binimow, *State Statutes Regulating Collection or Disclosure of Consumer Biometric or Genetic Information*, 41 A.L.R. 7th Art. 4 § 2 (2019) ("Physiological characteristics are those that concern the body's composition . . . [e]xamples include: hand geometry, fingerprints, DNA, and face, retina, iris, or ear features. Behavioral characteristics are . . . [those] such as typing rhythm, gait, and voice.").

44 Charlie Savage et al., *Electronic Surveillance Under Bush and Obama*, N.Y. TIMES, https://archive.nytimes.com/www.nytimes.com/interactive/2013/06/07/us/07nsa-timeline/html#/#time254_7516 (last visited Sept. 24, 2021).

45 T.C. Sottek & Janus Kopfstein, *Everything You Need to Know About PRISM*, THE VERGE (July 17, 2013, 01:36 PM), https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet; Patrick Toomey, *The NSA Continues to Violate Americans' Internet Privacy Rights*, ACLU (Aug. 22, 2018, 5:30 PM), https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy.

46 Olmstead v. United States, 277 U.S. 438 (1928).

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

48 Benson, *supra* note 20.

49 Harvey Gee, *Last Call for the Third-Party Doctrine in the Digital Age After Carpenter*?, 26 BOS. U. J. SCI. & TECH. L. 286, 288 (2020). The third-party doctrine was established by the leading cases of *United States v. Miller* and *Smith v. Maryland*. *Id.*

50 *Id.* at 289.

51 Nadia Kovacs, *Tips for Protecting Your Social Media Privacy*, NORTON, https://us.norton.com/internetsecurity-privacy-protecting-privacy-social-media.html (last visited Sept. 24, 2021).

52 Larry Alton, *10 Ways to Protect Your Privacy on Social Media*, LIFEHACK, https://www.lifehack.org/articles/technology/10-ways-protect-your-privacy-social-media.html (last visited Sept. 24, 2021).

option to prevent search engines from linking an account should someone search that individual's name.[53]

State and federal government use of facial recognition does have many positive aspects. The range of facial recognition technology systems provide varying levels of sophistication and identification ability.[54] Facial recognition can be used to identify, track, and detain criminals.[55] It can help solve cold cases, identify suspects from video footage, and find missing children.[56] The Department of Homeland Security uses biometrics identifiers to screen for "suspected terrorists" and "immigration violators."[57] The Law Enforcement Facial Recognition Use Case Catalog, created by the Integrated Justice Information Systems Institute ("IJIS") and International Association of Chiefs of Police ("IACP"), lists numerous ways facial recognition can be used to aid police investigations.[58] Common uses would be deceased identification of John Does, identify fraud, photo array construction, victim identification, and participants in parole, probation or sex offender registry.[59]

The New York case *People v. Reyes* provides an example of future uses of facial recognition technology to solve crimes and possible arguments to be made by defendants.[60] The detective used stills from a video of a burglary to run against the facial recognition system which provided a potential match to pursue and confirm using other resources.[61] In New York, and other states, a positive facial recognition software match does not create probable cause for an arrest.[62] The possible match must be further investigated and corroborated by other resources.[63] While using facial recognition systems may be advantageous as a preliminary investigative tool, potential false accusations or abuses of the system should require that more evidence than a

---

53 *How to Remove Your Facebook Profile from Google Searches*, GEEK POWERED STUDIOS (May 22, 2017), https://www.geekpoweredstudios.com/how-to-remove-facebook-profile-from-google-searches/.

54 CONG. RSCH. SERV., R46586, FEDERAL LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY 2 (2020). Organizations use different systems depending on their environments or objectives, and the specific terminology helps law enforcement, policymakers, and the public differentiate between them. *Id.* at 1. The following are key terms used in this industry: face detection technology, facial classification algorithms, facial comparison and facial identification, *facial recognition*, *facial recognition algorithms*, probe, *real-time facial recognition*, and threshold. *Id.* at 1-2 (emphasis added).

55 *Id.* at 4.

56 Shirin Ghaffary, *How to Avoid a Dystopian Future of Facial Recognition in Law Enforcement*, VOX (Dec. 10, 2019, 8:00 AM EST), https://www.vox.com/recode/2019/12/10/20996085/ai-facial-recognition-police-law-enforcement-regulation.

57 Office of Biometric Identity Management, *supra* note 33.

58 LAW ENFORCEMENT IMAGING TECHNOLOGY TASK FORCE, *supra* note 22, at 17.

59 *Id.* at 9-16.

60 People v. Reyes, No. 3351-19 (N.Y. Sup. Ct. Oct. 7, 2020).

61 *Id.* slip op. at 4. The detective used the match to read the defendant's criminal file and made an identification based on distinctive forearm tattoos. *Id.* slip op. at 3.

62 *Id.* slip op. at 2; Hill, *supra* note 6.

63 People v. Reyes, slip op. at 2.

positive match is needed to make an arrest. Similar processes should be incorporated for all law enforcement use of facial recognition software.

B. Possible Fundamental Rights Violations

The right of privacy is the first fundamental right at risk of being violated by biometric identification technology.[64] Social media platforms, such as Facebook, usually request consent to use biometric data when the individual creates an account and accepts the terms and conditions.[65] The collection of this data from users' accounts has become the issue of several lawsuits, such as *Patel v. Facebook*, for lack of user consent and vague data retention policies.[66] Another concerning issue is third-party usage of images from social media to create facial recognition databases.[67] However, recent lawsuits have held that although consent to use consumers' biometric data is required, some companies have violated their consumers' privacy.[68]

Stepping outside of the context of social media, an individual cannot take reasonable precautions to prevent their face from being captured by cameras in public places.[69] Many cities have "public-private" camera systems that allow police access without warrants.[70] Whether being out in public equates an individual's consent for their facial structure to be captured

---

64 Larry J. Pittman, *The Elusive Constitutional Right to Informational Privacy*, 19 NEV. L.J. 135, 141 (2019). The right to privacy doctrine has ranged from the right to use contraceptives to constitutional limitations on government surveillance. *See id.* The "right to be let alone" has implied the constitutional right to one's informational privacy. *Id.* at 141. Privacy rights include privacy in the home, intimacy, relationships, and personal information. *See id.*

65 Patel v. Facebook, Inc., 932 F.3d 1264, 1267 (9th Cir. 2019).

66 *Id.* at 1268-69.

