FACIAL RECOGNITION TECHNOLOGY AND THE CONSTITUTION

Mark Simonitis

FACIAL RECOGNITION TECHNOLOGY AND THE CONSTITUTION

Mark Simonitis

INTRODUCTION

Over the past several years, we have seen an increase in the adoption and use of facial recognition technology (FRT). Both private corporations and government organizations have increasingly used this technology over the past several years, and law enforcement agencies have been just as eager to utilize FRT in their operations. The potential uses for this technology in a law enforcement capacity are numerous. For example, FRT could be used to identify criminals whose faces were caught on surveillance footage, or it could be used to help identify citizens during border crossings. However, it is easy to imagine how an invasive use of this technology could potentially threaten several constitutional rights. There have been enough cases discussing inappropriate uses of biometric technologies, of which FRT is one, that it is only a matter of time before a case involving the technology is brought before the Supreme Court or until congressional legislation is passed that regulates its use. However, until that day comes, the invasive use of FRT by law enforcement exists in a sort of legal grey area on the federal level. As this is a relatively new technology, courts have not had the chance to rule on many cases concerning its use by law enforcement. With that in mind, the recent increase in the use of facial recognition technology by law enforcement agencies has resulted in a possible threat to rights guaranteed by the Constitution.

Of course, it should be acknowledged that private actors also have access to FRT, and its use by those entities prompts several unique legal questions distinct from its use by law enforcement. Furthermore, legislation or court decisions that bind law enforcement officials' use of FRT may not apply to private use. While this Note will mainly focus on the constitutional implications of FRT as used by law enforcement, private use of the technology will be addressed when it would be beneficial to the topic at hand.

To begin, facial recognition technology has often been used by law enforcement for general surveillance, with mixed results. For example, when FRT was used at the 2001 Super Bowl to screen for potential criminals and terrorists from the event, law enforcement was able to identify nineteen people with minor criminal records, although it was later admitted that the software only flagged petty criminals and resulted in some false positives.[1]

[1] Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOW STUFF WORKS, https://tinyurl.com/8vejjczc (last visited June 15, 2021); Richard Raysman & Peter Brown, *How Has Facial Recognition Impacted the Law?*, N.Y.L.J. (Feb. 9, 2016),

Unlike general surveillance, FRT has been extremely useful to law enforcement when investigating identification fraud, allowing officers to identify thousands of suspects in these cases, with particular success in cases of driver's license fraud. For example, New York has identified over 10,000 people with more than one driver's license with the help of FRT.[2] Similarly, New Jersey Department of Motor Vehicles officials have referred about 2,500 fraud cases to law enforcement since 2011.[3] Additionally, certain airports and the Transportation Security Agency (TSA) have begun to use FRT to assist airlines by having passengers board planes based on photographic images they take instead of utilizing boarding passes. These photos are then compared to a database of previously stored photographs from passports and visas on file with the U.S. Customs and Border Patrol.[4]

The software has also been useful in investigations when used in conjunction with other evidence. FRT has contributed to establishing probable cause for the arrest of suspected activity of assailants in videos of fights posted on the internet,[5] for passport fraud,[6] and in identity theft cases.[7] Facial recognition software was also used during the search for the suspects of the Boston Marathon Bombings in 2013, though the use of the software was ultimately unhelpful, due in part to the uncontrolled environment in which the surveillance images were taken, highlighting a major problem with FRT.[8] On the other hand, in a case that shows the true technological power of FRT, the NYPD arrested an individual after taking a surveillance image of the shooter from a nightclub and creating a full 3D image of him. The NYPD then ran it through a facial recognition software program.[9] Officers were then able to compare the resulting images and look for similar physical characteristics between them, enabling them to narrow the results

https://www.law.com/newyorklawjournal/almID/1202749127595/?slreturn=20210321124407.

[2] Jenni Bergal, *States Use Facial Recognition Technology to Address License Fraud*, GOVERNING MAG. (July 15, 2015), https://www.governing.com/archive/states-crack-down-on-drivers-license-fraud2.html.

[3] *Id.*

[4] *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.

[5] *In re* K.M., No. 2721 EDA 2014, 2015 WL 7354644, at *1 (Pa. Super. Ct. Nov. 20, 2015).

[6] United States v. Roberts-Rahim, No. 15-CR-243 (DLI), 2015 WL 6438674, at *3 (E.D.N.Y. Oct. 22, 2015).

[7] United States v. Green, No. 08-44, 2011 WL 1877299, at *2 (E.D. Pa. May 16, 2011).

[8] Brian Ross, *Boston Bombing Day 3: Dead-End Rumors Run Wild and a $1B System Fails*, ABC NEWS (Apr. 20, 2016), https://abcnews.go.com/US/boston-bombing-day-dead-end-rumors-run-wild/story?id=38375724; Sean Gallagher, *Why Facial Recognition Tech Failed in the Boston Bombing Manhunt*, ARS TECHNICA (May 7, 2013), https://arstechnica.com/information-technology/2013/05/why-facial-recognition-tech-failed-in-the-boston-bombing-manhunt/.

[9] Greg B. Smith, *Behind the Smoking Guns: Inside the NYPD's 21st Century Arsenal*, N.Y. DAILY NEWS (Aug. 20, 2017), http://creative.nydailynews.com/smokingguns.

down to a single image which was utilized in a photo array that was then shown to witnesses.[10]

I. WHAT IS FACIAL RECOGNITION TECHNOLOGY?

Reaching an exact definition of what facial recognition technology is can be more difficult than it sounds. This is a very new technology, and its capabilities are changing rapidly as new techniques and methodologies are developed. By the time this Note is published, there may be a brand-new revolution in FRT that changes the way we look at its usage. However, there are some basic principles that we can use to establish a baseline for what defines facial recognition technology.

