Facial Recognition as a Policing Tool by Law Enforcement: Balancing Between Personal Privacy and Public Security Interest

*Shuyu Zhong**

I. Introduction

Facial recognition technology is not as science fiction as it used to be, but a practical technology that is impacting society and people's daily lives.[1] There are several benefits from using facial recognition technology: the technology can be a layer of security on cellphones, improve security at home, airports, borders and shopping malls, and it provides the fun of tagging people on Facebook.[2]

Facial recognition is defined as a process to identify and verify the identity of people by their faces.[3] The technology will capture faces by camera, and then analyze and compare patterns based on the captured person's facial features.[4] The whole process has three steps: (1) detection and location of human faces, (2) capture faces and transformation of facial features into digital information, and (3) match faces to identify a person.[5] The technology is widely used, especially by law enforcement agencies for security purposes, by healthcare industries to track a patient's use

[*] Shuyu Zhong is a 2021 candidate for Juris-Doctorate at SMU-Dedman School of Law.

[1] Jesse Davis West, *A Brief History of Face Recognition*, FACEFIRST (Aug. 1, 2017), https://www.facefirst.com/blog/brief-history-of-face-recognition-software/.

[2] *Id.*; Nikki Gladstone, *How Facial Recognition Technology Permeated Everyday Life*, CTR. FOR INT'L GOVERNANCE INNOVATION (Sept. 19, 2018), https://www.cigionline.org/articles/how-facial-recognition-technology-permeated-everyday-life.

[3] *Facial Recognition: Top Seven Trends*, THALES, https://www.gemalto.com/govt/biometrics/facial-recognition (last updated Sept. 12, 2020).

[4] *Id.*

[5] *Id.*

of medicine and detect any genetic diseases, and by commercial merchants and retailers to gather customer information regarding shopping preferences for marketing purposes.[6]

While enjoying the convenience of using facial recognition technology, people are concerned about the negative consequences brought by the technology.[7] There are four main concerns about the technology: (1) the right of privacy, (2) civil liberties and mass surveillance, (3) bias, discrimination and wrongful conviction due to inaccuracy of the technology, and (4) lack of public disclosure about current use and effectiveness of the technology. The most concerning issues are related to right of privacy and civil liberties.[8] There is a lot of debate about the use of facial recognition technology at the state level and internationally.[9] Proponents of unrestricted governmental use of facial recognition technology insist that the technology is necessary for the police to ensure the safety of the people, and opponents say that the use of facial recognition by the government is a violation of people's rights of privacy.[10] As for civil liberties, people are worried about governmental use of facial recognition technology for mass surveillance, which can

[6] *Id.*

[7] Shaun Moore, *What Are the Impacts of Facial Recognition Tech on Society?*, READWRITE (July 2, 2017), https://readwrite.com/2017/07/02/done-the-impact-of-facial-recognition-dl1/.

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

[9] Jessica Lusamba, *Bill to Restrict Police Use of Facial Recognition Introduced in U.S. Senate*, JURIST (Nov. 15, 2019, 1:03 PM), https://www.jurist.org/news/2019/11/bill-to-restrict-police-use-of-facial-recognition-introduced-in-us-senate/.

[10] *Id.*

threaten people's democratic freedoms.[11] Facial recognition technology has raised two fundamental right issues under the First Amendment and Fourth Amendment of the U.S. Constitution.[12] Another concern that people have is that the technology is not mature enough to generate accurate results in identifying a person.[13] Research has shown that facial recognition technology is inaccurate in identifying people, especially in identifying women and people with darker skin color.[14] A federal study revealed that Asian and African American people were up to a hundred times more likely to be misidentified than a white male, and the probability of misidentification varies based on different algorithms used and types of searches conducted.[15] In the kinds of searches that police investigators are using, where an image was searched against

[11] Jimmy Gomez & Lisa Rosenberg, *In the Hands of Police, Facial Recognition Software Risks Violating Civil Liberties*, USA TODAY (Oct. 18, 2019 2:10 PM), https://www.usatoday.com/story/opinion/policing/2019/10/18/hands-police-facial-recognition-tech-violates-civil-liberties/3904469002/; Brad Smith, *Facial Recognition: It's Time for Action*, MICROSOFT (Dec. 6, 2018), https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/.

[12] Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will it Take Us?*, AM. BAR ASS'N, https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ (last visited Feb. 8, 2021).

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

[14] *Id;* Smith, *supra* note 11.

[15] Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019, 5:43 PM), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

thousands or millions of others to identify a suspect, African American females are misidentified more often than others.[16]

This Comment will not discuss the use of facial recognition technology in healthcare and commercial areas, but will focus on law enforcement agencies' use of facial recognition technology as a policing tool to identify criminal suspects, and how to justify the use of the technology to protect both the public interest of national security and the personal right of privacy and freedom. Part II briefly discusses the social and legal background of the development of facial recognition technology. Part III addresses the legal issues behind the use of the technology: the right of privacy, the right of civil liberties, discrimination and potential wrongful convictions, and the lack of public disclosure. Part IV will provide the arguments in supporting the restricted use of the technology: (1) facial recognition technology has a unique function for law enforcement especially when DNA and fingerprint technology do not work, and the technology is time and cost saving compared to DNA and fingerprint technology;[17] (2) there are great concerns about the right of privacy under the Fourth Amendment and civil liberties under the First Amendment; however, banning the use of this technology by law enforcement is against the policy of the development of technology and society's reliance on technology as a security tool; (3) even people who worried about facial recognition technology have admitted that the technology has the potential to improve the efficiency of police investigating, and called for regulations to minimize the risk created by

[16] *Id.*

[17] Jon Schuppe, *How Facial Recognition Became a Routine Policing Tool in America*, NBC NEWS (May 11, 2019, 3:19 AM), https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251.

using facial recognition system;[18] and (4) the possible regulation of facial recognition technology includes, but is not limited to, limiting the general use of facial recognition technology to non-surveillance purposes only, having special procedures in using the technology for surveillance, formally disclosing the use of technology to the public, manually verifying the facial recognition matching result for accuracy, having procedures for training people with authorized access, testing each system before it is qualified as a policing tool, and maintaining the databases.

Part V concludes that technology advancements are not neglectable. The legislature should not completely ban the use of facial technology as a policing tool. Instead, there should be federal rules governing the use of facial recognition technology.

II. Background

A. Current use of facial recognition technology by law enforcements in the United States

Facial recognition technology is used in several areas, such as security, healthcare, and marketing.[19] According to FACEFIRST, a technology company in California, its facial recognition service can be used to find missing children, locate victims of human trafficking, assist retailers and transportation centers, and help law enforcement agencies to stop crimes before a crime happens.[20] Early in 2001, the city of Tampa, Florida used a facial recognition surveillance system

[18] *EU Leaders to Consider Ban on Face Surveillance*, ELEC. PRIV. INFO. CTR. (Jan. 16, 2020), https://epic.org/2020/01/eu-leaders-to-consider-ban-on-.html.

[19] *Facial Recognition: Top Seven Trends*, *supra* note 3.

[20] *FaceFirst Sentinel – IQ Face Recognition*, GENETEC, https://www.genetec.com/partners/technology-partner-solutions/solutions-detail?appId=3300 (last visited Mar. 8, 2021).

when hosting the Super Bowl XXXV.[21] Tampa was the first city in the United States to test a facial recognition system, which was installed to identify felons and terrorists from the Super Bowl crowd.[22] The surveillance focused on Super Bowl-related events that took place in and around the stadium.[23] It was revealed that nineteen individuals with outstanding warrants were identified by the facial recognition system, but none were arrested after such identification.[24]

Nowadays, there are several well-known companies providing or using facial recognition technology, such as Facebook, Google, Microsoft, IBM, Megvii, and Amazon.[25] Amazon's promotional videos for Rekognition, its facial recognition product, encouraged police agencies to acquire Rekognition and use it with body cameras and smart cameras to track people.[26] Amazon Rekognition was acquired by several private entities, and U.S. government agencies, including Immigration and Customs Enforcement and police in Orlando, Florida.[27] Rekognition's algorithms make the system capable of detecting gender, age range, and even people's emotions such as

[21] Niraj Chokshi, *Facial Recognition's Many Controversies, From Stadium Surveillance to Racist Software*, N. Y. TIMES (May 15, 2019), https://www.nytimes.com/2019/05/15/business/facial-recognition-software-controversy.html.