67 Rowe, *supra* note 39, at 3. Clearview AI uses images from platforms like Facebook, YouTube, and Venmo to create facial recognition databases. *Id.* at 4. Clearview argues these images can be retained without violating the platforms' terms of service because they are within the public domain. *Id.* at 5-6.

68 Bobby Allyn, *Judge: Facebook's $550 Million Settlement in Facial Recognition Case is not Enough*, NPR (July 17, 2020, 11:36 PM ET), https://www.npr.org/2020/07/17/892433132/judge-facebooks-550-million-settlement-in-facial-recognition-case-is-not-enough.

69 *See* Thomas Ricker, *The US, Like China, Has About One Surveillance Camera for Every Four People, Says Report*, THE VERGE (Dec. 9, 2019, 10:48 AM EST), https://www.theverge.com/2019/12/9/21002515/surveillance-cameras-globally-us-china-amount-citizens (comparing how China and the United States use security cameras in public and mentioning that only three percent of security cameras in the United States are for city-wide surveillance); *see also* Liza Lin & Newley Purnell, *A World With a Billion Cameras Watching You Is Just Around the Corner*, WALL ST. J. (Dec. 6, 2019, 1:00 AM ET), https://www.wsj.com/articles/a-billion-surveillance-cameras-forecast-to-be-watching-within-two-years-11575565402?mod=hp_listb_pos1.

70 Sidney Fussell, *When Private Security Cameras Are Police Surveillance Tools*, WIRED (Aug. 11, 2020, 3:27 PM), https://www.wired.com/story/private-security-cameras-police-surveillance-tools/. Cities are using combinations of public and private camera systems where citizens or private companies allow access to police departments. *Id.* Another example is Newark's system where residents can watch public closed-circuit TV footage and report crimes. *Id.*

indefinitely by a private entity or the government has not yet been addressed by the Supreme Court.[71]

Disparities between equal applications of facial recognition technology would create a discriminatory impact on minorities.[72] A facial recognition "match" led to the false arrest and thirty-hour detainment of a Black man in Detroit.[73] The National Institute of Standards and Technology ("NIST") performed a study and found "many of [the] algorithms were [ten] to [one hundred] times more likely to inaccurately identify a photograph of a Black or East Asian face, compared with a white one."[74] In contrast, facial recognition algorithms in China showed lowered false positive rates for East Asians.[75] Algorithms reflect the data used to train it and generally "facial recognition systems that are 'trained' only on lighter skin tones will not work well at identifying faces with darker skin tones."[76] This could result in varying error rates for different races or ethnicities depending where it originated from.[77]

The summer of 2020 saw a surge in demonstrations and protests in the wake of the death of George Floyd.[78] Similar to 2014, with the death of Michael Brown in Ferguson, Missouri, and Eric Garner in New York, New York and again in 2015, with the death of Freddie Gray in Baltimore, Maryland, law enforcement used facial recognition during the 2020 protests and demonstrations.[79] Different articles and "tips" have circulated the internet to help protestors avoid being identified by use of clothes, face coverings, and makeup.[80] If participants posted a picture or videos from

---

71 Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020).

72 Eli Newman, *Detroit City Council Passes Police Facial Recognition Contract*, MICH. RADIO (Sept. 29, 2020), https://www.michiganradio.org/post/detroit-city-council-passes-police-facial-recognition-contract.

73 Allyn, *supra* note 68.

74 NAT'L INST. OF STANDARDS AND TECH., NISTIR 8280, FACE RECOGNITION VENDOR TEST PART 3: DEMOGRAPHIC EFFECTS (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; Sophie Bushwick, *How NIST Tested Facial Algorithms for Racial Bias*, SCI. AM. (Dec. 27, 2019), https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/.

75 NAT'L INST. OF STANDARDS AND TECH., *supra* note 74.

76 Sherman, *supra* note 12.

77 Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

78 Elliott C. McLaughlin, *How George Floyd's Death Ignited a Racial Reckoning That Shows No Signs of Slowing Down*, CNN (Aug. 9, 2020, 11:31 AM ET), https://www.cnn.com/2020/08/09/us/george-floyd-protests-different-why/index.html.

79 Mark Morales & Laura Ly, *Released NYPD Emails Show Extensive Surveillance of Black Lives Matter Protestors*, CNN (Jan. 18, 2019, 7:01 PM EST), https://www.cnn.com/2019/01/18/us/nypd-black-lives-matter-surveillance/index.html; Rowe, *supra* note 39.

80 Aaron Holmes, *These Clothes Use Outlandish Designs to Trick Facial Recognition Software into Thinking You're Not Human*, BUS. INSIDER (June 5, 2020, 9:14 AM), https://www.businessinsider.com/clothes-accessories-that-outsmart-facial-recognition-tech-2019-10.

protests, they received comments to not show protestors' faces for fear of being made targets of either the police or those who did not agree with the protests.[81] Social media giants have provided data, or allowed access by third-party companies that used a geographical location system, to map activity from online accounts in protest areas. [82] Law enforcement used this information to identify and arrest protestors who could be located through their posts.[83]

Amnesty International has proposed a ban of the use of all facial recognition technology by law enforcement because of its potential human rights violations worldwide.[84] The European Union ("EU") considered imposing a moratorium on facial recognition technology until potential risks have been explored.[85] The United States has a history of discrimination, and the effects are still evident in prison, education, housing, and law enforcement statistics.[86] Minority communities are already disproportionately targeted by law enforcement without the use of facial recognition.[87] Correcting accuracy rates of facial recognition algorithms that disproportionally affect minorities would likely still exacerbate the issues these communities struggle with.[88] Before facial recognition becomes a commonplace aspect of law enforcement, state and federal guidelines are imperative to prevent an increase in disproportionate results.

---

81 Madeleine Aggeler, *Face of a Dissident*, THE CUT (June 24, 2020), https://www.thecut.com/2020/06/face-of-a-dissident.html.

82 Russell Brandom, *Facebook, Twitter, and Instagram Surveillance Tool was Used to Arrest Baltimore Protestors*, THE VERGE (Oct. 11, 2016, 1:42 PM EDT), https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api; *see* Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU N. CAL. (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

83 Brandom, *supra* note 82.

84 *Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance*, AMNESTY INT'L (June 11, 2020, 6:00 PM), https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/.

85 Elena Sánchez Nicolás, *Facial-Recognition Moratorium Back on EU Agenda*, EUOBSERVER (July 3, 2020, 7:03), https://euobserver.com/science/148839.

