Marquette Intellectual Property & Innovation Law Review

Volume 25 | Issue 1 Article 5

Winter 2021

Regulating Facial Recognition Technology In An Effort To Avoid A Minority Report Like Surveillance State

Halie B. Peacher

REGULATING FACIAL RECOGNITION TECHNOLOGY IN AN EFFORT TO AVOID A MINORITY REPORT LIKE SURVEILLANCE STATE

HALIE B. PEACHER

ABSTRACT

In Steven Spielberg's science fiction film Minority Report, the film focuses on how technology is used in the future, as well as how society uses and understands that technology. Specifically, Minority Report focuses on eye-scanners that allow the police and corporations to track down and identify people on a daily basis. This movie identifies that there is a clear line that must be drawn between an individual's right to privacy and the law enforcement agency's ability to ensure safety. Like the technology in Minority Report, the use of facial recognition technology has led to much debate, mainly focused on privacy and civil liberties, but also encompassing constitutional and other legal concerns. These debates will raise very difficult questions regarding what a privacy right even entails and how much surveillance an individual is willing to allow with the hopes of a safer lifestyle. The discussion on how the United States utilizes facial recognition technology shows what a world looks like when unregulated surveillance techniques clash with highly protected constitutional rights, while the discussion on how China utilizes facial recognition technology shows what happens when a government is left to surveil individuals with no repercussions at all. Both the United States and China are presently using facial recognition technology in a manner that is unacceptable. Individuals' rights and freedoms must be guaranteed to avoid a draconian surveillance state where all privacy and civil liberties disappear into the lens of a camera.

In this paper, I will first explain facial recognition technology. Second, I will compare the United States' use of facial recognition technology with how China is using facial recognition technology. Third, I will discuss the privacy and legal concerns surrounding facial recognition technology in the United States and in China. Finally, I will discuss the best way of regulating this technology in a manner that: (1) ensures that individuals are granted inherent freedoms, such as the right to privacy and freedom of expression; (2) does not

stifle technological innovation; and (3) allows the government to make use of facial recognition technology.

I. INTRODUCTION

The use of facial recognition technology has led to much debate mainly focused on privacy and civil liberties, but also encompassing constitutional and other legal concerns. As more issues arise, it would be wise to develop a framework or regulation that lessens some of the individual concerns surrounding the use of facial recognition technology. In this paper, I will first explain facial recognition technology. Second, I will compare the United States' use of facial recognition technology with how China is using facial recognition technology. Third, I will discuss the privacy and legal concerns surrounding facial recognition technology in the United States and in China. Finally, I will discuss the best way of regulating this technology in a manner that: (1) ensures that individuals are granted inherent freedoms, such as the right to privacy and freedom of expression; (2) does not stifle technological innovation; and (3) allows the government to make use of facial recognition technology.

II. WHAT IS FACIAL RECOGNITION TECHNOLOGY?

Facial recognition technology is a biometric technology that "identif[ies] individuals by measuring and analyzing their physiological or behavioral characteristics."[1] This technology is comprised of a camera and an algorithm which simply could analyze photos. Once the camera captures the face of an

1. U.S. Gov't Accountability Office, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*, at 3 (2015), http://www.gao.gov/assets/680/671764.pdf.

unknown person or an unknown person's photograph is uploaded, the algorithm compares that "faceprint" of the unknown person with the images within the database of known people.[2] This facial recognition database is a system that can analyze visual data of millions of images and videos collected from Closed-Circuit Television (CCTV) cameras that are installed around cities, driver's license databases, government identification records, mugshots, and social media accounts.[3]

The technology generally provides machine learning and artificial intelligence capabilities included in the software that can distinguish facial features mathematically by looking for patterns in the visual data and then comparing new images and videos to determine identity.[4] On a more technical level, facial recognition technology creates a template of an unknown person's face. The template is measured through specific characteristics, also referred to as nodal points, such as the distance between the eyes, the width of the nose, and the length of the jaw line.[5] The nodal points are then translated into a template with a unique code.[6]

Facial recognition is most commonly utilized in consumer technology applications for unlocking smartphones or categorizing a person's Facebook and Google images.[7] In addition, facial recognition centers like Amazon, Microsoft, Google, and Clearview AI are making a practice out of selling or licensing this software to law enforcement agencies.[8] More recently, smaller companies like Idemia, Morpho Trust, Gemalto, and NEC have become big players in supplying local and state law enforcement agencies with facial recognition technology capabilities.[9] The federal government has invested approximately one billion dollars in the FBI's Next Generation Identification system ("NGI") database as well as the Face Analysis, Comparison, and

2. U.S. Gov't Accountability Office, *Facial Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, at 2 (2016), http://www.gao.gov/assets/680/677098.pdf.

3. Bernard Marr, *Facial Recognition Technology: Here are the Important Pros and Cons*, FORBES (Aug. 19, 2019), https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/#491c16da14d1.

4. *Id.*

5. Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will it Take Us?*, ABA (Feb. 19, 2020), https://www.americanbar.org/groups/criminal_ justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/.

6. *Id.*

7. Nila Bala & Caleb Watney, *What are the Proper limits on Police Use of Facial Recognition?*, BROOKINGS INSTITUTE (June 20, 2019), https://www.brookings.edu/blog/techtank/2019/06/20/what-are-the-proper-limits-on-police-use-of-facial-recognition/.

8. Dave Gershgorn, *Carnival Cruises, Delta, and 70 Countries Use a Facial Recognition Company You've Never Heard Of*, ONEZERO (Feb. 18, 2020), https://onezero.medium.com/nec-is-the-most-important-facial-recognition-company-youve-never-heard-of-12381d530510.