A. Technical Background of Facial Recognition Technology

The most basic form of FRT is the process of taking a target's facial image, converting it into a "faceprint," and then comparing that template to pre-existing photographs of faces.[11] A faceprint is created through the measurement of certain facial features, called "nodal points," such as the distance between the eyes, the width of the nose, and the depth of the eye sockets.[12] There are approximately eighty nodal points on an individual face to draw from, and their measurements are then used to create a numerical form, which is called a faceprint.[13] Once a faceprint has been made, it serves as a kind of template which can be compared with other pre-existing photographs.[14] These pre-existing photographs could be drawn from several sources, including government records, social media sites, and employee registers.[15] Additionally, in recent years we have seen the debut of more advanced forms of FRT. Rather than relying on 2D images such as photographs, 3D Facial Recognition captures a real-time 3D representation of a target's face and uses distinctive features of the face to identify the target, such as the curves of the eye socket.[16]

Regardless of which specific kind of FRT is being used, each involves a six-step process in its usage.[17] The first step is Detection, in which the FRT system receives a subject to be scanned in the form of a photograph (2D) or a live picture (3D).[18] The second is Alignment, where a system detects a face and determines the head's position, size, and pose.[19] The third is Measurement, in which the system measures the curves of the

[10] *Id.*

[11] Bonsor & Johnson, *supra* note 1.

[12] *Id.*

[13] *Id.*

[14] Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, A.B.A. CRIM. JUST. MAG., Spring 2019.

[15] *Id.*

[16] Bonsor & Johnson, *supra* note 1.

[17] *Id.*

[18] *Id.*

[19] *Id.*

face on a sub-millimeter scale and creates a template.[20] The fourth is Representation, when the system translates the template into a unique numeric code that represents the features on a subject's face, the previously mentioned "faceprint."[21] The fifth is Matching, where the system compares the faceprint to those in the database to find a potential match.[22] The sixth step can take the form of either Verification or Identification, depending on the goal of the process. If Verification is the goal, the image of the subject is matched to only one image sourced from a larger database.[23] For example, an image taken of a subject may be matched to an image in U. S. Customs and Border Protection database registered to the subject, so that law enforcement offices can verify that the subject is who he says he is. On the other hand, if Identification is the goal, then the image is compared to all the images in a given database, with each potential match being scored.[24] For example, a police department may take an image of a subject and compare it to a database of mug shots to identify who the subject is.

B. The Problems With Facial Recognition Technology

While facial recognition technology is an amazing technological development, it is by no means perfect. As with any technology, there are always going to be limitations governing its capabilities. To begin, FRT works best when it is dealing with images that meet certain professional standards.[25] With that in mind, it should be clear that the accuracy of FRT decreases when working with photos sourced from uncontrolled environments or where there is no standardized photo to use for comparison.[26] Furthermore, FRT works best when dealing with a picture that is taken head-on and has no movement.[27] Additionally, because faces change over time, unlike fingerprints or DNA, software can trigger incorrect results by changes in hairstyle, facial hair, body weight, and the effects of aging.[28] There is also some research indicating that FRT algorithms may not be as accurate in reading the faces of certain demographics, in particular

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, CTR. FOR CATASTROPHE PREPAREDNESS & RESPONSE, N.Y.U. (July 22, 2009).

[26] *Id.*

[27] Naomi LaChance, *Facebook's Facial Recognition Software Is Different from the FBI's. Here's Why*, NPR (May 18, 2016), https://www.npr.org/sections/alltechconsidered/2016/05/18/477819617/facebooks-facial-recognition-software-is-different-from-the-fbis-heres-why; *see* David Nicklaus, *Cops' Start-Up Uses Facial Recognition to Improve Security*, ST. LOUIS POST-DISPATCH (Mar. 17, 2017), https://www.stltoday.com/business/columns/david-nicklaus/cops-startup-uses-facial-recognition-to-improve-security/article_41b7c4aa-708f-5806-961f-6f07d1184a23.html.

[28] Richard Raysman & Peter Brown, *How Has Facial Recognition Impacted the Law?*, N.Y.L.J. (Feb. 9, 2016).

African Americans.[29] This concerning trend will be fully addressed at a later point.

Of course, there are even more technical difficulties inherent in FRT. It should be remembered that the development of facial recognition technology is still a work in progress, and like any new technology, there are going to be technical glitches in its implementation. The accuracy of a FRT system could be negatively impacted by the environment, aging, different emotions, and dissimilarities between the compared images such as the image's lighting conditions, camera distance, background, head orientation and size of the face in the image.[30] Even a time delay between the collection and analysis of the image being analyzed and the image in the database that is being compared to can result in substantial error, even if only a year has passed between the time when the two images were taken.[31] Additionally, some databases are just too large for the simpler FRT systems to properly utilize or effectively search.[32]

Of course, these difficulties have not gone unnoticed. Former Senator Al Franken, once chairman of the US Senate Judiciary Subcommittee on Privacy, Technology, and the Law, said that he has "serious concerns about facial recognition technology and how it might shape the future of privacy."[33] In a letter to the founder of NameTag, a commercially available FRT app, Franken wrote that "[u]nlike other biometric identifiers such as iris scans and fingerprints, facial recognition is designed to operate at a distance, without the knowledge or consent of the person being identified. Individuals cannot reasonably prevent themselves from being identified by cameras that could be anywhere-on a lamppost across the street, attached to an unmanned aerial vehicle, or, now, integrated into the eyewear of a stranger."[34] In 2019, both Republican and Democratic members of the House Oversight and Reform Committee strongly condemned the use of the technology, with Committee chairman Elijah E. Cummings (D-MD.) saying "there's a lot of agreement" among American lawmakers from both sides of the aisle that the technology should be regulated.[35] He went on to say that the question was whether the use of FRT

[29] Clare Garvie & Jonathan Frankel, *Facial-Recognition Software Might Have a Racial Bias Problem*, THE ATLANTIC (Apr. 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/.