86 Danyelle Solomon et al., *Systemic Inequality: Displacement, Exclusion, and Segregation*, CTR. FOR AM. PROGRESS (Aug. 7, 2019, 7:00 AM), https://www.americanprogress.org/issues/race/reports/2019/08/07/472617/systemic-inequality-displacement-exclusion-segregation/; German Lopez, *There are Huge Racial Disparities in How US Police Use Force*, VOX (Nov. 14, 2018, 4:12 PM EST), https://www.vox.com/identities/2016/8/13/17938186/police-shootings-killings-racism-racial-disparities.

87 Lopez, *supra* note 86 ("An analysis of available FBI data by Dara Lind for Vox found that US police kill black people at disproportionate rates.").

88 *Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance*, *supra* note 84 ("[African Americans] already experience disproportionate interference with privacy and other rights, and 'improving' accuracy may only amount to increasing surveillance and disempowerment of an already disadvantaged community.").

III. COMPARATIVE ANALYSIS OF STATE AND LOCAL LAWS ADDRESSING REGULATION

The various laws addressing biometric regulation differ among states and cities regarding the public and private sectors.[89] The longest established biometric laws target private and commercial usage of consumer biometric information.[90] Biometric regulation addressing usage within the public domain, such as law enforcement, is occurring at the local level rather than being addressed by the state governments.[91] There is no federal statute addressing the regulation of private or public usage of biometric information, or how one interacts with the other.[92]

A. Commercial Sector Use

Facial recognition technology has a wide range of uses in the private and business sector. Before the United States reaches a high level of technology integration, similar to the level seen in China, a federal statute is needed to prevent data and security breaches. Biometric information could easily be used to surveil citizens if companies, like Clearview AI, can collect unlimited data as a third-party entity.[93]

Concern about inaccuracies and the potential misuse of biometric data, several major technology companies, such as International Business Machines Corporation ("IBM"), Amazon, and Microsoft, announced they would stop the sale of facial recognition technology to governments.[94] Although these companies have halted sales to police departments in the United States, the top suppliers in the industry are still providing software to

---

89 Julie Carr Smyth, *States Push Back Against Use of Facial Recognition by Police*, ABC NEWS (May 5, 2021, 4:32 PM), https://abcnews.go.com/Politics/wireStory/states-push-back-facial-recognition-police-77510175.

90 Binimow, *supra* note 43.

91 Rachel Metz, *Portland Passes Broadest Facial Recognition Ban in the US*, CNN BUS. (Sept. 9, 2020, 8:06 PM ET), https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html.

92 Alicia Baiardo & Anthony Le, *U.S. Biometrics Laws Part II: What to Expect in 2021*, JDSUPRA (Feb. 8, 2021), https://www.jdsupra.com/legalnews/u-s-biometrics-laws-part-ii-what-to-7257250/.

93 Hill, *supra* note 39.

94 Pam Greenberg, *Facial Recognition Gaining Measured Acceptance*, NAT'L CONF. OF ST. LEGISLATURES (Sept. 18, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/facial-recognition-gaining-measured-acceptance-magazine2020.aspx; Julia Horowitz, *Tech Companies Are Still Helping Police Scan Your Face*, CNN (July 3, 2020, 8:36 AM ET), https://www.cnn.com/2020/07/03/tech/facial-recognition-police/index.html. Amazon has enacted a one-year moratorium and Microsoft's president has called for "'a strong national law grounded in human rights.'" *Id.*

United States law enforcement departments.[95] Companies like Facebook, Shutterfly, Ring LLC, and Instagram have not taken similar preemptive action likely because the usage of photos and videos is directly linked with the purpose of the platforms.[96] These platforms rely on the users interacting with ease. Although facial recognition software may make it easier for users to connect, several lawsuits have been brought against private companies, like Facebook, Shutterfly, Ring LLC, and Instagram, for alleged violations of Illinois' BIPA statute.[97] The lawsuits allege that these companies are using and retaining consumer data without consent.[98]

B. Current Laws Governing Biometric Identification Usage

The definition of "biometric" differs among statutes from a more tailored definition used by Illinois and Texas to a broader definition used by Washington.[99] Illinois, Texas, and Washington are at the forefront of shaping United States biometric privacy laws.[100] These three states' biometric laws apply to the commercial uses of biometric information.[101] While other states have data privacy laws, Illinois, Texas and Washington's regulations extend to "specific instances of biometric collection."[102] Comparatively, laws in California, New Hampshire, and Oregon are directed at facial recognition software in police body cameras.[103] The Illinois and Texas statutes have been enacted since 2008 and 2009 respectively; Washington more recently enacted its statute in 2017.[104] These laws vary in their protection of consumer

---

95 Horowitz, *supra* note 94. US vendor, Clearview AI, and foreign venders such as "Japan's NEC and Ayonix, Germany's Cognitec and Australia's iOmniscient . . ." have maintained their business relationships with American police departments. *Id.*

96 *See generally* Dominique Jackson, *Instagram vs Facebook: Which is Best for Your Brand's Strategy?*, SPROUTSOCIAL: SPROUTBLOG (June 30, 2019), https://sproutsocial.com/insights/instagram-vs-facebook/ (discussing the pros and cons of Facebook and Instagram, the structure of the platforms, and how individuals use it to engage and create content).

97 Class Action Complaint, Wise v. Ring LLC, No. 20-2-11887-7 SEA (Wash. Super. Ct. filed July 29, 2020); Class Action Complaint, Whalen v. Facebook, No. 20-civ-03346 (Cal. Super. Ct. filed Aug. 10, 2020); JOHN FITZGERALD, LAWSUIT: RING USES BIOMETRIC DATA FROM VIDEOS WITHOUT CONSENT (Thomson Reuters 2020), 27 No. 07 Westlaw Journal Class Action 05; Robert Burnson, *Instagram Faces Lawsuit Over Illegal Harvesting of Biometric Data*, BLOOMBERG (Aug. 13, 2020, 1:04 IST), https://www.bloomberg.com/news/articles/2020-08-12/facebook-s-instagram-targeted-in-new-lawsuit-over-biometrics; *see* Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019); discussion *infra* Section III.B (discussing the Illinois BIPA statute).

98 Class Action Complaint, Wise v. Ring LLC, *supra* note 97; Class Action Complaint, Whalen v. Facebook, *supra* note 97; Patel v. Facebook, Inc., 932 F.3d.