9. *Id.*

Evaluation Service ("FACE").[10] NGI has a component that can conduct facial analysis on photos from criminal mugshots, whereas FACE is capable of conducting facial analysis on photos collected from noncriminal sources like employment records and background check databases.[11]

In China, facial recognition is used to enhance public security, promote the development of artificial intelligence, and more recently, prevent the spread of COVID-19.[12] Some of the leading facial recognition and surveillance companies include Hikivison, Dagua, iFlyTek, SenseTime, and Jiadu Technology.[13] Presently, China has installed over 626 million facial recognition cameras around the country.[14]

Below, I will further discuss facial recognition technology by looking into how the United States and China utilize facial recognition technology. Then, I will describe the legal and privacy concerns and harms inherent in using facial recognition technology for surveillance purposes. Finally, I will recommend a policy that can be used by law enforcement agencies when using facial recognition technology for surveillance and investigatory purposes.

III. FACIAL RECOGNITION TECHNOLOGY USES: UNITED STATES V. CHINA

A. How is Facial Recognition Technology Used in the United States?

Federal, State, and local law enforcement use facial recognition technology in a variety of ways. The most common uses, which are described in greater detail below, include: general surveillance, targeted photo comparisons, active criminal investigations, and trial evidence. In addition, there are also a variety of ways that law enforcement could use facial recognition technology in the future.

On the most basic level, law enforcement utilizes facial recognition technology for general surveillance purposes. This can be accomplished by

---

10. Hamann, *supra* note 5. *See generally* Malkia Devich-Cyril, *Defund Facial Recognition*, THE ATLANTIC: TECHNOLOGY (July 5, 2020), https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/ (explaining that the Department of Homeland Security allocated $1.8 billion for preparedness-grants programs that would be given to state, local, tribal, and territorial governments).

11. Hamann, *supra* note 5.

12. Lauren Dudley, *China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash*, THE DIPLOMAT (Mar. 7, 2020), https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash/.

13. *Id.*

14. Billie Thomson, *China Will Have 'One Street Camera for Every Two People by Next Year' as the Country Tightens its Grip on State Surveillance*, DAILYMAIL (Aug. 21, 2019), https://www.dailymail.co.uk/news/article-7379255/China-one-CCTV-camera-TWO-PEOPLE-year.html.

utilizing the mugshot databases to identify unknown people in photos that are taken from social media, CCTV, cameras, or photographs that are taken by law enforcement while in the field.[15] For example, in 2001, facial recognition technology was utilized to screen Super Bowl attendees to ensure that there were no potential criminals or terrorists attending the event.[16] This process is comparable to field identification where an officer takes, processes, and submits a photo for a near-instantaneous response from the facial recognition database.[17] Images of unknown people can also be compared in real-time against "hot lists" of people suspected of illegal activity.[18] For example, the Baltimore police department utilizes facial recognition technology to monitor protesters.[19] Specifically, the Baltimore police department monitored protests to identify protestors with outstanding warrants.[20]

In addition to monitoring events and protests, law enforcement utilizes facial recognition technology for targeted photo comparisons which can be used to identify thousands of suspects that may be related to identification fraud.[21] This is particularly successful when used to identify driver's license fraud.[22] In New York, the NYPD has identified over ten thousand people who have committed driver's license fraud by having more than one driver's license.[23] Similarly, in New Jersey, the Department of Motor Vehicles ("DMV") has referred over twenty-five hundred fraud cases to law enforcement that were identified by utilizing facial recognition technology.[24] On a federal level, law enforcement has begun to utilize facial recognition technology in

15. *Face Recognition*, EFF (Apr. 7, 2020), https://www.eff.org/pages/face-recognition.

16. Hamann, *supra* note 5.

17. Clare Garvie, et al., *The Perpetual Line-Up*: *Unregulated Police Face Recognition in America*, GEORGETOWN LAW CENTER ON PRIVACY & TECHNOLOGY (Oct. 18, 2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf.

18. *Id.*

19. *Id.* (citing Benjamin Powers, *Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You*, ROLLING STONE MAG. (Jan. 6, 2017), https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885/); *see also* Kevin Rector & Alison Knezevich, *Maryland's Use of Facial Recognition Software Questioned by Researchers*, *Civil Liberties Advocates*, BALT. SUN (Oct. 18, 2016), https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html.

20. *Id.*

21. Hamann, *supra* note 5.

22. *Id.*

23. *Id.*

24. *Id.*

airports to make the security and boarding process more efficient.[25] This is accomplished by allowing passengers to board planes based on photographic images, in lieu of boarding passes, that are compared to previously used passport and visa photographs that are on file with the United States Customs and Border Patrol.[26]

Law enforcement also utilizes facial recognition technology for active criminal case investigations.[27] Based on a recent estimate in a report by the Center on Privacy & Technology, more than one in four of all state and local law enforcement agencies can "run face recognition searches of their own database, run those searches on another agency's face recognition system, or have the option to access such a system."[28] In Irving, Texas, the Irving Police Department uses NEC's facial recognition system on average six to ten times per week, and twenty-one percent of those searches result in a strong lead.[29] In conjunction with other evidence, facial recognition software is used in investigations to identify individuals and establish probable cause for arrest in suspected criminal activity such as assailants in fights, passport fraud, identity theft, shootings, and terrorist attacks.[30]

Since facial recognition technology can be used to establish probable cause, law enforcement also utilizes this technology for trial evidence in court.[31] This trial evidence is offered either to establish probable cause or as evidence of an identification.[32] However, it is difficult to prove the validity and reliability of facial recognition technology.[33] Thus, some researchers argue that once the

---

25. *See* Adam Vaccaro, *At Logan, Your Face Could Be Your Next Boarding Pass*, BOS. GLOBE (May 31, 2017), https://www.bostonglobe.com/business/2017/05/31/jetblue-will-test-facial-recognition-system-for-boarding-logan-airport/8zspAiYyd7Bq9c7SINozwO/story.html.