[22] Kanya A. Bennett, Comment, *Can Facial Recognition Technology Be Used to Fight The New War Against Terrorism?: Examining the Constitutionality of Facial Recognition Surveillance Systems*, 3 N.C. J.L. & TECH. 151, 157 (2001).

[23] *Id.*

[24] *Id.*

[25] *Facial Recognition: Top Seven Trends*, *supra* note 3.

[26] Jennifer Lynch, *HART: Homeland Security's Massive New Database Will Include Face Recognition, DNA, and Peoples' "Non-Obvious Relationships,"* ELEC. FRONTIER FOUND. (June 7, 2018), https://www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and.

[27] *Amazon Rekognition*, WIKIPEDIA, https://en.wikipedia.org/wiki/Amazon_Rekognition (last visited Mar. 8, 2021).

happiness, calmness and disgust, and other facial features such as beards, mustaches, eyeglasses, etc.[28] Rekognition is not only used by cities to identify suspects' faces but is also used by some nonprofit organizations, such as FamilySearch, to help users to see "which of their ancestors they most resemble based on family photographs".[29] In 2018, the Federal Bureau of Investigation (FBI) started to use Rekognition as a pilot program to analyze video surveillance.[30]

Clearview AI (Clearview) is a new American technology company that provides a facial recognition software service for law enforcements agencies to use.[31] Although the company is not a well-known company like Amazon, a number of Florida law enforcement agencies have tested or purchased access to Clearview's facial recognition system.[32] Pinellas County, Florida, has been using facial recognition for two decades as a tool to track suspects and joined several law enforcement agencies using Clearview after witnessing the usefulness of Clearview's system.[33] The turning point is when Pinellas Police tried to identify a suspect through a surveillance footage without any progress for several days.[34] Even sending the picture of the suspects to other law enforcement agencies did not help; facing the needle in a haystack situation, Pinellas Police asked

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] *Clearview AI*, WIKIPEDIA, https://en.wikipedia.org/wiki/Clearview_AI (last visited Mar. 8, 2021).

[32] Allison Ross et al., *Florida Cops Use This Facial Recognition Tech that Could Be Pulling Your Pics*, TAMPA BAY TIMES (Feb. 11, 2020), https://www.tampabay.com/florida-politics/buzz/2020/02/11/florida-cops-use-this-facial-recognition-tech-that-could-be-pulling-your-pics/.

[33] *Id.*

[34] *Id.*

for help from Tampa Police, who were using Clearview's facial recognition system, and quickly found a match of the wanted suspect.[35] Hours later, the suspect was arrested.[36] Since then, Pinellas Police decided to join the trend of using Clearview.[37] It is reported that at least thirteen Florida law enforcement agencies tried Clearview's system; among those agencies, at least four signed contracts with Clearview and a fifth is about to.[38] However, the use of Clearview has led to a heated discussion in the United States. In New Jersey, the Attorney General has asked for a temporary stop for using Clearview in the state because of Clearview's ability to combine online information into its facial recognition databases.[39]

B. Use of facial recognition technology in foreign countries

Facial recognition technology is broadly used in foreign countries such as China, Singapore, and Japan.[40] According to a forecast, the global market for the technology will reach $7 billion by 2022.[41] In China, there are 200 million surveillance cameras, which means there is one camera for every seven people.[42] By 2021, China plans to install 400 million more cameras to help with

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] Ross et al., *supra* note 32.

[39] *Id.*

[40] Sintia Radu, *The Technology That's Turning Heads*, U.S. NEWS (July 26, 2019, 4:38 PM), https://www.usnews.com/news/best-countries/articles/2019-07-26/growing-number-of-countries-employing-facial-recognition-technology.

[41] *Id.*

[42] *Id.*

national security and traffic control.[43] China's facial recognition systems are used to catch criminals in real time, even small ones like thieves and jaywalkers.[44] Additionally, the facial recognition system is used as a payment method.[45] For example, at the KFC restaurants in Hangzhou, China, people can "smile to pay" through the facial recognition system; some banks allow their customers to withdraw money by using their faces as a substitute of cards.[46]

Like China, Japan is one of the top countries with the fastest adoption rates of facial recognition systems; the goal of using the facial recognition system in Japan is to improve security by not entirely relying on ID cards because cards can be easily forged and duplicated.[47] The system is also used to track employee behavior; the McDonald's in Japan has been using the facial recognition system to track employees' working behavior including how much the employees are smiling to their customers.[48] The system will detect when an employee is not smiling enough, and will alert the employees that their "smiley face is below standard."[49] It is also notable that Japan is using facial recognition technology to address "societal challenges" such as gambling addiction;

[43] *Id.*

[44] Shannon Liao, *Chinese Facial Recognition System Mistakes a Face on a Bus for a Jaywalker*, THE VERGE (Nov. 22, 2018, 10:31 AM), https://www.theverge.com/2018/11/22/18107885/china-facial-recognition-mistaken-jaywalker.

[45] Abishur Prakash, *Facial Recognition Cameras and AI: Five Countries with the Fastest Adoption*, ROBOTICS BUS. REV. (Dec. 21, 2018), https://www.roboticsbusinessreview.com/ai/facial-recognition-cameras-5-countries/.

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.*

Japanese casinos are using advanced facial recognition cameras to tell how many times a person has visited the casino.[50]

In the United Kingdom (U.K.), the High Court ruled that the South Wales Police's use of facial recognition cameras on the street is acceptable and does not violate people's privacy rights or other rights.[51] A resident of Cardiff, Wales claimed that the use of facial recognition by the South Wales Police was a violation of his rights because he was recorded by the system without permission.[52] The purported unauthorized record happened once while the claimant was shopping, and once while he was attending a political rally.[53] The facial recognition system used by the South Wales Police scans faces in a crowd; once the system finds a match, it sends an alert to officers in a command center so that the command center can send an officer to stop the person identified.[54] The British court found that the police have "sufficient legal controls" to prevent improper use of facial recognition technology; the controls implemented include the deletion of data if the facial information regarding someone not one the police's watch list.[55] However, there is an argument in the U.K. that, unlike DNA and fingerprint data, which generally will be destroyed within a certain period once individuals arrested or charged are acquitted, there are no rules in the U.K. regulating

[50] *Id.*

[51] Adam Satariano, *Police Use of Facial Recognition Is Accepted by British Court*, N. Y. TIMES (Sept. 4, 2019), https://www.nytimes.com/2019/09/04/business/facial-recognition-uk-court.html.

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *Id.*

the retention of facial images in facial recognition databases.[56] In the U.K., the Police National Database has "snowballed to contain about twenty million" people's facial information,, and a great amount of those people in the database had never been charged or convicted of any offense.[57] Unlike DNA and fingerprint data, innocent people's facial information are stored in the database without their knowledge or consent.[58]

C. Legal background for law enforcement to use facial recognition as a policing tool in the United States

Although law enforcement agencies have been using facial recognition technology for years, there has been no federal law controlling such use of facial recognition technology, and there is no court decision restricting the use in the United States either.[59] The facial recognition technology is not under federal control at all in the United States.[60] Some state lawmakers say that the use of facial recognition technology by law enforcement agencies should be paused to allow lawmakers to take some time to decide whether the technology should be entirely banned.[61]

[56] Hannah Devlin, *"We Are Hurtling Towards a Surveillance State": The Rise of Facial Recognition Technology*, THE GUARDIAN (Oct. 5, 2019, 5:00 PM), https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurtling-towards-surveillance-state.