99 Benson, *supra* note 20.

100 Binimow, *supra* note 43.

101 TEX. BUS. & COM. CODE ANN. § 503.001 (West 2009); 740 ILL. COMP. STAT. 14/ (2008); WASH. REV. CODE § 40.26.020 (2017).

102 Benson, *supra* note 20.

103 Greenberg, *supra* note 94.

104 Binimow, *supra* note 43; BUS. & COM. § 503.001; § 14/; REV. § 40.26.020.

information, but do not provide restrictions on public use.[105] However, some large cities have implemented local ordinances regulating the use of facial recognition by the local police departments.[106]

The Illinois Biometric Information Privacy Act ("BIPA") was enacted in 2008.[107] It regulates what private entities are able to do with collected biometric information.[108] A private entity must have the following requirements to collect biometric information: (1) consent for the collection, (2) consent for disclosure and dissemination, (3) a prohibition against profiting, (4) a retention policy, and (5) a reasonable standard of care.[109] Although it is the oldest and most expansive statute, Illinois residents have only recently begun to bring suits under BIPA for the dissemination of their information.[110]

In 2009, Texas passed the Capture or Use of Biometric Identifier Act ("CUBI") regulating biometric technology uses by private entities with similar requirements as BIPA.[111] It provides less recourse for Texas residents, compared to the BIPA, because the only enforcement mechanism is through the attorney general.[112] Whereas Illinois' BIPA contains a private right of action with "liquidated damages of [one thousand dollars] per negligent violation [or five thousand dollars] per intentional or reckless violation."[113]

Washington enacted a biometric statute regulating commercial uses of biometrics, but expressly provided exceptions for "security or law enforcement."[114] In March 2020, Washington passed a new facial recognition privacy statute that requires "extensive accountability reports . . . human review of consequential decisions made, significant testing to prevent discriminatory effects, a warrant requirement and other restrictions."[115]

---

105 BUS. & COM. § 503.001; § 14/; REV. § 40.26.020.

106 Metz, *supra* note 91; PORTLAND, OR., ORDINANCE ch. 34.10 (2020) (prohibiting the use of facial recognition technologies by private entities in places of public accommodation); S.F., CAL., ADMIN. CODE ch. 19(B) (2019) (forbidding the use of facial-recognition technology by city departments); OAKLAND, CAL., ORDINANCES ch. 9.64.010 (2019) (banning the use of facial recognition technology or information obtained from it); Detroit Police Dep't, Manual Directive 307.5 (Sept. 12, 2019) (approving usage of facial recognition software, but not to assess immigration status or on live or recorded video).

107 § 14/.

108 § 14/15.

109 NOLAN, *supra* note 27.

110 *Id.*; § 14/. *See generally* Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103 (N.D. Ill. 2015); Rivera v. Google, Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2018); Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020); Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019); Binimow, *supra* note 43.

111 NOLAN, *supra* note 27; § 14/.

112 Benson, *supra* note 20; TEX. BUS. & COM. CODE ANN. § 503.001 (West 2009).

113 NOLAN, *supra* note 27.

114 *Id.*

115 Jim Halpert, *In Washington State's Landmark Facial Recognition Law, Public Sector Practices Come Under Scrutiny and Regulation*, DLA PIPER (Apr. 22, 2020), https://www.dlapiper.com/en/us/insights/publications/2020/04/in-washington-states-landmark-facial-recognition-law-public-

Although Illinois, Texas, and Washington lead the United States in biometric law, "there is a notable trend towards state regulation of biometric data."[116] On January 1, 2020, California and Oregon's consumer biometric protections became effective.[117] Eleven other states have proposed biometric privacy bills without success.[118] Currently three have pending legislation.[119] The COVID-19 pandemic delayed any potential progress that may have been made by states without biometric information laws but had been considering legislation.[120] In 2021, New York and Maryland have introduced bills similar to the Illinois BIPA.[121]

C. At a Local Level

Several large cities have addressed the use of facial recognition by their police departments.[122] For example, the New York Police Department ("NYPD") has an internal policy detailing the "scope, uses and procedures" for using facial recognition technology.[123] It is the NYPD's policy that "[f]acial recognition technology must only be used for legitimate law enforcement purposes."[124] The New York Supreme Court has held that facial recognition matches do not create probable cause for arrest but provide a source for police investigation.[125]

---

sector-practices-come-under-scrutiny/. The statute contains the first use of a definition regarding decisions that produce legal effects. *Id.*

116 Natalie A. Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, THE NAT'L L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.

117 Kristine Argentine & Paul Yovanic, *The Growing Number of Biometric Privacy Laws and the Post-COVID Consumer Class Action Risks for Businesses*, JDSUPRA (June 9, 2020), https://www.jdsupra.com/legalnews/the-growing-number-of-biometric-privacy-62648/.

118 *Id.*

119 *Id.* Past unsuccessful legislation includes Michigan, Alaska, Delaware, Florida, New Hampshire, Montana, and Rhode Island. *Id.* Current legislation includes Massachusetts, Hawaii, and Arizona. *Id.*

120 Argentine & Yovanic, *supra* note 117; *2020 Consumer Data Privacy Legislation*, NAT'L CONF. OF ST. LEGISLATURES (Jan. 17, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx (listing proposed bills with biometric privacy aspects in 2020 and whether the bills are pending, failed, adjourned, or were enacted). Sixteen bills are still pending in Puerto Rico, Virginia and New Jersey. *Id.* Only five bills were enacted: three from California, one in Michigan, and one in Virginia. *Id.*

121 Jad Sheikali, *Recent State Biometric Privacy Bills Put Spotlight on Federal Regulation*, HONIGMAN (Apr. 28, 2021), https://www.honigman.com/blogs-the-matrix,recent-state-biometric-privacy-bills.

122 Susan Crawford, *Facial Recognition Laws Are (Literally) All Over the Map*, WIRED (Dec. 16, 2019, 8:00 AM), https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/.

123 Press Release, N. Y. Police Dep't, NYPD Announces Facial Recognition Policy (Mar. 13, 2020) (on file at https://www1.nyc.gov/site/nypd/news/pr0313/press-release---nypd-facial-recognition-policy).

124 *Id.* (listing the six specific authorized uses for facial recognition technology).