26. *Id.*

27. *See* Bala, *supra* note 7 ("Facial recognition technology has real potential to help law enforcement catch criminals and improve public safety. For instance, the technology has already helped to identify Jarrod Ramos, a suspect who currently faces five charges for first-degree murder, when he refused to identify himself after police apprehended him. Most citizens would likely be comfortable with this is a use of facial recognition technology. And outside of traditional law enforcement contexts, facial recognition can also be used to authorize government employees at high-security facilities, combat child sex trafficking, and find missing persons.").

28. *See* Garvie, *supra* note 17, at 25.

29. *See* Gershgorn, *supra* note 8.

30. *See* Hamann, *supra* note 5 (showing officers also utilize this technology to narrow down photographs to show to witnesses).

31. *Id.*

32. *Id.*

33. Kelsey Y. Santamaria, *Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations*, Congressional Research Service (Sept. 24, 2020) https://crsreports.congress.gov/product/pdf/R/R46
541 (explaining that facial recognition technology would be scrutinized for reasons such as "whether the system's accuracy was meaningfully affected by factors that could result in misidentification").

scientific reliability of facial recognition technology can be established, prosecutors will have to utilize the *Frye* or *Daubert* standard in court so that the evidence can be properly admitted.[34]

Finally, in the future, law enforcement is expected to use facial recognition technology for real-time analysis of faces and for immediate identification.[35] Moreover, state and local governments are investing a substantial amount of money in technology that can allow for biometric and pattern recognition in hopes of decreasing or preventing domestic terrorism and other crimes.[36]

B. How is Facial Recognition Technology used in China?

China's facial recognition database includes nearly every one of China's 1.4 billion citizens.[37] The database is used to "achieve both ethnic unity and social stability."[38] For example, facial recognition is used to track big spenders in luxury retail stores, catch identity thieves, prevent violent crime, find fugitives, and ticket jaywalkers. One company, YITU, has developed a facial scanning platform that can identify a person from a database of at least two billion people in a matter of seconds.[39] Police use YITU particularly to analyze surveillance videos and identify people and cars.[40] While China does utilize facial recognition for consumer protection and surveillance purposes, China has

---

34. *See id*. (citing Frye v. United States, 293 F. 1013 (D.C. Cir. 1923) (holding the *Frye* test allows scientific evidence to be admitted if the science upon which it rested was generally accepted by the scientific community) and Daubert v. Merrell Dow Pharms., 509 U.S. 579, 580 (1993) (holding courts have a gatekeeping obligation to assess reliability of scientific evidence)). But *see Op-Ed, We Now Have Evidence of Facial Recognition's Harm. Time for Lawmakers to Act., WASH. POST (July 5, 2020), https://www.washingtonpost.com/opinions/we-now-have-evidence-of-facial-recognitions-harm-time- for-lawmakers-to-act/2020/07/05/e62ee8d0-baf8-11ea-80b9-40ece9a701dc_story.html* (explaining the racial consequences of facial recognition technology)*; Jennifer Lynch, Face Off: Law Enforcement Use of Face Recognition Technology, ELEC. FRONTIER FOUND. (Feb. 12, 2018), https://www.eff.org/wp/ law-enforcement-use-face-recognition.*

35. *See id*. (citing Ava Kofman, *Real-Time Face Recognition Threatens to Turn Cops' Body Cameras into Surveillance Machines*, THE INTERCEPT (Mar. 22, 2017), https://theintercept.com/2017/03/22/real-time-face-recognition-threatens-to-turn-cops-body-cameras-into-surveillance-machines/ (explaining "it soon may be possible for an officer's body-worn camera to use FRT to identify a person he or she observes on the street.")).

36. *Id.*

37. Amanda Lentino, *This Chinese Facial Recognition Start-Up Can ID a Person in Seconds*, CNBC (May 17, 2019), https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html.

38. Megha Rajagopalan, *This is What a 21st-Century Police State Really Looks Like*, BUZZFEED (Oct. 17, 2017), https://www.buzzfeednews.com/article/meghara/the-police-state-of-the-future-is-already-here.

39. Lentino, *supra* note 37.

40. *Id.* ("[T]he company's technology was being used in more than 20 provincial public security bureaus in over 300 cities.").

become known for using facial recognition technology for pervasive surveillance, tracking citizens, and manipulation.

Chinese authorities employ mass surveillance systems to monitor citizens by way of QR codes, biometrics, artificial intelligence, phone spyware, and big data.[41] More recently, China has employed drones equipped with facial recognition technology that mimic the "appearance and movements of real doves" so that the drones are undetectable by humans or radar.[42] China has also begun to equip law enforcement with sunglasses capable of real time facial recognition capabilities.[43] Both the drones and the sunglasses have helped law enforcement to capture suspected criminals as well as individuals travelling under false identities.[44]

Additionally, China utilizes pervasive surveillance techniques to ensure that anyone who disagrees with Chinese authorities is silenced, whether by silencing the individual or by harassing and detaining that individual's family.[45] This can be accomplished quickly because facial recognition technology is used to identify citizens in surveillance footage or a photograph.[46] Once the citizen is identified, the facial recognition technology collects data on that citizen's whereabouts and behavior.[47] The facial recognition algorithm can assess in real time the number and density of people in the frame, the individual's gender, and the corresponding characteristics of clothing and vehicles.[48] China's goal in using facial recognition technology is to provide "100 percent" coverage in specified types of areas by monitoring gender, clothing, and height of every citizen and transforming that information into data to be used at a later date.[49]

Once the data is collected, China uses it to track citizens.[50] Recently, China mandated that all telecom companies deploy "artificial intelligence and other technical methods" to check the identities of people purchasing cell phones and

41. *China: Events of 2018*, HUMAN RIGHTS WATCH (2018), https://www.hrw.org/world-report/2019/country-chapters/china-and-tibet.