[30] Mostafa A. Farag, *Face Recognition in the Wild* (Dec. 2013) (MS thesis, University of Louisville) (available at https://ir.library.louisville.edu/etd/2278/).

[31] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-03-174, TECHNOLOGY ASSESSMENT: USING BIOMETRICS FOR BORDER SECURITY 183 (2002).

[32] *Id.* at 57.

[33] Press Release from Senator Al Franken, Senator for Minn.,Sen. Franken Raises Concerns about Facial Recognition App that Lets Strangers Secretly Identify People, (Feb. 5, 2014), http://www.franken.senate.gov/?p=press_release&id=2699 [https://perma.cc/5KAW-NJTN].

[34] *Id.*

[35] Drew Harwell, *Both Democrats and Republicans Blast Facial-Recognition Technology in a Rare Bipartisan Moment*, WASH. POST (May 22, 2019), https://www.washingtonpost.com/technology/2019/05/22/blasting-facial-recognition-technology-lawmakers-urge-regulation-before-it-gets-out-control/.

systems should be restricted while the technology is assessed or refined, or whether it should be banned outright.[36] The committee's ranking Republican, Rep. Jim Jordan (Ohio), compared the use of FRT to George Orwell's "1984" and called for a united front from both Republicans and Democrats in order to address this concern.[37] From these comments, it seems clear that American lawmakers are well aware of the danger that the use of FRT poses to the constitutional rights of their constituents, and we may see additional attempts to regulate its use as the technology continues to develop.

One of the most repeated critiques of facial recognition technology is how it often has difficulties when working with images of non-male, non-Caucasian faces. According to a 2019 National Institute of Standards and Technology study of 189 facial recognition algorithms from 99 developers, algorithms had higher rates of false positives for female faces relative to male faces, Asian and African American faces relative to those of Caucasian faces, and faces of African American women overall.[38] The Department of Homeland Security encountered similar problems when running their own tests featuring FRT, finding that a number of facial recognition systems took longer to process people with darker skin and were less accurate at identifying them.[39] Even FRT systems produced by tech giants such as Microsoft and Amazon stumbled over this hurdle.[40] When discussing FRT as a member of the aforementioned House Oversight and Reform Committee, Rep. Alexandria Ocasio-Cortez (D-N.Y.) summed up the problem: "we have a technology that was created and designed by one demographic, that is only mostly effective on that one demographic, and they're trying to sell it and impose it on the entirety of the country."[41] This is a deadly serious problem, as false positives in facial recognition have the potential to implicate innocent individuals and have already resulted in at

[36] *Id.*

[37] *Id.*

[38] Patrick Grother et al., Nat'l Inst. of Standards & Tech., *Face Recognition Vendor Test (FRVT)*, (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf [https://perma.cc/6586-UMD6]. These findings were based on analysis in one-to-one matching; a notable exception to the findings of bias was that some algorithms that were developed in Asian countries did not demonstrate the significant rates of false positives in one-to-one matching between Asian and Caucasian faces. One posited reason for this exception is that the foreign-developed algorithm utilized more diverse training data, suggesting that such data could produce more equitable outcomes in facial recognition algorithms.

[39] C. M. Cook, J. J. Howard, Y. B. Sirotin, J. L. Tipton & A. R. Vemury, *Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, IEEE TRANSACTIONS ON BIOMETRICS, BEHAV., & IDENTITY SCI., vol. 1, no. 1, pp. 32-41, (Jan. 2019), doi: 10.1109/TBIOM.2019.2897801.

[40] *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81:1–15 (2018). *See also* Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU (July 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

[41] CSPAN (@cspan), TWITTER (May 22, 2019, 9:32 AM), https://twitter.com/cspan/status/1131236422214672384.

least one conviction of an innocent man.[42] This problem becomes even more apparent when one takes into account the fact that half of American adults already have their faces in at least one law enforcement facial recognition database.[43] Taking this even further, one needs to remember the role that social media plays in this dilemma. Each picture uploaded onto social media only makes it easier for the average citizen to be identified by a facial recognition program. After all, consumers generally do not have the right to prevent their data, including pictures, from being harvested. The amount of data the average citizen uploads to their social media accounts would only make it easier for any actor utilizing FRT, including law enforcement agencies, to complete the digital puzzle.[44] Furthermore, there is even a class issue at play here, as those who can afford plastic surgery procedures would be able to alter their faces in a way that would make them unrecognizable to FRT, allowing the wealthy to escape some of the realities of a world where law enforcement bodies are armed with this technology.[45]

Compounding these problems is the increasingly rapid pace that technology has developed. Even within the last few years, we have seen leaps and bounds in the progression of facial recognition technology. For example, there are already billboards that change in response to passing customers through the use of simplistic facial-recognition software that can identify the customer's gender, age, and even their mood.[46] With this information, the billboard can offer real time personalized advertising.[47] This type of real time advertising will only be further improved as Kraft foods is developing a similar technology to be used in supermarkets.[48] Soon

[42] Sidney Fussel, *A Flawed Facial-Recognition System Sent This Man to Jail*, WIRED (June 24, 2020), https://www.wired.com/story/flawed-facial-recognition-system-sent-man-jail/ [https://perma.cc/BAK8-AT9W].