125 People v. Reyes, No. 3351-19 (N.Y. Sup. Ct. Oct. 7, 2020).

Cities other than New York have begun to take action. Detroit's City Council approved a contract between the Detroit Police Department and DataWorks Plus to continue its surveillance program.[126] Portland, San Francisco, Oakland, and Boston have passed bans on the use of facial recognition by the cities, with Portland's ban going further to target local police and public business use.[127] The Chicago Police Department cut ties with Clearview AI after the American Civil Liberties Union filed a lawsuit alleging privacy violations.[128]

The New York Times published an article exposing controversial uses of data collected by Clearview AI by federal and state law enforcement agencies.[129] The Clearview AI system collects images from Facebook, YouTube, Venmo, and other sites.[130] It then creates a database for law enforcement to search against and provides links to the images' origin.[131] To highlight the difference between facial recognition searches twenty years ago and searches today, previously images were solely obtained from government systems such as drivers licenses, state IDs passports, and mugshots.[132] Now, photographs are taken from the internet, without the knowledge or consent of the specific individual, creating a database of more than three billion images.[133] Law enforcement agencies have been using the databases of third-party companies, like Clearview AI, to perform searches for suspected criminals.[134] Once images are uploaded, the servers store the pictures that were uploaded.[135] So in turn, "[t]he algorithms [law enforcement] rely on have likely been trained [using] pictures obtained without the subject's consent."[136]

IV. ON A GLOBAL SCALE

The use of biometric identifiers, specifically facial recognition, also occurs internationally.[137] This practice is already being abused as a method

---

126 Newman, *supra* note 72.

127 Metz, *supra* note 91.

128 Associated Press, *Chicago Police Drop Clearview Facial Recognition Technology*, U.S. NEWS AND WORLD REP. (May 29, 2020), https://www.usnews.com/news/best-states/illinois/articles/2020-05-29/chicago-police-drop-clearview-facial-recognition-technology.

129 Hill, *supra* note 39.

130 *Id*.

131 *Id*.

132 *Id*.

133 Rebecca Heilweil, *The World's Scariest Facial Recognition Company, Explained*, VOX (May 8, 2020, 11:51 AM EDT), https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement.

134 Hill, *supra* note 39.

135 *Id*.

136 Lindsey Barrett, *Ban Facial Recognition Technologies for Children - and for Everyone Else*, 26 B. U. J. SCI. & TECH. L. 223, 242 (2020).

137 Rowe, *supra* note 39.

of control for assembly and free speech.[138] Surveillance of protests serves to deter activism with the threat of arrest.[139] China has an extensive facial recognition program that is regulated by the Cybersecurity Law of the People's Republic of China.[140] Chinese companies have used the technology in a variety of ways, including to assess the health of potential clients, levels of honesty, or if the person is a smoker.[141] Facial recognition software is also used as payment methods for "vending machines, grocery stores, bakeries, subway systems and hospitals."[142] Additionally, this technology is being used on protestors in Hong Kong and to identify Uighur peoples, an ethnic minority in China.[143] In addition to facial recognition, other biometric identifiers, such as DNA collection, are allegedly being taken from the Uighurs.[144]

Chinese facial recognition companies comprised "nearly half of the global facial recognition business in 2018."[145] Over sixty countries are utilizing Chinese technologies for security and crime tracking.[146] There are concerns of human rights violations with providing surveillance technology to authoritarian governments.[147] China's dominance in the market could influence a "culture of surveillance" and encourage new societal uses for facial technology.[148] Government oppression of free speech, assembly, or

---

138 Khazan, *supra* note 13.

139 Sharon Tam & Jessie Pang, *First Hong Kong Protester to Admit 'Rioting' Gets Four Years'* [sic] *Jail*, REUTERS (May 15, 2020, 4:53 AM), https://www.reuters.com/article/us-hongkong-protests-court/first-hong-kong-protester-to-admit-rioting-gets-four-years-jail-idUSKBN22R1DZ; *see also* Michael Schuman, *Angering China Can Now Get You Fired*, THE ATLANTIC (Aug. 27, 2019), https://www.theatlantic.com/international/archive/2019/08/beijing-pressure-hong-kong-companies/596869//. Participating in the Hong Kong protests led to the suspension of a pilot and firings of cabin crew members. *Id.*

140 Rogier Creemers et al., *Translation: Cybersecurity Law of the People's Republic of China*, NEW AM. (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

141 Rowe, *supra* note 39.

142 *Id.*

143 Sherman, *supra* note 12.

144 Rowe, *supra* note 39.

145 Yang & Murgia, *supra* note 15.

146 *Id.*; Rowe, *supra* note 39. According to the Carnegie Endowment for International Peace, sixty-three countries have implemented Chinese artificial intelligence facial recognition technology, including the United States. Rowe, *supra* note 39, at 20.

147 Yang & Murgia, *supra* note 15.

148 Charlie Campbell, *How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens*, TIME: DAVOS 2019, https://time.com/collection/davos-2019/5502592/china-social-credit-score/ (last visited Sept. 16, 2021); Eric Olander, *China, Africa, and the Future of the Internet*, THE CHINAFRICA PROJECT (June 23, 2019), https://chinaafricaproject.com/podcasts/podcast-china-africa-internet-iginio-gagliardone/. Iginio Gagliardone posits that Chinese technology in Africa is being used by governments to prevent dissent and surveil their citizens. Olander, *supra*. A new system of "social credit" can affect all aspect of an individual's life and uses facial recognition to identify blacklisted or socially irresponsible individuals. *Id.*; *see* Sheridan Prasso, *China's Digital Silk Road is Looking More Like an Iron Curtain*, BLOOMBERG BUSINESSWEEK (Jan. 9, 2019, 11:01

unlawful surveillance are inconsistent with the values and foreign policy of the United States. A federal biometric statute would express this position.

The advances in facial recognition technology have not been accompanied by equivalent regulation or sufficient enforcement of the regulations passed.[149] In October 2019, the first facial recognition lawsuit in China was filed.[150] A wildlife park upgraded their biometric identification technology from fingerprint scanning to facial recognition.[151] A law professor sued after requesting a refund when he learned the park would be using visitors' facial biometric data from a photo provided when signing up for an annual pass.[152] The park had switched to using a facial recognition system without any prior consent from the visitors.[153] The plaintiff brought suit under the legal theory of breach of contract because Chinese law does not regulate the collection of biometric information.[154] The court held that the wildlife park could not retain biometric facial data without the visitor's consent.[155] As a country leading in the advancement of facial recognition technology, this lawsuit signals possible willingness to protect and regulate these new technological systems.[156] This lawsuit has been significant in the city of Hangzhou, China, headquarters to many technology companies, for the consideration of a ban on property management companies requiring biometric data.[157] However, the concerns regarding the use of biometric information may be more related to data breaches, rather than oppressive government usage against dissidence.[158]

Protestors in China have used different techniques to counter the extensive surveillance.[159] Face masks, headgear, umbrellas, lasers, destroying cameras, and cutting down lampposts are done in an effort to prevent identification and a possible ten-year jail sentence.[160] In response to

---

PM EST), https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain.