42. Kayla Marie Cannon, America's Panopticon: Privacy Implications of Facial Recognition by Law Enforcement, 19 (May 13, 2019) (unpublished Master's thesis, Tallinn University of Technology) (on file with author).

43. *Id.*

44. *Id.*

45. *See China: Events of 2018*, *supra* note 41.

46. *See* Cannon, *supra* note 42, at 30.

47. *Id.*

48. Xiao Qiang, *The Road to Digital Unfreedom: President Xi's Surveillance*, 30 J. OF DEMOCRACY 1, 57 (2019).

49. *Id.*

50. *Id.*; *see also* Alfred Ng, *How China Uses Facial Recognition to Control Human Behavior*, CNET (Aug. 11, 2020) https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/ (explaining how China uses facial recognition technology to shame and control its citizens).

registering SIM cards.[51] This is accomplished by requiring that every citizen who purchases a cell phone have his or her face scanned by a facial recognition technology.[52] The Chinese Ministry of Industry and Information reasoned that the collection of every citizen's biometric information by facial recognition technology will "protect the legitimate rights and interests of citizens in cyberspace" by making Chinese mobile phone and internet users easier to track.[53]

By leveraging this data collected by facial recognition technologies, China can manipulate and control citizens.[54] Perhaps the best example of this is China's use of biometrics for automated surveillance purposes where citizens are rewarded or punished under its social credit system ("SCS").[55] Under the SCS, China monitors an individual's activities and assigns that individual a computational score.[56] This score is used to determine whether that individual should be granted a reward or given a punishment, such as the revocation of travel rights.[57] Once a citizen has done something that warrants a punishment, Chinese authorities also use SCS for humiliation purposes.[58] For example, in Jinan, a jaywalker was humiliated by having his photo, home address, and personal identification number projected on a public screen.[59] To achieve a "more trustworthy country," China creates a List of Dishonest Persons Subject to Enforcement of citizens that are deemed untrustworthy.[60]

Similarly, Chinese authorities also utilize facial recognition technology to manipulate citizens who do not share the same beliefs or ideologies as those approved by the Chinese Communist Party. In addition to tracking Chinese citizens through the SCS, Chinese authorities also monitor the Xinjian region for signs of unrest and dissent.[61] Chinese authorities claim that this is necessary to "neutralize the threat of violence posed by Uyghur militants."[62] Facial recognition cameras seek out Uyghur citizens, based on appearance, to track

51. Lily Kuo, *China Brings in Mandatory Facial Recognition for Mobile Phone Users*, THE GUARDIAN (Dec. 2, 2019), https://www.theguardian.com/world/2019/dec/02/china-brings-in-mandatory-facial-recognition-for-mobile-phone-users.

52. *Id.*

53. *Id.*

54. *See* Qiang, *supra* note 48, at 53.

55. *See China: Events of 2018*, *supra* note 41.

56. *See* Cannon, *supra* note 42, at 45.

57. *Id.*

58. *Id.* at 45-6.

59. *Id.*

60. *Id.*

61. *See China: Events of 2018*, *supra* note 41.

62. *See* Cannon, *supra* note 42, at 45.

and control their movements.[63] While tracking the Uyghur citizen's movements, the authorities also use facial recognition technologies to punish the Uyghurs for offenses such as using Western social media applications and to place the Uyghurs in reeducation camps.[64]

IV. LEGAL CONCERNS: UNITED STATES V. CHINA

A. What are the Legal and Privacy Implications in the United States?

Facial recognition technology in the United States creates federal, state, and local level regulatory issues. It also implicates an individual's First Amendment, Fourth Amendment, Fifth Amendment, and Fourteenth Amendment due process and equal protection rights.

There is currently no federal regulation on facial recognition technology.[65] However, there are some state biometric laws.[66] These laws strictly limit the private sector use of facial recognition technology and have created carveouts or loopholes for law enforcement.[67] For example, the Illinois Biometric Information Privacy Act ("BIPA") creates a carve-out for state agency or local government use when a contractor, subcontractor, or agent is working for a State agency or local unit of government.[68] In addition to state regulations, some cities, such as San Francisco, Oakland, and Somerville, have taken matters into their own hands by banning facial recognition altogether.[69] Similarly, some cities, such as Detroit, have limited the use of facial recognition by only allowing for its use in connection with investigations of violent crimes and home invasions.[70]

Aside from regulatory implications, the use of facial recognition technology can create First Amendment issues by violating individuals' right to freedom of association and right to privacy.[71] The use of facial recognition

---

63. *Id.*

64. *Id.*

65. Orion Rummler, *2020's First Wave of Facial Surveillance Bills*, AXIOS (Feb. 19, 2020), https://www.axios.com/facial-surveillance-legislation-2020-47063834-a7fb-47bf-b53c-e770b0e16d1a.html.

66. *See* Biometric Information Privacy Act, 740 ILCS 14 (2008); *see also* Tex. Bus. & Com. Code Ann. § 503.001.