[43] Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIVACY & TECH. (2016), https://www.perpetuallineup.org [https://perma.cc/NSD5-38VS]. *See also* Lily Hay Newman, *Cops Have a Database of 117M Faces. You're Probably in It*, WIRED (Oct. 18, 2016), https://www.wired.com/2016/10/cops-database-117m-faces-youre-probably/.

[44] Matthew Wall, *Is Facial Recognition Tech Really a Threat to Privacy?,* BBC TECH. NEWS (June 19, 2015), http://www.bbc.com/news/technology-33199275 [https://perma.cc/F8WS-6UZL].

[45] Richa Singh et al., *Plastic Surgery: A New Dimension to Face Recognition*, 5 IEEE TRANSACTIONS ON INFO. FORENSICS & SEC. 441 (2010); Xin Liu, Shiguang Shan & Xilin Chen, *Face Recognition After Plastic Surgery: A Comprehensive Study*, in 2 Computer Vision – ACCV 2012 at 565 (2013).

[46] Heather Fletcher, *Facial Recognition: Ads Target Consumers for You*, TARGET MKTG. (Oct. 5, 2015), http://www.targetmarketingmag.com/article/facial-recognition-ads-target-consumers/all/ [https://perma.cc/3G4N-T7E2].

[47] *Id.*

[48] *Compare* Kashmir Hill, *Kraft To Use Facial Recognition Technology To Give You Macaroni Recipes*, FORBES (Sept. 1, 2011), http://www.forbes.com/sites/kashmirhill/2011/09/01/kraft-to-use-facial-recognition-technology-to-give-you-macaroni-recipes/#3e59f86a301c [https://perma.cc/KQR9-TDEW], *with* Clare McDonald, *Almost 30% of Retailers Use Facial Recognition Technology to Track Consumers in Store*, COMPUTERWEEKLY.COM (Sept. 15, 2015), http://www.computerweekly.com/news/4500253499/Almost-30-of-retailers-use-facial-recognition-technology-to-track-consumers-in-store [https://perma.cc/Y75H-5NEJ], *and* Laura Northrup, *This Freezer Case Knows When You're Frowning At The Bagel Bites*, CONSUMERIST (Jan. 19, 2016), https://consumerist.com/2016/01/19/this-

enough, facial recognition could be made even easier through further technical improvements in devices as innocuous as cell phones. The President's Council on Science and Technology expressed similar concerns in a 2014 report:

> It is foreseeable, perhaps inevitable, that these capabilities will be present in every cell phone and security surveillance camera, or every wearable computer device. (Imagine the process of negotiating the price for a car, or negotiating an international trade agreement, when every participant's Google Glass (or security camera or TV camera) is able to monitor and interpret the autonomic physiological state of every other participant, in real time.) It is unforeseeable what other unexpected information also lies in signals from the same sensors. Once they enter the digital world, born-analog data can be fused and mined along with born-digital data. For example, facial-recognition algorithms, which might be error-prone in isolation, may yield nearly perfect identity tracking when they can be combined with born-digital data from cell phones (including unintended emanations), point-of-sale transactions, RFID tags, and so forth; and also with other born-analog data such as vehicle tracking (e.g., from overhead drones) and automated license-plate reading.[49]

While these examples all primarily deal with facial recognition technology in the hands of commercial actors, they serve to demonstrate how the technology is continuously improving. In just a few years, the facial recognition systems being used by law enforcement may be far more advanced than what we are seeing now.

Similarly, the simple fact is that we often do not know when facial recognition technology is being deployed by law enforcement or other government actors. Moreover, we do not know, and might never know, how that data is processed and used to discover new and potentially damaging information about us. With all these unknowns, we might very well wind up existing in a world where we are subject to substantial and pervasive harms due to facial recognition, including censorship, control and inhibition of our actions, and the mental stress of knowing that we might be under surveillance at any time.[50]

Another problem facing FRT is how subjectively it can be applied by law enforcement agencies. During the 2016 protests for the death of Freddie Gray while he was in police custody, the Baltimore Police Department used social media to track specific protestors and used facial recognition software to identify those with outstanding warrants.[51] This

freezer-case-knows-when-youre-frowning-at-the-bagel-bites/ [https://perma.cc/H7C3-MSA9].

[49] PRESIDENT'S COUNSEL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 23 (May 2014), http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [https://perma.cc/LQ8D-97V2].

[50] Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 434-35 (2013).

[51] 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-

demonstrates an alarming measure of subjectivity, as Baltimore police were essentially choosing which protestors were subjected to an advanced form of surveillance and which were not. Tellingly, this use of FRT drew a significant outcry from those concerned with preserving the civil liberties of the protestors.[52]

Finally, there have been concerns that extensive use of FRT will only lead to further discrimination among law enforcement agencies. Depending on the algorithm in use, FRT could be able to incorporate easily discriminable characteristics such as age, race or gender, social status, religion and even immigration status.[53] This could lead to the use of FRT in predictive policing algorithms and would place several constitutional rights in danger as a result.