149 Rowe, *supra* note 39.

150 Shen Lu, *Facial Recognition Is Running Amok in China. The People are Pushing Back.*, VICE (Dec. 10, 2020, 12:45 AM), https://www.vice.com/en/article/4adnyq/facial-recognition-is-running-amok-in-china-the-people-are-pushing-back.

151 *Id.*

152 *Id.*

153 *Id.*

154 *Id.*

155 *Id.*

156 Lu, *supra* note 150.

157 *Id.*

158 Yang & Murgia, *supra* note 15. A survey showed the Chinese public is concerned about data leaks, but most people approved of the use for security and convenience. *Id.* There is a contrast between how the privacy debate is framed and leaks to third parties in China versus the debate in the United States regarding the government or companies surveilling people. *Id.*

159 Sidney Fussell, *Why Hong Kongers are Toppling Lampposts*, THE ATLANTIC (Aug. 30, 2019), https://www.theatlantic.com/technology/archive/2019/08/why-hong-kong-protesters-are-cutting-down-lampposts/597145/.

160 *Id.*; Tam & Pang, *supra* note 139.

the use of face covings, facial recognition technology has been updated to identify faces even when covered.[161] As a result of the COVID-19 pandemic, this technology has also incorporated thermal imaging and mask recognition.[162]

China's reaction to protests in Hong Kong foreshadowed the United States' reaction to the George Floyd protests.[163] Deployment of security forces, extensive surveillance, numerous arrests and suppression of the press were present at protests in China and the United States.[164] The United States has signaled it disagrees with oppression in China and yet ironically practiced similar tactics during the George Floyd protests.[165] Both governments' attempted suppression of freedom of assembly, speech, and press and the use of physical force and digital surveillance should signal concern.[166] A deadly combination of physical and digital suppression is not an image the United States should convey as a leading democratic republic. Instead of using similar tactics, the United States needs a legal foundation to prevent future violations of privacy.

V. PROPOSED COMPONENTS OF A FEDERAL STATUTE REGULATING THE USE OF BIOMETRIC INFORMATION

The current proposed federal bills do not wholly address the risks posed by the use of biometric technology. There are two bills that propose a moratorium on facial recognition technology.[167] Another bill proposes limitations and regulations, but only for private entities.[168] However, there is no bill with a suggested process for federal and state governments to regulate and use biometric technology.[169] The proposal in this note specifically addresses the use of biometric technology by federal, state, and local governments as well as private commercial use. This proposal will also include the use of mandatory monitoring, updating, and studying of the biometric software systems. This issue creates a rare opportunity for

---

161 Seungha Lee, *Coming into Focus: China's Facial Recognition Regulations*, CTR. FOR STRATEGIC & INT'L STUD. (May 4, 2020), https://www.csis.org.

162 Rowe, *supra* note 39.

163 Sahil Singhvi, *Disturbing Parallels in Crackdowns on Protestors in the U.S. and Hong Kong*, BRENNAN CTR. FOR JUST. (Oct. 29, 2020), https://www.brennancenter.org/our-work/analysis-opinion/disturbing-parallels-crackdowns-protesters-us-and-hong-kong.

164 *Id.*

165 *Id.*

166 *Id.*

167 S. 4084, 116th Cong. (2020); H.R. 7356, 116th Cong. (2020).

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

169 *See* Nerissa Coyle McGinn, *FTC, Federal and State Lawmakers Signal Focus on Biometric Data*, LOEB & LOEB LLP (Mar. 2021), https://www.loeb.com/en/insights/publications/2021/02/ftc-federal-and-state-lawmakers-signal-focus-on-biometric-data.

bipartisan agreement.[170] A comprehensive bill to address both public and private usage is possible with the current alignment of political and commercial concern.[171]

A. Current Proposed Federal Biometric Information Bills

There are multiple federal bills introduced addressing facial recognition and biometric regulation from the 116th and 117th sessions of Congress.[172] The first of the introduced bills would prohibit the use of biometric surveillance technology by federal law enforcement and render local or state governments ineligible for federal law enforcement funds if they fail to comply with similar restrictions regarding biometric identification systems.[173] If a comprehensive federal biometric statute were enacted, congress would need to enact a separate statute that gives specific authorization to agencies for the use of biometric systems.[174] In contrast, the second bill proposes regulations for "the collection, retention, disclosure, and destruction of biometric information, and for other purposes" by private entities.[175] The last bill would require the Department of Commerce to report and study possible effects, risks, and trends of facial recognition within industry sectors and their federal agencies.[176] The U.S. Chamber of Commerce has also released facial recognition policy principles to guide policymakers to the mitigate risks and increase the benefits.[177]

---

170 *Id.*

171 Drew Harwell, *Senators Seek Limits on Some Facial-Recognition Use by Police, Energizing Surveillance Technology Debate*, WASH. POST (Apr. 21, 2021, 3:29 PM), https://www.washingtonpost.com/technology/2021/04/21/data-surveillance-bill/; *See generally* Fussell, *supra* note 158. Republicans and Democrats are both concerned with the potential risks along with private corporations like Microsoft, Amazon, and Axon. *Id.*

172 H.R. 6929, 116th Cong. (2020); S. 4084; S. 4400; H.R. 7356; S. 3284, 116th Cong. (2020); H.R. 3907, 117th Cong. (2021); S. 1265, 117th Cong. (2021); Olivia Solon, *Facial Recognition Bill Would Ban Use by Federal Law Enforcement*, NBC NEWS (June 25, 2020, 12:08 PM CDT), https://www.nbcnews.com/tech/security/2-democratic-senators-propose-ban-use-facial-recognition-federal-law-n1232128.

173 Solon, *supra* note 172; S. 4084; H.R. 7356; H.R. 3907; S. 3284 (proposing the prohibition of engaging in activities using facial recognition technology without a warrant until legislation is passed establishing guidelines). The House and Senate bills propose the same moratorium on biometric technology. S. 4084; H.R. 7356; H.R. 3907; S. 3284.