[57] *Id.*

[58] *Id.*

[59] Olivia Solon, *Facial Recognition Database Used by FBI Is Out of Control, House Committee Hears*, THE GUARDIAN (Mar. 27, 2017, 6:00 PM), https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports.

[60] *Id.*

[61] Stacey Barchenger, *Facial Recognition Can ID You in a Crowd. But Who's Using It, How to Regulate It*, NORTH JERSEY (Feb. 6, 2020, 12:18PM), https://www.northjersey.com/story/news/2020/02/06/facial-recognition-clearview-police-new-jersey-attorney-general/4666380002/.

Due to lack of federal regulation, states, and even cities in the same state, have various rules hold different views regarding the use of facial recognition technology. Some states such as California and Massachusetts have banned, though not completely, the use of facial recognition technology in body cameras used by law enforcement.[62] Some states such as Oregon and New Jersey are using the technology.[63] In Washington County, Oregon, officers use the facial recognition system by running suspect's images which usually come from security camera footage against the jail booking database, and potential matches will show up in seconds if there are any.[64] The technology saves the department time, manpower, and effort compared to manually searching a database with more than 300,000 pictures.[65] According to the officers in Washington County, Oregon, the facial recognition system is a tool that they use only when there is a probable cause that a person committed a crime, and the department only searches the suspect's photo against the jail booking photos without searching the Department of Motor Vehicle database.[66] However, Portland, the largest city in Oregon, has the intention to ban facial recognition technology used by private companies.[67] Yet, it is unknown whether pending legislation for the ban will be passed and

[62] *Id.*; Gomez & Rosenberg, *supra* note 11.

[63] *See* Barchenger, *supra* note 61.

[64] Ghaffary, *supra* note 13.

[65] *Id.*

[66] *Id.*

[67] Kristin Lam, *Portland, the Largest City in Oregon, Plans to Propose First Facial Recognition Ban Affecting Private Companies*, USA TODAY (Feb. 4, 2019, 9:39 PM), https://www.usatoday.com/story/tech/2019/12/03/facial-recognition-portland-oregon-ban/2601966001/.

how it is going to influence the law enforcement agencies' uses in Portland.[68] Different cities in Florida also hold different views about the technology. Police in Orlando, Florida tried to use Amazon Rekognition as a policing tool but ultimately decided not to use it.[69] The department had failed to use the facial recognition system effectively, and the department encountered both technical difficulties and constant public criticism.[70] The City Council reportedly said that the testing of Rekognition did not have any "noticeable progress."[71] Law enforcement agencies in Volusia County, Florida purchased Clearview's facial recognition system to help catch up wanted suspects.[72] As mentioned, Clearview is able to look through sources on the Internet to identify a person, and the Volusia County Sheriff stressed that not all the employees have authorized access to the Clearview system.[73] Additionally, Volusia County emphasized that they use facial recognition technology as an investigative tool without creating a facial recognition database.[74] In Newark, New Jersey's largest city, officials admitted that their police department is using facial recognition technology to identify suspects.[75] Anthony F. Ambrose, the Newark Department of

[68] *Id.*

[69] Ghaffary, *supra* note 13.

[70] *Id.*

[71] Mariella Moon, *Orlando Won't Use Amazon's Facial Recognition Software Anymore*, ENGADGET (July 19, 2019), https://www.engadget.com/2019/07/19/orlando-amazon-rekognition-pilot/.

[72] Claire Metz, *Volusia County Sheriff's Now Using Facial Recognition Software*, WESH2, https://www.wesh.com/article/volusia-county-sheriff-s-office-using-facial-recognition-software/30735498 (last updated Feb. 3, 2020).

[73] *Id.*

[74] *Id.*

[75] Barchenger, *supra* note 61.

Public Safety Director, confirmed that the city has been using the technology for years, and the technology is incredibly helpful in cases of robberies and burglaries.[76]

III. Issues behind law enforcement's use of facial identification technology

There have been endless debates about federal use of recognition technology at both the state and federal level and in foreign countries.[77] United States senators, Chris Coon and Mike Lee, recognized problems and risks arose from use of the technology and proposed a new bill aimed to limit the federal use of the facial recognition technology.[78] The bill was titled as The Facial Recognition Technology Warrant Act of 2019 and was proposed to make sure that law enforcement agencies have the tools necessary to keep the safety of the United States while protecting people's personal rights.[79] While several legal issues regarding police use of facial recognition technology have risen, there is no regulation yet.

A. Fourth Amendment Right of Privacy and Data Privacy

The Fourth Amendment is designed to protect people from unlimited police power and government overreach; it bars the government from unreasonable search and seizure of an individual and their property.[80] Search of an electronic devices' content, cellphone history, and Internet surfing history can all be a violation of the Fourth Amendment.[81] However, while a

[76] *Id.*

[77] Lusamba, *supra* note 9.

[78] *Id.*

[79] *Id.*

[80] U.S. CONST. amend. IV.

[81] *See Constitutional Limits to Cell Phone Searches Incident to Arrest*, FINDLAW, https://practice.findlaw.com/practice-guide/constitutional-limits-to-cell-phone-searches-incident-to-arrest.html (last updated June 20, 2016).

thermal-imaging device pointed at a private home from a public street to detect heat within the home is a "search" in violation of the Fourth Amendment, it is not clear whether running an image against a facial recognition database constitutes a "search" that violates a person's reasonable expectation of privacy.[82]

The next question arose as to where law enforcement agencies collected people's facial information for facial recognition purposes and when do people surrender their facial features to law enforcement agencies?[83] There are two kinds of sources to build up the facial recognition databases.[84] Ordinarily, police departments acquire facial recognition software from a technology company, and they will use the technology to run searches against their existing law enforcement-controlled databases of photos.[85] The databases usually include mugshots, driver's licenses, and sex offender registries.[86] Similar to the law enforcement-controlled databases in the U.K., about half of adult Americans' photos, without the individuals knowledge and consent, are stored in the facial recognition databases that are accessible to the FBI with the purposes of hunting criminal suspects.[87] Approximately eighty percent of the photos in the FBI database network are non-criminal entries, including pictures from driver's licenses and passports.[88] Despite the consent from people for using their photos in facial recognition databases, law enforcement agencies are

[82] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[83] *See* Gladstone, *supra* note 2.

[84] *See* Ross et al., *supra* note 32.

[85] *Id.*

[86] *Id.*

[87] Devlin, *supra* note 56; Solon, *supra* note 59.

[88] Solon, *supra* note 59.

using people's photos. There are also technology companies, such as Clearview, building their own databases based on online public sources; Clearview's software scrapes public photos from commercial site into its databases and the law enforcement agencies will use the Clearview's own database to make a search.[89]

No matter how the facial recognition system is building up its databases, most people never consent to provide photos to be part of the databases.[90] Photos of innocent persons are collected and compiled proactively into facial recognition databases, which is different from the collection of fingerprints and DNA information from people who had already been arrested.[91] While people gave no consent for their driver's license photos to be used in the facial recognition databases, the FBI dealt with eighteen states in the United States to access the states' databases of driver's license photos.[92] Even worse, without consent and awareness of the collection of facial information, people's facial information is under the risk of being hacked by parties with improper purposes.[93] As long as there law enforcement agencies or private companies storing people's biometric information, the databases that contain such biometric information can possibly be accessed by an unauthorized employee or hacked if not stored properly.[94] Richard Parris, CEO of Intercede, a

[89] Ross et al., *supra* note 32.

[90] Jack Laperruque, *Unmasking the Realities of Facial Recognition*, PROJECT ON GOVERNANCE OVERSIGHT (Dec. 5, 2018), https://www.pogo.org/analysis/2018/12/unmasking-the-realities-of-facial-recognition/.

[91] Solon, *supra* note 59.

[92] *Id.*

[93] *Facial Recognition System*, WIKIPEDIA, https://en.wikipedia.org/wiki/Facial_recognition_system (last visited Mar. 9, 2021).