C. Establishing a Legal Precedent

As facial recognition technology is a relatively new technology, it has barely been brought before the courts. However, a legal precedent already exists for invasive uses of FRT. Courts at nearly every level have heard cases involving the invasive use of surveillance technologies such as wire taps, surveillance cameras, thermal imaging, and more. As will be discussed in detail later in the Note, the improper use of these kinds of technologies can threaten the constitutional rights of citizens placed under surveillance. Therefore, we can use these findings as a precedent when it comes to reviewing uses of FRT.

II. WHAT RIGHTS ARE BEING IMPLICATED THROUGH THE ABUSE OF FRT?

Of course, it is not inherently wrong for law enforcement agencies to make use of facial recognition technology, as long as they do not threaten the rights of individual citizens. However, the question must be asked, what constitutional rights are being threatened when FRT is improperly used by law enforcement? Looking at past Supreme Court decisions and modern

20161017-story.html [https://perma.cc/UAW3-543A]; *see also* Russell Brandon, *Facebook, Twitter, and Instagram Surveillance Tool Was Used to Arrest Baltimore Protestors*, THE VERGE (Oct. 11, 2016), https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api [https://perma.cc/Y5V4-BYEF].

[52] Stephen Babcock, *Report Raises Troubling Questions About Facial Recognitmmion Technology in Maryland*, TECHNICAL.LY (Oct. 19, 2016); 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 [https://perma.cc/UAW3-543A]; ACLU Letter to Principal Deputy Assistant Attorney General Vanita Gupta, Leadership Conference (Oct. 18, 2016) (available at https://tinyurl.com/3yawjwv7).

[53] Sharon Nakar & Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 B.U. J. SCI. & TECH. L. 88, 119 (2017).

legal discourse, it becomes clear that an improper use of FRT could result in threats to the right to privacy, the right to anonymity, and the right to freely associate.

A. The Right to Privacy

While the right to privacy is not explicitly guaranteed by the Constitution in the manner of other protected rights, the Constitution does forbid certain trespasses against individual privacy. In *Katz v. United States*, the Supreme Court found that the Fourth Amendment guaranteed that what a citizen "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[54] However, the Court also warned that the Fourth Amendment should not be interpreted as a general protection of the right to privacy.[55] The Court makes it very clear that legislation concerning the protection of general policy should be left to individual states.[56] Instead, the Court has written that individual aspects of privacy are protected in various provisions of the Constitution. For example, the Third Amendment's ban on the quartering of soldiers in American households could be read as a protection of a specific aspect of privacy.[57] Additionally, the Fifth Amendment protects the rights of citizens to maintain "a private enclave where he may maintain a private life."[58] Finally, the First Amendment protects the right to privacy while freely associating.[59]

Katz v. United States also serves as a useful source for the Supreme Court's reasonable expectation of privacy test. In order to determine whether or not a person has a reasonable expectation of privacy, the Court considers (1) whether the person exhibited an actual, subjective expectation of privacy and (2) whether that expectation is one that society recognizes as reasonable.[60] While the Court has not yet applied this test to the use of facial recognition, it has applied it to other forms of electronic surveillance. In *Carpenter v. United States*, the Court ruled that a person's reasonable expectation of privacy included the records of historical cell phone data which could reveal the person's physical location or movements, and that a person's Fourth Amendment rights were violated when the government received historical cell phone data from cell phone companies without first obtaining a search warrant.[61] While there are obvious distinctions between historical cell phone data and FRT, both technologies can essentially be used to monitor a person's locations. With this in mind, we can apply FRT to the *Carpenter* Court's goal to work towards the preservation of privacy

[54] Katz v. United States, 389 U.S. 347, 351 (1967).

[55] *Id.* at 350.

[56] *Id.* at 350-351.

[57] *Id.* at 350 n.5.

[58] Tehan v. Shott, 382 U.S. 406, 416 (1966).

[59] NAACP v. Ala. ex rel. Patterson, 357 U.S. 449, 462 (1958). The right of free association will be discussed in more depth later in this Note.

[60] *Katz*, 389 U.S. at 361.

[61] Carpenter v. United States, 138 S. Ct. 2206 (2018).

in the face of technologies that enhance the government's ability to encroach upon on the private lives of citizens.[62]

When discussing the necessity of privacy in the face of unwarranted and public surveillance, one of the most important cases to consider is 2004's *Illinois v. Lidster*.[63] In this case, the Supreme Court was questioning the legality of setting up a traffic checkpoint in order to identify the suspect in a severe hit and run accident.[64] Lidster argued that preserving the privacy of the citizens who were subjected to police surveillance was more important than catching the culprit, but the Court found that the kind of surveillance that the police conducted was permitted under the Fourth Amendment.[65] Judge Posner would later write that "*Lidster* is important because it divorces searching from suspicion. It allows surveillance that invades liberty and privacy to be conducted because of the importance of the information sought, even if it is not sought for use in a potential criminal proceeding against the people actually under surveillance."[66] To see how this treatment of privacy has changed with the introduction of new technologies, we can look to *Kyllo v. United States,* where the court found that the use of a thermal imaging device to search for radiating heat that was assumed to be associated with marijuana cultivation, and to then obtain a search warrant based on that radiating heat was an unlawful search.[67] In defining what a "search" actually consisted of, the *Kyllo* Court expanded on the sentiment first expressed in *Katz*, stating that "[a]'search' does not occur -- even when its object is a house explicitly protected by the Fourth Amendment -- unless the individual manifested a subjective expectation of privacy in the searched object, and society is willing to recognize that expectation as reasonable."[68]

As was previously stated, we have yet to see any major examples of facial recognition technology in the courts. However, in *People v. Johnson*, the California Court of Appeals suggested that in the use of FRT, a database search merely provides law enforcement with an investigative tool, not evidence of guilt, and that the reason a person came to be suspected of a crime is not a relevant issue to be discussed at trial.[69] The court then went on to compare a positive result from FRT to an eyewitness investigation, using the following analogy:

> For example, assume police are investigating a robbery. The victim identifies "Joey" as the perpetrator. The means by which "Joey" becomes the focus of the investigation—the eyewitness identification—is relevant because that

[62] Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

[63] 540 U.S. 419 (2004).