67. *Id.*

68. *See* 740 ILCS 14 (limiting a private entity's use of biometric information or biometric identifiers by ensuring that private entity is transparent with and gains consent from the subject whose biometric information is in use by the private entity).

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

70. *Id.*

71. *See* Garvie, *supra* note 17, at 16.

technology could have a chilling effect on individuals' behaviors, such as one's ability to associate freely and advocate for minority positions, which could lead to self-censorship.[72] Courts have upheld the right to anonymous speech and association;[73] however, courts appear to be split on whether law enforcement's use of photography at public demonstrations violates the First Amendment right to freedom of association.[74]

Similarly, there are Fourth Amendment issues where facial recognition technology is used for suspicion-less general investigatory or real-time surveillance.[75] Particularly, Fourth Amendment issues arise when law enforcement uses facial recognition to scan the faces of unknown individuals in connection with identifying information such as place of employment, age, immigration status, criminal and arrest records, outstanding warrants and tickets, or perceived gang involvement.[76] Under the *Katz* framework, the use of facial recognition technology likely requires a warrant where "the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy," and "the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable."[77] The Sixth Circuit, when analyzing the constitutionality of license plate readers in *United States v. Ellison*, reasoned that the information that is private rests on the aggregation of general information that a certain car was observed at a certain time, date, and place, with specific identifying information held in a government database.[78]

With *Katz* and *Ellison* in mind, it could be determined that like a license plate, a person also has a reasonable expectation of privacy in his or her face when the government is aggregating general information of where that person was at a certain time, date, and place, which was based on specific identifying information held in a government database.[79] The recent Supreme Court case *Carpenter v. United States* found that the government's warrantless access to an extensive compilation of cell site location data violated the Fourth

72. *Id.* at 43.

73. *See* NAACP v. Alabama, 357 U.S. 449, 466 (1958); *see also* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).

74. Compare Laird v. Tatum, 408 U.S. 1 (1972); Phila. Yearly Meeting of Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1337–38 (3d Cir. 1974); Donohoe v. Duling, 465 F.2d 196, 202 (4th Cir. 1972) *with* Hassan v. City of New York, 804 F.3d 277, 292 (2d Cir. 2015) (finding targeted use of pervasive video, photographic, and undercover surveillance of Muslim Americans may have caused those individuals "direct, ongoing, and immediate harm," and it may have created a chilling effect).

75. Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591 (2017).

76. *Id.* at 1595.

77. United States v. Katz. 389 U.S. 347 (1967).

78. United States v. Ellison, 462 F.3d 557 (6th Cir. 2006).

79. *See Katz*, 389 U.S. at 361–3; *see also Ellison*, 462 F.3d at 563–4.

Amendment, lending support to the idea that a person has a reasonable expectation of privacy in information about his or her face that is stored in a database for facial recognition purposes.[80]

Additionally, facial recognition technology also likely raises a due process issue when presented as evidence because the results have never been deemed reliable when submitted as trial evidence.[81] While facial recognition technology is allowed to play a role in investigations, there are issues inherent in allowing a technology to be used during investigations that cannot hold up to judicial scrutiny; particularly where law enforcement does not give the defense all of the information necessary to properly defend against the state accusations, such as how the algorithm functions or information about the other potential matches.[82] Jurisdictions have varying ideas on whether the use of facial recognition technology should be shared with the defense.[83] Moreover, recent investigations of law enforcement's use of facial recognition have uncovered that not all results are logged, and some questionable or negative results are not recorded.[84] By failing to share all of the evidence with the defense and by failing to accurately log all of the results, state and local law enforcement are doing the defendant and the judicial system a disservice by not allowing the defense to properly defend its case.

Finally, there are also equal protection issues since facial recognition technology has a greater potential for racial discrimination.[85] The Department of Commerce's National Institute for Standards and Technology ("NIST") identified that some facial recognition systems are anywhere from ten to one hundred times more likely to misidentify groups like the young, the elderly,

80. Carpenter v. United States, 138 S. Ct. 2206, 2212–21 (2018); *see also* United States v. Jones, 565 U.S. 400 (2012) (Sotomayor, J., concurring).

81. *See* U.S. Const. amend V; *see also* U.S. Const. amend XIV, § 1; Jennifer Valentino-DeVries, *How the Police Use Facial Recognition, and Where it Falls Short*, N.Y. TIMES (Apr. 7, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

82. *See generally* Brief for ACLU, EFF, et al. as Amici Curiae Supporting Petitioner, Lynch v. Florida, No. 1D16-3290 (Mar. 11, 2019), https://efactssc-public.flcourts.org/casedocuments/2019/298/2019-298_notice_86166_notice2dappendix2fattachment20to20notice.pdf.

83. *Id.* ("In some of the Florida cases The Times reviewed, the technology was not mentioned in initial warrants or affidavits. Instead, detectives noted "investigative means" or an "attempt to identify" in court documents, while logging the matters as facial recognition wins in the Pinellas County records. Defense lawyers said in interviews that the use of facial recognition was sometimes mentioned later in the discovery process, but not always.").