[94] *Id.*

cybersecurity company, said that "hackers will already be looking to replicate people's faces to trick facial recognition systems."[95] Since both the law enforcement agencies and the companies providing facial recognition technology are holding people's facial information in the databases, the data is vulnerable from both the law enforcement agencies and the technology companies end.[96]

B. First Amendment Right of Freedom – Civil Liberties and Mass Surveillance

The First Amendment protects the right of expression, free speech and press, and the right to protest; it also protects the right to religious beliefs and practices so that the government will not favor a particular religion.[97] People now worry that the implementation of facial recognition technology as a policing tool will start an era of mass surveillance, which is arguably a First Amendment violation.[98] It is not unreasonable for people to worry about mass surveillance since state law enforcement agencies had already used facial recognition technology in public.[99] Police in Baltimore, Maryland ran photos of protesters, who were protesting the death of Freddie Gray, from social media against the facial recognition database to identify protesters and arrest them.[100] This is not the only instance of facial recognition being used in police making arrests.[101] In 2019,

[95] Hannah Williams, *Facial Recognition Technology: What Are The Dangers?*, WINSONIC, https://www.ewinsonic.com/blog-Facial%20recognition%20technology.html (last visited Mar. 9, 2021).

[96] *See id.*

[97] U.S. CONST. amend. I.

[98] *Ban Face Surveillance*, ELEC. PRIV. INFO. CTR., https://epic.org/banfacesurveillance/ (last visited Mar. 9, 2021).

[99] Lynch, *supra* note 26.

[100] *Id.*

[101] Id.

after a mass shooting happened in Annapolis, Maryland, the police used facial recognition technology to identify the suspect because the arrested suspect was neither identifiable nor cooperative.[102] While some people are happy that a suspected shooter that killed five people was identified, several civil liberty groups expressed fear of overly oppressive surveillance.[103] With the help of facial recognition technology, the police department in Clermont, Florida successfully identified and arrested a women accused of stealing a grill.[104] The facial recognition technology helps law enforcement officers to identify suspects, but the technology's excellent ability makes people afraid that the government is always watching people.[105]

The face is a unique part of a person's body, and facial recognition data is categorized as sensitive personal data that needs additional protection under the General Data Protection Regulation (GDPR).[106] The GDPR is implemented by the European Union (EU) to protect both live and non-live images of people's face.[107] France's data protection watchdog expressed

[102] Ian Bogost, *The Way Police Identified The Capital Gazette Shooter Was Totally Normal*, THE ATLANTIC (June 29, 2018), https://www.theatlantic.com/technology/archive/2018/06/capital-gazette-shooting-face-recognition/564185/.

[103] Kate Conger et al., *San Francisco Bans Facial Recognition Technology*, N. Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

[104] Jon Jankowski, *Grill Thief Arrested After Photo Ran Through Facial Recognition Software, Police Say*, CLICK ORLANDO (Dec. 27, 2019, 4:06 PM), https://www.clickorlando.com/news/local/2019/12/27/grill-thief-arrested-after-photo-ran-through-facial-recognition-software-police-say/.

[105] Schuppe, *supra* note 17.

[106] Akshaya Asokan, *Facial Recognition Use Triggers GDPR Fine*, BANK INFO SEC. (Aug. 28, 2019), https://www.bankinfosecurity.com/facial-recognition-use-triggers-gdpr-fine-a-12991.

[107] Ella Jakubowska, *Facial Recognition and Fundamental Rights 101*, EUR. DIGIT. RTS. (Dec. 4, 2019), https://edri.org/facial-recognition-and-fundamental-rights-101/.

concerns that people's faces, which are a "very personal form of personal data," have a particular sensitivity when it comes to surveillance; a face can be "a marker of protected characteristics under international law such as your right to freely practice your religion."[108] Distinguishable from a password, faces are unique to everyone; a person can keep his or her password out of sight and even reset it when it is not safe anymore, but it is impossible to do the same with a face.[109] Furthermore, unlike other forms of biometric data such as fingerprints and DNA data that can never be scanned automatically on the street, it is hard to avoid being subject to facial surveillance if facial recognition technology is used in public places.[110] By collecting and analyzing people's unique facial information, the facial recognition technology is highly intrusive.[111] Once the technology is used for mass surveillance, it threatens not just the right to privacy, but also will encroach "democracy, freedom, and the opportunity to develop one's self with dignity, autonomy and equality in society."[112] Such surveillance can result in a chilling effect on "any legal dissent, stifling legitimate criticism, protest, journalism and activism by creating a culture of fear and surveillance in public spaces."[113]

Facial recognition data is so unique, and facial recognition technology now actually has the capacity to scan and identify the faces of people in real time.[114] The technology, since its first

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] Jakubowska, *supra* note 107.

[114] *Ban Face Surveillance*, *supra* note 98.

creation, has evolved to become capable of mass surveillance and political control; it is capable of making "human identification, behavioral assessment and predictive analysis."[115] Jason Chaffetz, the former Chairman of the U.S. House Committee on Oversight and Government Reform, said that facial recognition technology is "a powerful police tool to protect people, border and [our] nation," and a great tool to "protect financial transactions and prevent fraud or identity theft" from a private perspective.[116] However, Chaffetz also acknowledged the risk of the technology being used to harass or stalk individuals, to "chill free speech and free association by targeting people attending certain political meetings, protests, churches, or other types of places in the public."[117] In New Jersey, Assemblyman Andrew Zwicker also suggested the technology could lead to widespread mass surveillance.[118] Nowadays, because cameras are virtually everywhere in the public spaces, the facial recognition technology could easily be used to identify "people who are carrying out their First Amendment rights" during protests or religious activities.[119]

C. Bias, discrimination and inaccurate facial recognition data leading to wrongful conviction

One reason that facial recognition technology is not accurate in identifying people it that people's faces change overtime. On the contrary, fingerprints and DNA data that law enforcement

[115] *Id.*

[116] Solon, *supra* note 59; *Jason Chaffetz*, WIKIPEDIA, https://en.wikipedia.org/wiki/Jason_Chaffetz (last updated Oct. 9, 2020).

[117] Solon, *supra* note 59.

[118] Barchenger, *supra* note 61.

[119] *Id.*

agencies are using are genetic biometric data that generally do not change during a person's life.[120] In maintaining the accuracy of facial recognition technology, one has to take into account different factors.[121] The factors influencing a person's facial features include, but are not limited to, aging, plastic surgery, cosmetics, effects of drug abuse or smoking, and pose of the subject.[122] The nature of facial features changing overtime result in the technology's inaccuracy, which means we cannot entirely depend on the result of facial recognition matches.

Beside the natural changing of people's faces, the facial recognition systems themselves are not accurate enough in providing results. According to a federal government study in 2019, there are great disparities generated by different facial recognition software.[123] The study examined nearly two hundred algorithms used in a facial recognition system and found that even one algorithm can have a different accuracy rate for different demographic groups.[124] Some of the algorithms have a higher rate of misidentifying images of African American women.[125] The biased results make people afraid that the "unreliable" technology will not protect the communities because of the significant discrimination and bias present in the results.[126] Massachusetts Institute of Technology's Media Lab also conducted research and found that Amazon's Rekognition has

[120] *Facial Recognition*, INTERPOL, https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition (last visited Mar. 9, 2021).

[121] *Id.*

[122] *Id.*

[123] Barchenger, *supra* note 61.

[124] *Id.*

[125] *Id.*

[126] *Id.*

the problem of gender and racial bias, although Amazon has advanced technology in detecting people faces.[127] Using Amazon Rekognition, a study made by the American Civil Liberties Union (ACLU) found that twenty-eight members of Congress were misidentified as people who had been arrested for crimes.[128] In addition, the study showed the same result as other researches that facial recognition technology is more biased against women with darker skin than white men.[129] The ACLU test shows about forty percent of the false matches generated were of people of color.[130] The use of the "biased" technology may make black men and boys more susceptible for arrests or claims against them for criminal activity, not to mention black males are "already more than twice as likely to die during an encounter with police than their white counterparts."[131]

It is no question that bias and discrimination exist in today's society.[132] Researchers used verified data on police killings from 2013 to 2018 and found that approximately one in one thousand black boys and men will be killed by police in their lifetime.[133] However, the number is thirty-nine out of 100,000 for white counterparts, which means people of color are more likely to be killed by police.[134] If the facial recognition technology is also biased, which it is according to

[127] Gomez & Rosenberg, *supra* note 11.