[64] *Id.* at 422.

[65] *Id.*

[66] RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 91 (2006).

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

[68] *Id.* at 29.

[69] People v. Johnson, 139 Cal. App. 4th 1135, 1150 (2006).

> identification is itself evidence of guilt. Suppose instead that a surveillance camera captures the robbery on tape. Police use facial recognition software to check the robber's facial features against driver's license photographs. When the computer indicates a match with "Joey," officers obtain his name and address from DMV records, then go to his house and interview him. In the course of the interview, "Joey" confesses. Whether facial recognition software is discerning and accurate enough to select the perpetrator, or whether it declared a match involving many different people who resembled "Joey," or how many driver's license photographs were searched by the software is immaterial: what matters is the subsequent confirmatory investigation.[70]

Finally, U.S. privacy law has developed even outside of Supreme Court cases. In fact, Congress has passed several pieces of legislation over the years designed to protect the privacy of American citizens.[71] Going forward, unreasonable uses of facial recognition technology by the FBI may be stopped by a number of these statutes. When discussing the use of facial recognition technology by the FBI, their actions are most likely governed by a number of these statutes, such as the E-Government Act of 2002[72] and the Privacy Act of 1974.[73] In accordance with these laws, the FBI must conduct Privacy Impact Assessments (PIA) for its facial recognition programs.[74] Furthermore, the FBI is required to employ the Fair

[70] People v. Johnson, 139 Cal. App. 4th 1135, 1150-1151 (2006).

[71] DANIEL J. SOLOVE ET AL., PRIVACY, INFORMATION, AND TECHNOLOGY 31 (2006) (Listing the Privacy Act of 1974, 5 U.S.C. § 552a (2012)); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2012); Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (2012); Right to Financial Privacy Act of 1978, 12 U.S.C.§§3401-3422 (2012); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2012); Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a (2012); Employee Polygraph Protection Act of 1988, 22 U.S.C.§§2001-2009 (2012); Electronic Communications Privacy Act of 1986, 18 U.S.C.§§2510-2522 (2012); Cable Communications Policy Act of 1984 47, U.S.C. § 551 (2012); Privacy Protection Act of 1980, 42 U.S.C. ch. 21A (2012); Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. ch. 36 (2012); Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2012); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2012); Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No.104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C. (2012)); Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 (2012); Children's Online Privacy Protection Act of 1998, 15 U.S.C.§§3501-6506 (2012); Gramm-Leach-Bliley Act of 1999, Pub. L. No.106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12 U.S.C. (2012)); CAN-SPAM Act of 2003 15 U.S.C. §§7701-7713 (2012); Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended in scattered sections of 15 U.S.C. (2012)); Video Voyeurism Prevention Act of 2004 18 U.S.C. § 1801 (2012).

[72] The E-Government Act of 2002, 44 U.S.C. § 101 ("The purposes of this subchapter are to … ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to (A) privacy and confidentiality, including section 552a of title 5 [Privacy Act of 1974].").

[73] The Privacy Act of 1974, *supra* note 71.

[74] *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY (2016) at 38,

Information Practices Principles when utilizing its facial recognition programs.[75] Even with these statutes in effect, the ever-changing nature of FRT may result in Congress needing to pass new legislation that specifically protects citizens' privacy from abuses of the technology.

B. The Right to Anonymity

Anonymity is best defined as "the freedom from being identified and tracked by name while going through the motions of daily life, including physical movement in private and public spaces, the transaction of business online, and the maintenance of personal and professional relationships, habits, and beliefs - however unpopular or repugnant."[76] While the right to anonymity is not explicitly guaranteed by the Constitution, the Supreme Court has a history of defending it.

The right to anonymity protects citizens from the government learning about, as the Court in *United States v. Jones* put it:

> A person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations…. [Tracking of individuals will disclose] trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[77]

In that very same case, Justice Flaum expressed concerns that a government with the capability to easily track and monitor its citizens' personal lives would "alter the relationship between citizen and government in a way that is inimical to democratic society."[78]

While the Supreme Court has indeed defended anonymity in the past, its definitive attitude towards anonymity as a general constitutional right is hazy at best, and there remain unanswered questions regarding where and when anonymity is constitutionally protected. In one of the first Supreme Court cases dealing with anonymity, *People of New York ex rel. Bryant v. Zimmerman,* the Court held that a Klu Klux Klan membership list

http://www.gao.gov/assets/680/677098.pdf [https://perma.cc/ZA46-B3CG] [hereinafter GOV'T ACCOUNTABILITY OFFICE, PRIVACY AND ACCURACY].

[75] *See, e.g.*, U.S. DEP'T. HOMELAND SEC., MEMORANDUM NO. 2008-01, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-01_0.pdf.

[76] Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 413 (2014) (citing DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008)).