84. *Id.*

85. U.S. Const. amend XIV, § 1 ("nor deny to any person within its jurisdiction the equal protection of the laws.").

women of color, and people of Asian or African descent.[86] Additionally, some lawmakers believe that this software can exacerbate existing prejudices and over-policing of schools, communities of color, and communities that are designated to have more criminal activity.[87]

The purpose of the equal protection clause of the Fourteenth Amendment is to secure "every person within the State's jurisdiction against intentional and arbitrary discrimination, whether occasioned by express terms of a statute or by its improper execution through duly constituted agents."[88] However, facial recognition technology is known to show significant bias against marginalized groups.[89] Specifically, facial recognition technology has been shown to be less accurate when applied to women, transgender people, and people with darker skin tones.[90] A recent federal study found "Asian and African American people were up to 100 times as likely to be misidentified than white men."[91]

Moreover, there is also bias when it comes to the specific subject matter because of the overinclusion bias towards black and Latinx individuals.[92] For example, black and Latinx individuals are more likely to be arrested which makes black and Latinx individuals more likely to be included in a criminal database that is susceptible to a facial recognition search.[93] There are significant issues of bias and discrimination based on the disproportionate rate of racial minorities involved in the criminal justice system, which could lead to an increase in wrongful convictions and racial disparities in the criminal justice system.[94] These examples of facial recognition technology's inaccuracy and possible bias and prejudice would violate the equal protection clause because of the discrimination inherent in utilizing a technology that has a biased algorithm.

---

86. Khari Johnson, *From Washington State to Washington, D.C., Lawmakers Rush to Regulate Facial Recognition*, VENTUREBEAT (Feb. 19, 2020), https://venturebeat.com/2020/01/19/from-washington-state-to-washington-dc-lawmakers-rush-to-regulate-facial-recognition/.

87. *Id.*

88. Vill. of Willowbrook v. Olech, 528 U.S. 1073 (2000) (per curium) (quoting Sioux City Bridge Co. v. Dakota Count*y*, 260 U.S. 441, 445 (1923)).

89. *See* Johnson, *supra* note 86.

90. Mason Kortz, *Facial Recognition Regulation – A Year in Review*, ACS LAW (Dec. 17, 2019), https://www.acslaw.org/expertforum/facial-recognition-regulation-a-year-in-review/.

91. *Law Enforcement's Rising Problem*, AXIOS (Dec. 19, 2019), https://www.axios.com/law-enforcements-rising-problem-b5e5628e-be13-4ab8-9c1f-ccaf37b5426e.html.

92. *See* Kortz, *supra* note 90.

93. *Id.*

94. *See* Bala, *supra* note 7.

B. What are the Legal and Privacy Implications in China?

In 2019, China enacted the Personal Information Security Specifications regulation which states that the collection of personal information should be for "legal, justified, necessary, and specific purposes."[95] This regulation requires individual consent and that personal information be kept secure. However, this regulation outlines eleven exceptions to consent.[96] The exceptions include collection of data that is directly related to: (1) national security and national defense; (2) public safety, public health, and significant public interests; (3) criminal investigation, prosecution, trial, and judgment enforcement, etc.; and (4) when safeguarding the major lawful rights and interests such as life and property of PI subjects or other persons, and it is difficult to obtain the consent of the PI subject.[97]

China's National Information Security Standardization Technical Committee also issued a national standard on personal information security.[98] In addition, China enacted a Cybersecurity Law in 2017 which has led to the implementation of regulations and guidelines.[99] Some of the regulations include the National Standard of Information Security Technology – Personal Information Security Specifications, Guidelines on Internet Personal Information Security Technology, and Guidelines on Personal Information Security Impact.[100] There are also general data protection rules stemming from the Decision on Strengthening Online Information Protection and the Guideline for Personal Information protection within Information Systems for Public and Commercial Services.[101]

But while there are plenty of laws, regulations, and guidelines in place, there are a slew of examples which show that China is far from practicing what

---

95. *See* Mingli Shi, et al., *Translation: China's Personal Information Security Specification*, NEW AMERICA: DIGICHINA (Feb. 8, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/; *see also* Dudley, *supra* note 12.

96. Mingli, *supra* note 95.

97. *Id.*

98. Carolyn Bigg & Venus Cheung, *Data Protection Laws of the World: China*, DLA PIPER (Apr. 22, 2020) (outlining that data must be protected by "clarifying the rights of personal data subjects and requiring a higher level of protection for "personal sensitive information" than for ordinary "personal information," requiring data controllers to obtain "explicit consent", that is, written consent or other affirmative action by a personal data subject, such as electronically clicking to consent, before collecting and using personal sensitive information, and requiring network operators to notify regulators and affected individuals of security incidents involving an actual or potential leak, damage or loss of personal information.").

99. *Id.*

100. *Id.*

101. *Id.*

it preaches. First, China employs poor data protection practices.[102] Although China ensures that data centers are within its borders and that companies undergo a security assessment before transferring collected information, Chinese authorities censor content and fail to anonymize data by requiring real-name registration.[103] In addition, national security and social stability will trump all other priorities in China, so China's access to data from facial recognition systems could be far-reaching by using broadly-defined national security purposes that are not restricted.[104]

Moreover, there is a lack of consent and transparency. The National Information Security Standardization Technical Committee, TC 260, released a proposal which stated that consent is not always practical when data is being collected in public places.[105] Since consent is not always practical, the committee recommended that owners of facial recognition technology just identify the nature and purpose of the information collection.[106] However, most Chinese citizens do not know that their data is being collected, how it is being used, or how it is stored.[107] Chinese citizens are also unaware of how the algorithms work. Specifically, the Chinese authorities have created a facial recognition database by populating information and images from criminal records, mental illness records, drug use records, and from individuals who have petitioned the government over grievances.[108]

These databases can be used for nontransparent and discriminatory treatment because protections do not apply to populations deemed a threat to social stability.[109] One Chinese start-up, CloudWalk, has created facial recognition technology that can recognize "sensitive groups."[110] For example, Chinese authorities continuously surveil and persecute ethnic Muslim minorities in Xinjian Uygur.[111] Surveillance is conducted on a level that allows

---

102. *See* Qiang, *supra* note 48, at 55.