[128] *Id.*

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] Brentin Mock, *What New Research Says About Race and Police Shootings*, BLOOMBERG CITYLAB (Aug. 6, 2019 1:28 PM), https://www.citylab.com/equity/2019/08/police-officer-shootings-gun-violence-racial-bias-crime-data/595528/.

[133] *Id.*

[134] *Id.*

research, this will cause “double bias” situations towards people with color and will lead to wrongful convictions if law enforcements relied on the biased results.[135] What makes the situation worse is that law enforcement agencies will share databases and information to work more efficiently, which means inaccurate and biased facial recognition data is not only being used in one department, but is also being shared with other agencies for them to use.[136] Police in Newark, New Jersey once confirmed that they keep their own database of images for facial recognition comparison and they also have the access to database maintained by New Jersey State Police.[137]

D. Lack of disclosure regarding use of facial recognition technology

Although law enforcement agencies confirmed their use of facial recognition technology as a policing and investigative tool to identify suspects, they never made any disclosure of such use in court during pretrial disclosures because facial recognition results cannot be presented in courts as evidence.[138] Generally, police use the facial recognition results in conjunction with other evidence to make a conclusive identification of an individual.[139] Hence, the use of facial recognition technology does not show up in public records usually or is not subject of many judicial rulings.[140] Without certain documents and rulings, the use of facial recognition technology in identifying suspects and the spread of the technology are not easy to track.[141] The Washington

[135] Barchenger, *supra* note 61.

[136] *Id.*

[137] *Id.*

[138] Schuppe, *supra* note 17.

[139] Hamann & Smith, *supra* note 12.

[140] Schuppe, *supra* note 17.

[141] *Id.*

County Police Department in Oregon disclosed that, in 2018, they did around 1,000 searches using the facial recognition system when there is reasonable suspicion that a person committed a crime.[142] After all, the Washington County Police made no effort to measure how many of the conducted searches led matched identities and whether such matches were correct or incorrect, according to the department's public information officer Daniel DiPietro.[143] Without enough disclosure about how the facial technology is used and the accuracy of the technology, people are more likely to worry about the technology's use and effectiveness in reducing crimes.[144] Especially, people worried about whether or not public anonymity will exist anymore if law enforcement agencies keep the use of technology as a secret without disclosing how they are utilizing facial recognition data and whether there is surveillance conducted on the public streets.[145]

IV. Arguments for restricted use of facial recognition technology

A. Facial recognition has unique advantages as a policing tool

Like fingerprints and DNA technology that were used by the law enforcement decades ago, the new facial recognition technology has the unquestionable potential to advance the effectiveness and efficiency of police investigations.[146] This is especially true when dealing with "violent crime, burglary, kidnapping and missing persons, where establishing a timeline and identifying suspects

[142] Ghaffary, *supra* note 13.

[143] *Id.*

[144] *Id.*

[145] Eoin O'Carroll, *Face Off? Americans Fear Privacy Loss to Recognition Software*, CHRISTIAN SCI. MONITOR (June 20, 2019), https://www.csmonitor.com/Technology/2019/0620/Face-off-Americans-fear-privacy-loss-to-recognition-software.

[146] Amy Mckeown, *It's Time for Consensus on Facial Recognition in Law Enforcement*, GCN (May 15, 2019), https://gcn.com/articles/2019/05/15/facial-recognition-law-enforcement.aspx.

as quickly as possible is key."[147] In assisting the law enforcement agencies' investigations, the facial recognition technology has unique advantages that fingerprint and DNA technology do not have: relatively lower price for building the system, time saving in conducting matches, and more secured from hackers.

The cost in building a facial recognition system is relatively lower than building and maintaining DNA databases because DNA data requires special laboratory tests, places for storing samples, and DNA tests usually take several days to obtain results.[148] Facial recognition systems, on the contrary, only need a small amount of overhead expenses once the system is installed. There is no need for laboratory tests and police officers can use the facial recognition system as a part of their daily work like using the normal computer which is easy to operate.[149] Unlike DNA technology, which is usually reserved for serious or high-profile cases, facial recognition technology is easy and simple to be used for routine crimes and can make a match quickly without waiting for days.[150] More importantly, it is harder for hackers to hack the facial recognition system than to hack fingerprint system or voice recognition system.[151] While more convenient to use and harder to be hacked, the facial recognition systems are also more affordable because they do not require additional hardware outside of computers.[152]

[147] *Id.*

[148] Schuppe, *supra* note 17.

[149] *Id.*

[150] *Id.*

[151] *Facial Recognition System*, *supra* note 93.

[152] Ashley Williams, *Four Reasons Why Facial Recognition Is Better at Biometric Verification than Fingerprints Scans*, SHUFTIPRO (Jan. 25, 2019), https://shuftipro.com/blogs/4-reasons-facial-recognition-better-biometric-verification-fingerprint-scans.

Facial recognition technology is more efficient in locating wanted persons compared to DNA and fingerprint technology because the facial recognition system can locate a person remotely. The FBI used facial recognition technology to locate Walter Yovany-Gomez, a man on the FBI's Ten Most Wanted Fugitives list.[153] Gomez is a member of the MS-13 street gang and was on the list due to a brutal murder happened in Plainfield, New Jersey.[154] For years, Gomez was able to evade authorities, but he was finally arrested by law enforcement with the help of "digital facial recognition system."[155] Although the FBI had Gomez's fingerprint information on file, the fingerprints were not able to lead to the arrest of Gomez, but only served as a confirmation of the person's identity.[156] In London, the Metropolitan Police tested facial recognition system in ten different locations, and the results confirmed that facial recognition technology has an excellent ability in spotting persons of interest.[157] Officials said that during the tests, seventy percent of wanted persons were spotted by the facial recognition system, and only one in 1,000 people were misidentified.[158] With the DNA and fingerprint technology, the police need to find the wanted person as a premise to have the chance to collect either the person's DNA or

[153] Ryan Lucas, *How a Tip – and Facial Recognition Technology – Helped the FBI Catch a Killer*, NAT'L PUB. RADIO (Aug. 21, 2019 5:01 AM), https://www.npr.org/2019/08/21/752484720/how-a-tip-and-facial-recognition-technology-helped-the-fbi-catch-a-killer.

[154] *Id.*

[155] *Id.*

[156] *See id.*

[157] Will Knight, *London Cops Will Use Facial Recognition To Hunt Suspects*, WIRED (Jan. 25, 2020, 7:00 AM), https://www.wired.com/story/londons-cops-facial-recognition-hunt-suspects/.

[158] *Id.*

fingerprint data to make a comparison with the existing databases.[159] However, facial recognition technology allows remote verification that saves the time and effort of finding a wanted person manually.[160]

When DNA or fingerprint technology is not able to come up with any match, facial recognition technology can supplement as a safeguard tool.[161] In Orlando, Florida, the police pulled over a man that had no identification cards.[162] The man had passed out after putting something in his mouth and his fingerprints were not available because it was chewed off.[163] The police were only able to identify the man by running his image through the facial recognition system.[164] The takeaway is that it is impossible to identify a person by DNA technology if the person's DNA data is not in the database; it is also impossible to identify a person through fingerprints if no such information exists in the database or the person loses his fingerprints; and it is possible that a person loses his government issued identification card or forged one. When all these methods fail, the facial recognition technology can be a great tool to remedy the situation. Even though there is a possibility of "no match" after running the facial recognition

[159] *See* Schuppe, *supra* note 17.

[160] Williams, supra note 152.