[77] United States v. Jones, 565 U.S. 400, 415 (2012) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

[78] *Id.* at 416 (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

was not protected from disclosure to the state under a New York statute.[79] The Court reasoned that it was a rightful exertion of a state's police power to demand the Klan's membership list, and that states have the right to be informed about associations within their purview, so that the associations in question might be deterred from violations of individual rights.[80] However, this ruling was later distinguished by *NAACP v. Alabama ex rel. Patterson*, in which the Supreme Court held that Alabama had not demonstrated sufficient justification for requiring the disclosure of an NAACP membership list.[81] The Court explained that unlike the Klu Klux Klan in *People of New York*, the NAACP had attempted to comply with state statutes regarding associations, and its activities did not historically consist of violations of individual rights, namely the practice of unlawful intimidation and violence against fellow citizens.[82]

Up until now, this Note has discussed anonymity within the context of freedom of association. However, in 1960's *Talley v. California,* the Supreme Court established a protection on anonymous speech that was distinct from the protection on free association.[83] In overturning a Los Angeles ordinance that required persons distributing handbills to print their name and address on the cover of the handbill, the *Talley* Court tied their protection of anonymous speech to the First Amendment's guarantee of freedom of expression, writing that anonymity is essential to enabling expression when there is a fear of retaliation.[84] The Court ruled that laws which enable that fear of retaliation cannot be allowed to stand.[85] 35 years later, the Supreme Court would again rule in favor of anonymity in 1995's *McIntyre v. Ohio Elections Commission*, where the Court protected the distribution of anonymous campaign leaflets.[86] In an interesting evolution of its logic from its previous rulings, the Court wrote that the right to remain anonymous when writing any kind of literature is protected by the First Amendment.[87] In essence, the Court decided that no matter the reason, someone may choose to remain anonymous in exercising their freedom of expression, be it for political or non-political reasons, that person's right to anonymity is constitutionally guaranteed.

Seven years later, the Supreme Court would once again address the topic of anonymity in 2002's *Watchtower Bible v. Village of Stratton*, in which Jehovah's Witnesses challenged the village of Stratton's ordinance that required anyone engaged in door-to-door advocacy to register with the mayor's office and obtain a permit, with an applicant's name and address being disclosed in the process.[88] The Court found the ordinance to be

[79] People of New York ex rel. Bryant v. Zimmerman, 278 U.S. 63, 77 (1928).
[80] *Id.* at 65.
[81] NAACP v. Ala. ex rel. Patterson, 357 U.S. 449, 462 (1958).
[82] *Id.* at 465.
[83] Talley v. California, 362 U.S. 60 (1960).
[84] *Id.* at 64, 65.
[85] *Id.*
[86] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).
[87] *Id.* at 342.
[88] Watchtower Bible v. Vill. of Stratton, 536 U.S. 150, 153 (2002).

excessively restrictive and that what it suggested was "offensive . . . to the very notion of a free society—that in the context of everyday public discourse a citizen must first inform the government of her desire to speak to her neighbors and then obtain a permit to do so."[89] However, what truly makes *Watchtower Bible* remarkable is how the Court defines anonymity. The Court maintained that even though the door-to-door petitioners showed their faces to those who answered the door, they still maintained anonymity as they did not directly reveal their identities.[90] This firmly established that an individual does not need to be totally concealed for their anonymity to be protected by the First Amendment.

In 2010, the Supreme Court once again dealt with the issue of anonymity, questioning whether the disclosure of referendum petitions violated the First Amendment in *Doe v. Reed*.[91] This time, the Court ruled against anonymity by upholding the disclosure requirement, basing its decision on the relationship between the "state's interest in preserving the integrity of the electoral process" and the disclosure requirement.[92] From this logic, it can be concluded that the Court is suggesting that a sufficiently important government interest can supersede a citizen's right to anonymity. However, the Court did note that the outcome might have been different if the petitioner in *Doe* had demonstrated that there was "a reasonable probability that the compelled disclosure . . . will subject them to threats, harassment, or reprisals from either Government officials or private parties,"[93] which would effectively reconcile this decision with the Court's previous ruling in *Talley v. California*.

Taking these Supreme Court decisions into account, there are five questions to answer when it comes to the question of anonymity. It must be determined (1) whether the First Amendment protects only core political speech; (2) whether broad disclosure requirements are constitutional; (3) what kinds of compelling state interests might overcome First Amendment protection; (4) whether election law cases are exceptions to or illustrative of the required balance between state interests and anonymity; and (5) how much of a showing of retaliation, if any, is necessary to establish the First Amendment right.[94]

Based on our review of the Court's decisions, it would be safe to frame *Talley*, *McIntyre*, and *Watchtower Bible* as the primary sources of a right to anonymity that can be derived from the First Amendment. The first question we need to answer is how broadly the right to anonymous speech extends past political speech. At this point, the Court has made it very clear that anonymous political speech is protected, but are other kinds of anonymous speech equally deserving of First Amendment protection?

[89] Watchtower Bible v. Vill. of Stratton, 536 U.S. 150, 165-166 (2002).

[90] *Id.* at 167.

[91] Doe v. Reed, 561 U.S. 186 (2010).

[92] *Id.* at 197.

[93] *Id.* at 200 (quoting Buckley v. Valeo, 424 U.S. 1, 74 (1976)).

[94] Margot E. Kaminski, *Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 815, 843 (2013).

There is not a definitive answer to this question, as the Court has indicated that any potential restriction on anonymous speech must meet a balancing test between the value of the anonymous speech and state interests. The balancing test for protection of anonymity weighs the value of the speech being protected against the nature of the state interest being propagated. The first point of division between commentators is whether the speech must be "core" First Amendment speech to be protected.[95] This leaves open the question of whether nonpolitical anonymous speech is protected by the First Amendment.