103. *Id.*

104. Sheena Chestnut Greitens, *Dealing with Demand for China's Global Surveillance Exports*, BROOKINGS (April 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200428_china_surveillance_greitens_v3.pdf; Johnson, *supra* note 86.

105. Dudley, *supra* note 12.

106. *Id*.

107. *See China: Events of 2018*, *supra* note 41.

108. Paul Mozur, *One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority*, TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html ("A national database of criminals at large includes about 300,000 faces, while a list of people with a history of drug use in the city of Wenzhou totals 8,000 faces . . . .").

109. *Id.*

110. Dudley, *supra* note 12.

111. *See* Sarah Zheng, *China Keeps Turning Screw on Civil Liberties and Free Speech, says US-Backed Campaign Group Freedom House*, SCMP (Mar. 4, 2020),

authorities to receive alerts immediately when a potential Uygur appears on the screen.[112] In the Chinese city of Sanmenxia, the facial recognition system screened whether residents were Uygurs 500,000 times over the course of one month.[113] Through this surveillance technique, over thirteen million Uygurs have been persecuted by means of "mass arbitrary detention, torture, mistreatment in detention facilities, and pervasive controls of daily life."[114]

The Uygurs are not the only group that Chinese authorities are using facial recognition to discriminate against and control. Chinese authorities have also utilized facial recognition to surveil and persecute the Christian communities in the Henan Province and the Hui Muslims in Ningxiz.[115] Similarly, Chinese authorities have used facial recognition technology to harass citizens during peaceful pro-independence speeches and to ban entire political parties from the government.[116] Women and children are also discriminated against, and facial recognition technology could be employed to ensure that women do not receive rights, cannot participate in activist movements, and do not violate the "two-child policy."[117] Facial recognition could also be used to ensure that citizens do not date or marry who they want since same sex marriage is not legal in China.[118]

All of China's discriminatory practices appear to violate Chinese citizen's fundamental right against discrimination.[119] In addition, other fundamental rights are largely violated by Chinese authorities' misuse of facial recognition technology. Chinese citizens have the right to enjoy "freedom of speech, of the press, of assembly, of association, of procession and of demonstration."[120] However, Chinese authorities have continued to surveil, prosecute, and limit the freedom of speech of website editors, labor rights activists, and human rights lawyers.[121] Chinese authorities have also harassed and detained

---

https://www.scmp.com/news/china/diplomacy/article /3064950/china-keeps-turning-screw-civil-liberties-and-free-speech-says (noting that "at least a million people were estimated to have been held in what the government called re-education camps.").

112. *See* Dudley, *supra* note 12.

113. *See* Mozur, *supra* note 108.

114. *See China: Events of 2018*, *supra* note 41.

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.* (showing a Chinese social media platform deleted posts related to gay culture in an effort to "clean up" the platform).

119. Constitution of the People's Republic of China, Article 33.

120. Constitution of the People's Republic of China, Article 35.

121. *See China: Events of 2018*, *supra* note 41 (showing the Chinese government maintains tight control over internet, mass media, and academia).

journalists who cover human rights issues as well as their interviewees.[122] Similarly, Chinese authorities utilize active surveillance to arrest citizens who fight against current political or social issues.[123] For example, in 2018, students were arrested and detained for "gathering to show support to factory workers."[124] These authorities do not just stop when punishing the specific individuals who speak out either. China has harassed and detained activists' family members on many occasions.[125]

Chinese citizens are guaranteed "the freedom of the persons of citizens" such that arbitrary arrests cannot be made.[126] However, Chinese authorities held one woman under an eight-year house arrest as a punishment for dissent and expression.[127] The Chinese authorities also restricted her family from leaving China.[128] China also continuously arrests, tortures, and charges human rights activists for fighting for basic human rights and arrests people for "illegal border crossing."[129]

Finally, Chinese citizens have the protection of their personal dignity as insults, libel, false charging or "frame up's" directed against citizens is prohibited.[130] But the Chinese government restricts religious practice only to those religions that are officially recognized.[131] The government classifies many religious groups outside its control as "evil cults," and subjects members to police harassment, torture, arbitrary detention, and imprisonment.[132] This over-policing and harassment of religious groups lends to the idea that Chinese citizens do not in fact have any protection of their personal dignity or against false charging.

V. POLICY RECOMMENDATION

Based on the legal and privacy implications associated with the use of facial recognition technology, as seen by law enforcement's use of the technology in both the United States and China, there are a few rights that must be granted to individuals in a law enforcement's use policy.

---

122. *Id.*

123. *Id.*

124. *Id*.

125. *Id*.

126. Constitution of the People's Republic of China, Article 37.

127. *China: Events of 2018*, *supra* note 41.

128. *Id*.

129. *Id*. (explaining that Chinses authorities prosecute and disbar human rights lawyers for "subvert[ing] state power" and "obstructing public duties").

130. Constitution of the People's Republic of China, Article 38.

131. *China: Events of 2018*, *supra* note 41.