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

[162] *Id.*

[163] *Id.*

[164] *Id.*

system, it allows law enforcement agencies a larger possibility of identifying a hard-to-identify person.[165]

There are a large number of law enforcement officials who have used or tested the facial recognition technologies and speak highly of the facial recognition technologies. Bob Gualtieri, the Pinellas County Sheriff in Florida said his agency is carefully considering whether to purchase licenses for facial recognition technology from Clearview, observing that Clearview's facial recognition database has great power to match images to faces.[166] Ferrara, the Detective Sergeant in the Gainesville Police Department in Florida, said he made plentiful identifications of suspects, from suspects for shoplifting to financial fraud cases, using facial recognition.[167] Timothy Downes, the Detective Sergeant in the Clearwater Police Department in Florida, had talked to several officers around the United States, and said that they are all satisfied with the technology.[168] Hoan Ton-That, the chief executive of Clearview, said that their facial recognition technology is meant to "help identify perpetrators and victims of crimes from materials that have already been obtained, not to identify random members of the public."[169] And it is true, facial recognition technology is truly helping the law enforcement agencies to fight crimes.

B. Safeguards to regulate facial recognition technology is necessary

Only with proper regulation can society start to take advantage of the facial recognition technology. Even in the European Union, where facial information is classified as "particular[ly]

[165] *Id.*

[166] Ross et al., *supra* note 32.

[167] *Id.*

[168] *Id.*

[169] *Id.*

sensitive" personal data that requires additional protection under the GDPR, people are considering using facial recognition technology as long as there are adequate rules and regulations as safeguards to mitigate the technology's risks.[170] POLITICO reports that the EU President and Commissioner have considered banning the use of facial recognition technology in public spaces until there are safeguards to mitigate the technology's risks.[171] Several organizations and experts from over forty countries urged to "establish the legal rules, technical standards, and ethical guidelines necessary to safeguard fundamental rights and comply with legal obligations before further deployment of this technology occurs."[172]

In the United States, both law enforcement agencies and companies providing the facial recognition systems are emphasizing the necessity of regulation as a safeguard to oversee the use of facial recognition technology. NEC Corporation of America, one of the major developers of facial recognition systems, expressed that NEC is caring about the balance rights of citizens to privacy and law enforcement's ability to protect public safety.[173] Axon, the largest supplier of police body cameras in the United States, has acknowledged the public concerns of real-time facial recognition.[174] Axon stressed that it is not working on developing facial recognition for its devices.[175] However, Steve Tuttle, an Axon spokesman, said that "we do see a day when facial

[170] Asokan, *supra* note 106; *EU Leaders to Consider Ban on Face Surveillance*, *supra* note 18.

[171] *EU Leaders to Consider Ban on Face Surveillance*, *supra* note 18.

[172] *Id.*

[173] Jon Schuppe, *Facial Recognition Gives Police a Powerful New Tracking Tool. It's Also Raising Alarms*, NBC NEWS (July 30, 2018, 3:08 AM), https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936.

[174] *Id.*

[175] *Id.*

recognition, with the right controls and sufficient accuracy, could reduce bias and increase fairness in policing."[176] Orlando Police Chief John Mina, Florida, emphasized to the public that usually it is hard to find a suspect until the suspect accidently confronted with the police face to face, citing a 2017 murder case, where the suspect moved around the city for weeks before actually spotted by the police.[177] Mina thinks that the facial recognition system may make a difference to such a situation because the system can notify law enforcement officers, and once they have spotted the suspect, and they can respond to the notification immediately.[178] Mina had a positive view about facial recognition technology as a policing tool, and said that "ultimately, it's about enhancing public safety."[179] It is true, the use of facial recognition technology is ultimately a public safety question and should not be a threat to people's personal right. However, such balance requires rules justifying and regulating the law enforcement's use of the technology.

"I think we're very close to getting the technology into our law enforcement here," said Nicola Dickinson, vice president of Digital Barriers, who is responsible for the company's business in North and South America.[180] Digital Barriers disclosed that its real-time facial recognition system was acquired by law enforcement agencies in Europe, Asia, and within the U.S. government without disclosing detailed names of each agency.[181] Digital Barriers says that it is weighing the national security benefits of the technology and the public concerns regarding the

[176] *Id.*

[177] *Id.*

[178] *Id.*

[179] Schuppe, *supra* note 173.

[180] *Id.*

[181] *Id.*

possibility of mass-surveillance.[182] The company agrees that facial recognition technology should not be overused but it does not have any details in the user policy to tell what their customers can or cannot do.[183] The company simply trusts that the U.S. government has "rules and regulations within their organizations to use it effectively and safely."[184] It is true that the technology can be used effectively and safely under regulation. However, there is no such regulation yet.[185] It is foreseeable that, with proper regulation and guidelines, technology companies will have more guidelines in the user policies of the facial recognition system and the law enforcement agencies can use the technology is the best interest for society. To find a balance between personal rights and government power, a regulation is necessary.

C. Fourth Amendment "search" for non-surveillance facial recognition system

There are no applicable precedents to the use of facial recognition technology as a policing tool from the Supreme Court and no Federal Statues addressing the issue.[186] But, it is helpful to refer to Supreme Court's cases discussing the constitutionality of surveillance devices to better understand the idea of the Fourth Amendment. In *Katz v. United States*, the Court used a two-prong test to decide whether the right of privacy under the Fourth Amendment is violated: (1) a subjective expectation for privacy held by the individual, and (2) the privacy interest must be objectively recognized by society.[187] The most important factor in determining the whether a

[182] *Id.*

[183] *Id.*

[184] *Id.*

[185] Schuppe*, supra* note 173.

[186] *See* Bennett, *supra* note 22, at 161.

[187] *Id.*

constitution protection is necessity is a person's reasonable expectation of privacy.[188] Courts have held that in places such as public streets, sidewalks, employee work areas and public-school classroom, there is no reasonable expectation of privacy for people and no warrant is required for surveillance in such places.[189] Meanwhile, thermal-imaging devices aimed at a private home from a public street to detect relative amounts of heat within an individual's home constitutes a "search" within the meaning of the Fourth Amendment.[190] The Court said that "where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[191] According to the Supreme Court's decisions, people have fewer expectations of privacy in public, and surveillance in public is not a "search" under the Fourth Amendment.

The cases above help determine what is a "search" under the Fourth Amendment, and it is more likely that the Supreme Court will find running a search in the facial recognition system is not a prohibited "search" because comparing a wanted person's picture against the facial recognition databases is like people being identified by a police officer while walking on the street without any physical intrusion.[192] Such comparisons are for the public interest in identifying suspects that may harm national security.[193] It is no doubt that a person's right of privacy is invaded

[188] *Id.* at 161–62.

[189] *Id.* at 162.

[190] Kyllo v. United States, 533 U.S. 27, 52 n.1 (2001).

[191] *Id.*

[192] Bennett, *supra* note 22, at 162–63.

[193] *Id.*

if the law enforcement set up a device aimed at a private home under the Fourth Amendment.[194] However, a facial recognition search is fundamentally different because the databases consist of public information collected either by state and federal agencies or by technology companies through public pictures online. [195]

If the law enforcement agencies are not running a person's picture against a database of pictures, but are running against video footage from public spaces that they suspect a wanted person may have appeared, it is important to note this is still the equivalent of officers observing a crowd and comparing the faces to a wanted person's pictures at their hands; it is just much faster and may be more accurate.[196] Such comparison is no difference than a robotic police officer viewing people faces on the street without any physical instruction and people have no reasonable expectation of privacy in public spaces since they are expected to be indented by acquaintance any time at anywhere in public.[197] In the United Kingdom, the Metropolitan Police created a special unit called the "super-recognizers."[198] The members in the special "super-recognizers" team have the ability to identify a person who they had encountered years ago which has helped them with arresting wanted suspects.[199] It is hard to see a difference between an officer with good memory looking at people's face to identify suspects and facial recognition system's comparison of picture

[194] *See id.* at 167–68.

[195] *See* Ross et al., *supra* note 32.