174 S. 4084; S. 3284.

175 S. 4400.

176 H.R. 6929.

177 *See* U.S. CHAMBER OF COM., FACIAL RECOGNITION POLICY PRINCIPLES (2019), https://www.uschamber.com/issue-brief/us-chamber-facial-recognition-policy-principles-0.

B. A Proposal for a Federal Bill

This note proposes that a federal biometric information technology bill should specifically address the use of biometric identifiers by law enforcement as well as private commercial use. Local law enforcement has demonstrated it will contract with third-party organizations providing facial recognition technology.[178] Although state governments have broad reign to decide how law enforcement is conducted within their state, Congress could incentivize compliance with any restrictions in a federal statute or regulation by providing federal grants to states that follow federal regulations.[179] The federal government can attach conditions to federal grants as long as the terms are not ambiguously established, it is enticement and not coercion, it does not violate any provisions of the Constitution, and the conditions are related to the purpose of the federal funds.[180] An optional provision would allow states to create their own oversight teams that comply with federal guidelines. The federal funds would be an incentive to comply with any federal restrictions or reports from independent committees analyzing the technology for bias.

The bill should contain standards and methods to review for possible adverse effects of using facial recognition. The algorithms should be regularly monitored for disproportionate results based on race, gender, and age.[181] Similar to the proposed bill, H.R. 6929, one section would set up a committee to conduct studies and provide reports to ensure accountability, transparency, and consistency with the use of facial recognition technology.[182]

A committee of technology experts would be created to provide recommendations for revision to any government biometric information systems.[183] This committee would help to mitigate unjust results by ensuring the facial recognition algorithms are regularly tested and updated to prevent biases. By keeping technology as up-to-date as possible, facial recognition algorithms can be continually trained to incorporate diversity. The committee could meet on a scheduled basis to review the usage of facial recognition systems within the government. Including protections for "privacy, free

---

178 Newman, *supra* note 72.

179 Solon, *supra* note 172.

180 CONG. RSCH. SERV., R44797, THE FEDERAL GOVERNMENT'S AUTHORITY TO IMPOSE CONDITIONS ON GRANT FUNDS 7 (2020); U.S. CONST. art. 1, § 8, cl. 1. Congress can attach conditions to federal grants under the Spending Clause. *See generally* South Dakota v. Dole, 483 U.S. 203 (1987); Bell v. New Jersey, 461 U.S. 773 (1983).

181 Solon, *supra* note 172.

182 H.R. 6929, 116th Cong. (2020).

183 *See generally Bureaus and Offices*, U.S. DEP'T OF COM., https://www.commerce.gov/bureaus-and-offices (last visited Jan. 11, 2021).

speech, and racial, gender and religious equality" should be a top priority throughout the drafting of the bill.[184]

In addition to restrictions and oversight, a data retention policy would be recommended for state law enforcement and required for federal law enforcement. Once an individual's images have been put into the search system, it should not be retained indefinitely where no arrests or charges were made. Whether a warrant should be obtained for each search may be considered too burdensome. However, a system to document when and why an image was searched would need to be implemented. The system would also require a brief statement as to how the image was obtained. In addition to guidelines for public use, the inclusion of requirements used by the Illinois BIPA for commercial biometric usage would provide protection for consumer information. Current lawsuits show that BIPA does provide actual protection and remedies for commercial use.[185] Since the comprehensive federal statue would address public and private biometric information use, the remedies should expand to include injunctive relief and criminal charges for misuse.

Washington's new public sector facial recognition statute contains requirements and limitations on state and local government agencies that promote accountability when using the system.[186] To promote accountability, the federal bill should contain a section dedicated to government transparency when using and entering into contracts with companies that specialize in biometric identification. A combination of private and public requirements would provide adequate remedies, accountability, and enforcement procedures.

A suggested structure for this bill would include the first part of the bill to define relevant terms such as biometric identifiers, different types of facial recognition technology, private entities, and governmental agencies.[187] A brief suggestion for sections and statute language is as follows:

> Section for Purpose:
>
> - To regulate the collection, retention, and destruction of consumer biometric data by private entities.
> - To create a procedure to ensure transparency and continuous oversight of governmental use of facial recognition algorithms and systems.

---

184 Solon, *supra* note 172.

185 Hazlitt v. Apple, Inc., 500 F. Supp. 3d 738 (S.D. Ill. 2020); Rivera v. Google, Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017); *See generally* Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019). BIPA creates concrete privacy interests and violations harm or pose a material risk of harm to those interests. *Id.*

186 Halpert, *supra* note 115.

187 CONG. RSCH. SERV., R46586, FEDERAL LAW ENFORCEMENT USE OF FACIAL RECOGNITION TECHNOLOGY 2 (2020).

- To use the advantages of biometric information technology with an established process to prevent potential misuses and errors and uphold constitutional protections.
- To invite state compliance with federal regulations and policy by providing federal funds to those that comply.

Section for Private Entity Usage of Biometric Information:

- A private entity must develop a policy to collect, retain, and destroy biometric data. Biometric data from facial recognition technology must be obtained with the written consent of the individual.
- A private entity must have sufficient security to prevent biometric data breaches.
- Collection of such data must have a publicized policy to prevent indefinite retention, to prevent the unlawful selling of biometric data, and to protect individuals' unique biometric markers.

Section for Federal Biometric Information Technology Use:

- Unless authorized by a separate federal statute, regulation, or order, the use of biometric identification such as facial recognition shall be limited to law enforcement and surveillance related to criminal offenses. Written approval should be sought for continued surveillance. Positive facial recognition matches do not provide probable cause to make an arrest. A departmental policy shall be required for each positive facial recognition match to be separately confirmed to prevent misuse as evidence and deter sole reliance on facial recognition systems.
- Special authorization shall be required for real-time or live video facial recognition surveillance.
- Federal funding to be made available to States willing to comply with and incorporate recommended federal guidelines and biometric information protection policy.

Section for Penalties for Noncompliance:

- Private Cause of Action Against Commercial and Government Entities.

    - Tiered fines beginning at five thousand dollars per consumer for private entities.
    - Additional fines dependent on the amount of violations, duration the violations lasted, and for intentional or reckless behavior.
    - Damages in civil suits against law enforcement.
    - Injunctive relief.
- Governmental Action at Federal, State and Local level.
    - Suspension.
    - Termination.
    - Police misconduct investigations or lawsuits.
    - Injunctive relief.
- Failure to receive federal funding for governmental violations.