132. *Id.*

First, there must be transparency. The law enforcement agency must require routine monitoring, periodic audits, enforcement, and public transparency to ensure that facial recognition technology is not being misused. Transparency is attained when law enforcement agencies give the public access to how facial recognition technology is used. Specifically, the agency should give the public information on how facial recognition technology works, what it is, how the agency complies with the rules, what incidents have occurred, etc. Second, there must be notice transparency and consent. Notice refers to telling individuals that a particular collection is taking place and what is being done with that information. A recent study showed that few facial recognition systems are audited for misuse, and only ten percent of fifty-two agencies that acknowledged utilizing facial recognition technology had a publicly available use policy.[133] Law enforcement agencies should be required to publish a publicly available use policy as well as provide individuals with information on whether criminal and non-criminal images are being used for facial recognition surveillance. Similarly, law enforcement agencies should be required to seek informed consent for the use of individual's photos just as the Illinois biometric law requires consent before a business may obtain or use an individual's biometric data.[134]

Third, data access must be assessed, and a determination must be made on who is granted access. A multitude of private companies have either sold or leased facial recognition technology to law enforcement agencies, raising a large question: Who has access to this data related to individuals' faces once facial recognition software is used by law enforcement? A recent study conducted by the ACLU shed light on concerns of placing mug shots into Amazon's cloud storage when law enforcement utilizes Amazon's Rekognition technology.[135] Specifically, one of the concerns is that Amazon now has access to technology that can "identify persons of interest against a collection of millions of faces in real-time."[136] Because of the risks inherent with facial recognition technology, it is important that access only be granted under controlled circumstances. Presumably, that would mean that organizations requesting access must have appropriate restrictions and training and commit

133. *See Face Recognition*, *supra* note 15.

134. Benjamin Hodges & Kelly Mennemeier, *The Varying Laws Governing Facial Recognition Technology*, IPWATCHDOG (Jan. 28, 2020), https://www.ipwatchdog.com/2020/01/28/varying-laws-governing-facial-recognition-technology/id=118240/.

135. Tom Simonte, *Few Rules Govern Police Use of Facial-Recognition Technology,* WIRED (May 22, 2018), https://www.wired.com/story/few-rules-govern-police-use-of-facial-recognition-technology/ (citing Amazon employees concerns that "the government [is] getting in bed with big data").

136. *Id.*

to using it only for authorized purposes. The ACLU argued that this technology will be misused because the private companies and the government now have access to a "powerful surveillance system readily available to violate rights and target communities of color."[137] Similarly, over six hundred law enforcement agencies utilize Clearview AI's facial recognition system, which stores photos that have been scraped from sites that the site owners have claimed violates the sites terms of service.[138] News reports have alleged that Clearview AI allows law enforcement to scan these photos after a search is conducted.[139]

Since a multitude of private companies have either sold or leased facial recognition technology to law enforcement agencies, the law enforcement agency must conduct a privacy impact assessment on the company. The law enforcement agency must also ensure that the company has a privacy policy and terms of service posted on the company's website. Finally, the law enforcement agency must ensure that the company does not utilize any of the data that is collected, maintained, monitored, or used by the law enforcement agency while the law enforcement agency is utilizing the company's service.

Fourth, law enforcement agencies must strive for the highest accuracy rate possible. Facial recognition technology can be accurate when the images meet certain professional scientific standards. Specifically, professional scientific standards such as NIST's photography standards and the ISO/IEC Joint Technical Committee's biometric performance testing and reporting standards.[140] Even with a professional scientific standard, accuracy greatly decreases when there is no standardized photo for comparison, when the comparison photo comes from an uncontrolled environment, when the photo is a partial image, or when there is an issue with the photo angle.[141] Thus, law enforcement agencies must be required to conduct due diligence by testing and auditing the facial recognition systems. Failure to properly conduct due diligence could lead to the misidentification of innocent individuals, an increase in discriminatory investigative practices, and improper oversight of law enforcement agency's surveillance practices.

---

137. *Id*.

138. Connor Perrett, *A Startup Company Took Billions of Photos from Facebook and Other Websites to Create a Facial-Recognition Database, and Hundreds of Law-Enforcement Agencies are Using It*, BUSINESS INSIDER (Feb. 19, 2020), https://www.businessinsider.com/law-enforcement-using-unknown-facial-recognition-technology-facebook-photos-2020-1.

139. *Id.*

140. *Facial Recognition Technology*, NIST (Feb. 6, 2020), https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0.

141. *See* Hamman, *supra* note 5; *see also* Valentino-DeVries, *supra* note 81 (quoting a technical support specialist of the Pinellas County Sheriff's Office who aids in running the facial recognition program, "it comes down to image quality . . . if you put garbage into the system, you're going to get garbage back").

Finally, there must be a regulation relating to how law enforcement may use facial recognition technology. Each law enforcement agency should require reasonable suspicion that the individual to be identified has committed a crime, the individual's actions present a danger to human life or may cause serious physical harm, or that law enforcement must use facial recognition to identify someone who is not able to identify him or herself. Moreover, real-time use of facial recognition technology should be prohibited. Prohibiting real-time use allows for third-party review and ensures that law enforcement agencies have, at a minimum, reasonable suspicion before investigating or arresting an individual. These restrictions ensure that law enforcement may only utilize facial recognition technology in limited circumstances.

VI. CONCLUSION

Law enforcement's use of facial recognition technology will continue to be a hotly debated topic between those who are pushing hard for a complete moratorium of facial recognition technology and those who believe that facial recognition technology should be used but highly regulated. These debates will call into question what a privacy right even entails and how much surveillance an individual is willing to allow with the hopes of a safer lifestyle. The discussion on how the United States utilizes facial recognition technology shows what a world looks like when unregulated surveillance techniques clash with highly protected constitutional rights. The discussion on how China utilizes facial recognition technology shows what happens when a government is left to surveil individuals with no repercussions at all. Both the United States and China are presently using facial recognition technology in a manner that is unacceptable. Individuals' rights and freedoms must be guaranteed to avoid a draconian surveillance state where all privacy and civil liberties disappear into the lens of a camera.