[196] *See* Bennett, *supra* note 22, at 162–63.

[197] *Id.*

[198] Patrick Radden Keefe, *The Detectives Who Never Forget a Face*, THE NEW YORKER (Aug. 15, 2016), https://www.newyorker.com/magazine/2016/08/22/londons-super-recognizer-police-force.

[199] *See id.*

against police-controlled databases. The only difference is that the facial recognition search is faster in providing a result which is time saving, and this can lead to better results when time is the key point in a cases such as murder and kidnapping.[200]

D. Establishing a federal rule in regulating law enforcement's use of facial recognition technology

Facial recognition technology, while being extremely helpful as a policing tool, can be used for mass surveillance in combination with public cameras, and it can be used in a "passive way that doesn't require the knowledge, consent, or participation of the subject."[201] There should be laws and regulations to refer to rules that law enforcement can use regarding facial recognition technology in order to allow them to use it while also regulating it.

1. Protection of data privacy

Facial information in facial recognition databases are hackable and procedures regulating the access and the protection of the data is necessary.[202] Technology development makes people's facial information vulnerable since "the use of the face in AI algorithms has gone far beyond mere identification to enter the realm of recreation."[203] The technology advances have significantly changed the non-transferable nature of people's facial features.[204] The non-transferable features of

[200] Bennett, *supra* note 22, at 168; *See* Ghaffary, *supra* note 13.

[201] *Face Recognition Technology*, AM. C.L. UNION, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology (last visited Mar. 12, 2021).

[202] Karen Epper Hoffman, *Biometric Hacking: Even Your Face Is Hackable*, CHIEF INV. OFFICER (Sept. 30, 2019), https://www.ai-cio.com/news/biometric-hacking-even-face-hackable/.

[203] Javier Yanes, *How to Hack a Face: From Facial Recognition to Facial Recreation*, OPENMIND BBVA (July 26, 2019), https://www.bbvaopenmind.com/en/technology/innovation/how-to-hack-a-face-from-facial-recognition-to-facial-recreation/.

[204] *Id.*

people's faces means that whenever and wherever a person's face appears in a place, that means the person is actually there because no one can take the person's face elsewhere.[205] However, starting from 2016, it is reported that some algorithms have the ability to modify videos of a person's face.[206] Such algorithms have great power that they can transplant one person's facial expressions to another person's picture or videos, which means a person's movement of lip can be modified to say something that they never had expressed in the video.[207] Once, the former US President Barack Obama's face was transplanted to a speech that he had never delivered.[208] The face-transplanting technology seems fun, but there is a potential that technology can be used for not so noble purposes.[209] Once a hacker gets people's facial information form facial recognition databases, it is unimaginable what they can do with all of the sensitive information. Generally, any new technological tool that can make a huge difference to the society may lead to undesirable consequences, and that is why we need safeguards to tackle the malicious uses of such technologies.[210]

The data in facial recognition databases contained both facial information and personal information related to each face. In protecting people's facial information from being unitized by unauthorized parties, rules regulating employees from both the law enforcement agencies and the companies with access to the facial recognition databases should be implemented to make them

[205] *Id.*

[206] *Id.*

[207] *Id.*

[208] *Id.*

[209] Yanes*, supra* note 203.

[210] *Id*.

accountable.[211] When there is already a data breach, breach notification legislation should be in place. Though no data breach notification requirement exists yet for facial recognition databases, states have their own breach notification statutes when it comes to personal information.[212] For example, in California, if there is a data breach that could result in the unauthorized acquisition of unencrypted personal information, the entity keeping such information should notify the person whose information is at risk without unreasonable delay.[213] Taking various states' existing regulations to protect personal information, the new regulation regulating facial recognition databases should have the same breach notification requirement so that people have knowledge when their information is hacked and can take some actions to prevent or mitigate any damages due to the improper use of their facial information.

2. Restriction on purpose for using the technology

It has been discussed that if the technology is not for surveillance purposes, but only for identifying a wanted person, is it likely that courts will find that is not a "search" under the Fourth Amendment. What if the law enforcement agencies want to use the technology to surveil a specific group of people? The Facial Recognition Technology Warrant Act of 2019 was introduced to Congress to restrict the federal use of facial recognition technology and provided a model of future federal rules.[214] The bill said that the technology should not be used for on-going surveillance of

[211] Clare Garvie et al., *The Perpetual Line-Up: Section XI Model Face Recognition Use Policy*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/appendix/model-police-use-policy.

[212] *Data Breach Notification Laws by State*, IT GOVERNANCE, https://www.itgovernanceusa.com/data-breach-notification-laws (last updated July 2018).

[213] *Id.*

[214] *See* Lusamba, *supra* note 9.

certain individuals or groups of individuals even in public spaces where people have no expectation of privacy.[215]

Under the proposed bill, there are exceptional circumstances where facial recognition technology can be used for on-going surveillance, but only if the law enforcement agency obtained a covered court order and such surveillance is necessary for the law enforcement agency's activity.[216] The bill also proposed that when there is exigent circumstances and it is impracticable to obtain a covered court order, then law enforcement agencies may do the surveillance without court order.[217] Any person aggrieved by facial recognition as an on-going surveillance tool has a right to challenge the use.[218] More importantly, the judge issuing or denying a warrant for the use of facial recognition surveillance shall file a report with Administrative Office of the United States Courts so that there is someone who can oversee the whole process since facial recognition surveillance is a special use of the technology and the technology is a unique powerful tool.[219] The proposed bill provided great rules in regulating facial recognition technology's use as a surveillance tool, and the proposed rules resemble the existing rules regulating "search warrant[s]."

3. Public disclosure of the technology

Knowing that law enforcement agencies have been using the facial recognition system, it is not known how long the agencies have been using the software or how many people have been

[215] Facial Recognition Technology Warrant Act of 2019, S. 2878, 116th Cong. § 3(a) (2019).

[216] *Id.*

[217] *Id.* at § 3(c).

[218] *Id.* at § 3(e).

[219] *Id.* at § 4(a); *See* Garvie et al., *supra* note 211.

arrested due to the use of the technology.[220] It is also unclear that except from photos of driver's licenses, identification cards, passports, mugshots of arrested people and online sources as discussed, whether police departments are using other sources to build up facial recognition databases to enhance the searching ability. For example, there are at least thirty police departments in New Jersey that have agreements with Amazon-owned Ring doorbell cameras to access the company's videos, but no one disclosed whether such videos are used in facial recognition databases.[221] "We don't know who is using it, we don't know how they're using it," said Assemblyman Zwicker from New Jersey, who is worrying about how the technology can be used for mass-surveillance.[222] The relatively new technology has led to people wondering who is using the technology, whether the result of the technology is accurate, what the law enforcement agencies will do with people's information, with whom the law enforcement agencies are sharing the sensitive facial information to, and what will happen if someone is identified by the technology.[223]

Most people's fears about facial recognition technology comes from limited knowledge about how the technology is used and whether it is effective in reducing crimes.[224] Without systemic federal regulation or permitting processes that make the use of facial recognition technology transparent, the public has little information about the technology and will never feel

[220] Megan Cruz et al., *Florida Law Enforcement Agencies Use Facial Recognition to Identify Alleged Thief*, WFTV (Dec. 27, 2019, 10:23 PM), https://www.wftv.com/news/local/florida-law-enforcement-agencies-use-facial-recognition-identify-alleged-thief/SGHPUGB5W5CX3FYVSLU7P6EV7I/.

[221] Barchenger, *supra* note 61.

[222] *Id.*

[223] *Id.*

[224] Ghaffary, *supra* note 13.

safe in front of the invisible technology.[225] Generally, the public will overestimate the capabilities of facial recognition technology and without concrete details about the purpose of the technology, people may speculate that something improper is going on without their knowledge.[226] Maja Pantic, the research director at the Samsung AI Centre, disclosed that people are worrying about how cameras can track people while shopping and store their biometric data into the databases.[227] However, Pantic cleared up that even the world's leading algorithm for learning new faces can only store the information up to about fifty faces and then it will stop working.[228] She also said that "people don't understand how the technology works and start spreading fear for no reason."[229] This is why public disclosure is a must for people to trust the technology.