Section for Independent Review:

- This act would authorize the creation of an independent committee to conduct annual reviews of the facial recognition system to ensure compliance with established procedures to reduce any potential impacts on civil rights, liberties, privacy, and marginalized communities.

If a partisan agreement cannot be reached for proposed sections of the federal privacy bill, a moratorium on federal use of facial recognition technology should be implemented until a decision can be made. It is important to prevent irreversible harm from occurring. The threat to an individual's biometric information is substantial because a person's characteristics are unique and cannot be replaced. The Supreme Court's Fourth Amendment doctrines may never hold facial recognition systems constantly used in public places are unreasonable; however, Congress can remedy this potential issue by passing a statute to limit law enforcement's continuous usage of these systems on the public. By creating a federal statute to regulate the expansive possible uses of the technology, businesses, federal, and state governments will be held accountable and restricted from abusing biometric data.

VI. ADDITIONAL COMMENT FOR SUPREME COURT ACTION

In addition to the United States' need for a federal statute addressing biometric identification usage by private and public entities, the Supreme Court will need to address the constitutionality of use of biometric information within the Fourth Amendment and the right to privacy in the near future. The Fourth Amendment provides an individual protection against unreasonable search and seizure.[188] One of the first cases involving facial recognition technology will likely be related to the commercial use of consumer biometric data. One issue these third-party companies pose is the retention of images that were uploaded and removed.[189] One company created a safeguard for images by using its link, instead of the actual photo, and making the link invalid if the user deleted or made the image private.[190] Whether the Court will view uploaded photos as "forever on the Internet" and in the public domain, or still within the account owner's control, will be an essential element in solving complex legal questions about biometric identification technology. The Court could allude to their stance on the government use of facial recognition technology if a commercial data use case reaches the Supreme Court. It is likely there will be future cases regarding the constitutionality of law enforcement's usage of facial recognition technology.

The protection for unreasonable searches and seizures in the Fourth Amendment is at the heart of this issue. Running faces though facial recognition software should be considered a search under the Fourth Amendment.[191] The degree to which facial recognition technology aids police officers is arguably far outside one's "natural senses" and in other situations, a search warrant would be needed to obtain similar identification information.[192]

When presented with a first impression facial recognition case, the Court will look to Fourth Amendment precedent and its evolution; however, the digital nature of the technology may require a new category of Fourth Amendment doctrine. Justice Sotomayor and Justice Alito have both

---

188 U.S. CONST. amend. IV.

189 Rowe, *supra* note 39.

190 *Id.*

191 Julian R. Murphy, *Chilling: The Constitutional Implications of Body-Worn Camera and Facial Recognition Technology at Public Protests*, 75 WASH. & LEE L. REV. ONLINE 1, 16-17 (2018), https://scholarlycommons.law.wlu.edu/wlulr-online/vol75/iss1/1/ (suggesting that the avenue for the Court to consider it a "search" under the Fourth Amendment is through First Amendment concerns); *See generally* Matthew Doktor, *Facial Recognition and the Fourth Amendment in the Wake of* Carpenter v. United States, 89 U. CIN. L. REV. 552, 566 (2021) (suggesting a minimum requirement to prevent privacy abuses would be to require a warrant).

192 Murphy, *supra* note 191; *see* Kyllo v. United States, 533 U.S. 27 (2001); United States v. Jones, 565 U.S. 400 (2012).

discussed how new technology will require different understandings of what the Fourth Amendment means in the twenty-first century.[193] The Court may distinguish between searches conducted on an individual in public versus an individual taking reasonable precautions to protect their identity online. Biometric data from photos has the potential to reveal intimate details about an individual's life as well as provide a timeline of their activities.[194]

A Fourth Circuit District Court extended *Carpenter*'s reasoning to cases involving social media finding there is a reasonable expectation of privacy.[195] The court evaluated whether the defendant intentionally took steps to prevent the public from accessing select content on his Facebook profile.[196] As technology advances and becomes more capable of delving into an individual's personal life, the third-party doctrine may become outdated and less relevant to Fourth Amendment analysis.[197] The complexity of this issue will be discussed by the Court in future years, but basic constitutional guidelines would aid Congress with navigating the boundaries of the Fourth Amendment while drafting a federal statute.

VII. CONCLUSION

Biometric identifiers have vast potential contributions to society; they have already advanced technology for the next century. The ability to use unique facial structures, physical characteristics and one's physiology has the potential to create unparalleled tools within the consumer, security, and employment sectors. However, this potential comes with the threat of equally terrible abuses of power. Private companies' actions to slow the access of facial recognition technology to state governments reflect public concern regarding the use and potential abuse of biometric data.

Currently, state laws do not uniformly approach the issue of facial recognition. Three out of fifty states have laws specifically addressing commercial abuses of biometric information and none have statutes restricting use by law enforcement. A federal statute is necessary to show the United States is concerned with the potential abuses of biometric identification both domestically and globally. China has surpassed the United States with the use of facial recognition technology and is providing it to other countries.

---

193 United States v. Jones, 565 U.S. (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."); Doktor, *supra* note 191.

194 Doktor, *supra* note 191.

195 *Id.*

196 United States v. Chavez, 423 F. Supp. 3d 194, 202 (W.D.N.C. 2019).

197 Doktor, *supra* note 191.

Before companies like Geofeedia, DataWorks Plus or Clearview AI improve their existing technology to exceed and violate United States citizen's privacy rights, the United States' federal government needs to provide clarity and limitations. Uniform limits to what can be done with biometric information by the government and private companies should be addressed by Congress. A federal bill should address both the commercial sector use and law enforcement. In contrast to China, the United States needs to take a firm stance to protect its citizens' privacy rights from overreaches of power and data breaches. While government entities have already begun to utilize facial recognition systems, they have avoided creating their own databases by using third-party companies' databases that compile images from the internet. It may only be a matter of time before public systems are created to search images pulled from the internet. To fully utilize the positive advantages of facial recognition and biometric identification technology, there must be a federal statute to regulate public and private usage and reduce the threats that accompany it.

As a super-surveillance state, China has integrated advanced technology to monitor social media, the internet, and the general public. Freedom of assembly, speech, or ideology are repressed and censored with the aid of biometric technology like facial recognition. Although the United States' Constitution, explicitly and implicitly, provides for certain fundamental freedoms, the descent into oppression often occurs without notice.