Facial recognition technology has its risks, but a report has shown that people, even the Technology and Civil Liberties Director at the ACLU of North California and members from Electronic Frontier Foundation (EFF) who have been fighting for civil liberties, supports the use of the technology as long as there are more detailed rules and disclosures about the accuracy of the figures and how the technology is performed on different ethnic groups.[230] If the law enforcement agencies are using the technology, it is better for them to disclose to society that they are using it in the way expected by people to reduce society's anxiety about the technology.

4. Human Verification of Facial Recognition Results

[225] *Id.*

[226] Devlin, *supra* note 56.

[227] *Id.*

[228] *Id.*

[229] *Id.*

[230] *EU Leaders to Consider Ban on Face Surveillance*, *supra* note 18.

The ACLU of New Jersey pointed out that facial recognition technology creates the risk of wrongful arrests if there was an incorrect identification.[231] The concern of misidentifying people is truly happening because of lack of audits.[232] The Davie Police Department in Florida once ran a reporter's photo through Clearview's system during an interview to show how the system works.[233] In seconds, more than thirty pictures of the reporter's face showed up; the pictures are mainly from news websites and social media.[234] According to the search results, the police were able to see the reporter's name, and also the names of the reporter's friends and co-workers.[235] Clearview's system is incredible in identifying wanted persons and even the wanted person's friends and families, but the only verification of the system's accuracy comes from Clearview's own audit.[236] Clare Garvie from the Georgetown University Law Center on Privacy and Technology pointed out that there is no guarantee that personal identities associated with each photo in the facial recognition system are correct, and it is possible that innocent people can be arrested if there is a misidentification.[237] The databases for facial recognition systems are so large that there is a huge chance for people who look alike to be misidentified.[238]

[231] Barchenger, *supra* note 61.

[232] *See* Ross et al., *supra* note 32.

[233] *Id*.

[234] *Id*.

[235] *Id*.

[236] *Id.*

[237] *Id.*

[238] Ross et al., *supra* note 32.

According to a report, there are plenty of innocent people being convicted in the past decade due to eyewitness's misidentification of people.[239] People make mistakes, and facial identification will make misidentifications more serious since it is not accurate enough in producing results.[240] However, even if the results can be biased due to technological flaws, it is much better than judgment by human beings alone because human beings are not bias-free as well.[241] Eddie Reyes, the Director of Public Safety Communications for 911 in Prince William County, Virginia, once said that people should not compare facial recognition technology's use to a perfect status quo because such perfectness never exists.[242] According to Reyes, facial recognition technology can do things much better at identifying people than human beings because people can be biased, will make mistakes, and can get tired after a long time of comparing work.[243] Hence, instead of banning the technology, it is necessary to combine manpower and facial recognition systems to make police investigations more efficient. The proposed bill, the Facial Recognition Technology Warrant Act of 2019, also supports human review and testing; though the bill is more about facial recognition as a surveillance tool, it is equally applicable to non-surveillance use of the technology.[244] The Metropolitan Police in London with the super-recognizers team expressed their support in the manual check of the facial recognition system,

[239] *DNA Exonerations in the United States*, INNOCENCE PROJECT, https://www.innocenceproject.org/dna-exonerations-in-the-united-states/ (last visited Mar. 12, 2021).

[240] *Id.*

[241] Ghaffary, *supra* note 13

[242] *Id.*

[243] *Id.*

[244] Facial Recognition Technology Warrant Act of 2019, S. 2878, 116th Cong. § 5(b) (2019).

saying that "facial recognition technology is absolutely outstanding, but you always need someone at the end to confirm it."[245] When considering whether to keep using facial recognition technology, representatives of both the Newark and the Attorney General's office from New Jersey told lawmakers that there must be someone independently verifying the results generated by the facial recognition system; the key point is that the facial recognition system should only be a pointer that gives police a hint in identifying people, but not as sole evidence to justify arrests.[246]

5. Other procedural restrictions: training, testing and maintenance

Supporters of facial recognition technology claim that the facial recognition systems law enforcement agencies choose to use should be tested by the National Institute of Standards and Technology (NIST) and any untested systems are not qualified to be a policing tool.[247] Similarly, the Facial Recognition Technology Warrant Act of 2019 proposed testing procedures between law enforcement agencies and the NIST as well to ensure the technology's development and accuracy.[248] Apart from testing, it is necessary that the technology is not used as sole evidence to arrest suspects, but only as a technical identifier of possible suspects to avoid arbitrary decisions.[249]

Rules regulating the FBI's investigation using DNA samples have stressed that for DNA identification records to be included in the Combined DNA Index System (CODIS), the DNA analyses must come from laboratories or state, local, or federal agencies that meet certain

[245] Katie Collins*, "Super Recognizer" Cops Give Facial Recognition Systems a Run for Their Money*, CNET (Apr. 1, 2019, 11:57 AM), https://www.cnet.com/news/super-recognizer-cops-give-facial-recognition-systems-a-run-for-their-money/.

[246] Barchenger, *supra* note 61.

[247] Mckeown, *supra* note 146.

[248] S. 2878, 116th Cong. § 5(b).

[249] Barchenger, *supra* note 61.

guidelines and, in the case of external laboratories, undergo external audits.[250] Applicable to facial recognition databases, the new federal rule should indicate what data the law enforcement agencies can put in the databases and what procedures there should be to ensure no alteration was made to the data since facial information can be altered by AI technology.[251] Due to the sensitivity of the facial information stored, all persons authorized to access the facial recognition systems, including the company who developed the system, should receive special training.[252] The training should include educating the authorized employees on the proper purpose and use of the facial recognition system, how to take high quality pictures for the system, how to share the facial information safely, and how to delete undesired information.[253] Furthermore, there shall be a special department auditing the use and search within the facial recognition system, so as to have retrievable and detailed records of how the data within the facial recognition system was used.[254]

V. Conclusion

More than fifty percent of crimes still remain unsolved because of difficulties in arresting suspects according to the FBI universal crime reporting data.[255] With facial recognition technology, which can identify persons remotely, police can do better to keep communities safe and lower the

[250] 34 U.S.C. § 12592(b) (LEXIS through Pub. L. No. 116-163) (approved Oct. 2, 2020).

[251] Yanes, *supra* note 203.

[252] Matt Ford, *How the Supreme Court Could Rewrite the Rules for DNA Searches*, THE NEW REPUBLIC (Apr. 30, 2018), https://newrepublic.com/article/148170/supreme-court-rewrite-rules-dna-searches.

[253] Garvie et al., *supra* note 211.

[254] *Id.*

[255] Mckeown, *supra* note 146.

rate of the unsolved crimes. However, the question becomes "Do you want to pick the 'Big Brother's watching you' side or the side where you want to catch the bad guy?"[256]

In this era, according to Sonia Suter, a George Washington University law professor, there is a tendency that society will minimize the privacy costs because the gains are so great. Compared to the concrete benefits of catching killers and rapists that will do great harm to people's lives, the concession of privacy to facial recognition technology is easily discounted because privacy is always more amorphous.[257] Though DNA technology has raised the same privacy issues in early days, it is now considered the gold standard for criminal prosecutions in the United States. It is always a question about how the government uses and protects the data that people surrendered for public safety purposes. To better use the technology, we need federal regulations regulating how the technology should be used to balance people's privacy right and the public interest of national security. It is true that the technology is not accurate enough. However, technology is developing in a rapid pace, and with regulation and special oversight, it is foreseeable that facial recognition technology can greatly enhance law enforcement's ability to find wanted persons. It is important to acknowledge that we are in an era of science and technology, and it is unavoidable that facial recognition technology is going to play a role in helping with the national security system, as fingerprints and DNA technology did in the past.

[256] Ross et al., *supra* note 32.

[257] Ford, *supra* note 252.