The other half of the balancing equation concerns what constitutes a sufficiently compelling state interest. Once again, commentators are divided, but largely point to the regulation of fraud, false advertising, and libel as sufficient state interests for the regulation of anonymous speech, so long as the statute does not go too far.[96] The state interest alone is not enough, however; others point out that the regulation must not overstep in its restrictions and it must be narrowly tailored.[97] As such, commentators disagree over whether a compelling state interest might allow regulation of any and all anonymous speech.

The biggest challenge facing the protection of anonymous speech is the body of election law cases such as the previously discussed *Doe*. Some distinguish these cases as specific to the electoral context, arguing that there is a long American tradition of anonymous speech that deserves to be protected, just as transparent political proceedings deserve to be protected.[98] This brings us to a final question regarding existing case law: whether an anonymous speaker must show a danger of retaliation or if a court may conclude without evidence that the fear of retaliation is suppressing speech that would otherwise not be made anonymously. In *NAACP*, the Court pointed out that the NAACP made a strong concrete showing that its members would experience retaliation if their names were made public.[99] In *Doe*, the Court explained that the facial challenge failed because the petitioner had failed to make a showing of retaliation for all disclosures.[100] However, the Court did not seem concerned with the danger of retaliation

[95] A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J. L. & COM. 395, at 427 (1996) ("Doctrinal discussions of permissible restrictions on the freedom of speech commonly divide the discussion into 'political' and 'non-political' speech, and the sketch which follows adopts this convention."); Lyrissa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 NOTRE DAME L. REV. 1537, 1541 (2007) ("Laws requiring disclosure in the context of political speech, on the other hand, should be (if anything) even more difficult to justify; in the context of commercial speech, however, the assumption of a rational, critical audience may give way to more paternalistic assumptions and thus make it relatively easy for the state to compel disclosure.").

[96] *See, e.g., Talley*, 362 U.S. at 66.

[97] Victoria Smith Ekstrand, *Unmasking Jane and John Doe: Online Anonymity and the First Amendment*, 8 COMM.. L. & POL'Y 405, 411 (2003).

[98] Chesa Boudin, *Publius and the Petition: Doe v. Reed and the History of Anonymous Speech*, 120 YALE L.J. 2140, 2164 (2011).

[99] NAACP v. Ala. ex rel. Patterson, 357 U.S. 449, 463 (1958).

[100] Doe v. Reed, 561 U.S. 186, 201 (2010).

in both *Talley* and *McIntyre*, further complicating any potential answer to this question.

These questions simultaneously become both simpler and more complex when Facial Recognition Technology is brought to bear. In many cases where FRT is being used by law enforcement, political speech is not being used. A burglar caught on home security footage is certainly not expressing political speech. However, this issue becomes more complicated when one considers the use of FRT during protests. As was discussed earlier in this Note, police departments have applied FRT to protestors in an effort to identify protestors with outstanding warrants. One could easily argue that this would qualify as an existing threat of retaliation that could serve to stifle anonymous political speech.

C. The Right to Freely Associate

While the Freedom of Association may not be explicitly listed in the Constitution, it has long been recognized as an essential First Amendment freedom since 1958, with the aforementioned *NAACP v. Alabama ex rel. Patterson* establishing the right of people to associate for expressive purposes, oftentimes political ones.[101] This case's ruling prompted First Amendment scholar Thomas I. Emerson to write that "freedom of association in the United States has assumed increasing significance as modern society has developed, and problems of associational rights have given rise to new and perplexing constitutional issues."[102] This quote rings especially true today, and the impact that facial recognition technology may have on this fundamental right deserves to be fully explored.

Although freedom of association may be defended by the Constitution, there is a certain standard that must be met before the Supreme Court acknowledges that a constitutional right has been violated. For example, the Court has decided in the past that simple surveillance of public gatherings by law enforcement does not constitute a violation of the First Amendment. In *Laird v. Tatum* a group of protestors claimed that their rights were being violated when the Army conducted surveillance of their lawful and peaceful protest, alleging that their constitutional rights were being violated.[103] The Army justified this surveillance by characterizing it as gathering by lawful means and maintaining and using in their intelligence activities, information relating to potential or actual civil disturbances or street demonstrations.[104] The Supreme Court took issue with the specifics of the civilians' claim, writing that the claim depended on a belief that this surveillance produced a chilling effect on the exercise of First Amendment rights.[105] As a result, the Court held that mere allegations of a chilling effect

[101] NAACP v. Ala. ex rel. Patterson, 357 U.S. 449, 462 (1958).

[102] Thomas I Emerson, *Freedom of Association and Freedom of Expression,* 74 YALE L. J. 1, 35 (1964).

[103] Laird v. Tatum, 408 U.S. 1 (1972).

[104] *Id.*

[105] *Id.* at 13.

were not sufficient for proper standing, as opposed to a claim of actual or threatened harm.[106]

On the other hand, specific and targeted surveillance of a group has been shown to rise to the level of an actual First Amendment violation. In *Hassan v. New York* the Third Circuit heard a case where Muslim citizens alleged that they were being subjected to a discriminatory surveillance program at the hands of the NYPD.[107] The Third Circuit found that these citizens had standing in court to sue as discriminatory classification constituted a harm to their rights to religious liberty and equal protection.[108]

III. WHAT CAN BE DONE?

While the abuse of facial recognition technology by law enforcement officials can certainly lead to the constitutional rights being put in danger, that does not mean that violations of these rights are the inevitable result of the adoption of FRT. On the contrary, FRT can be of great use to law enforcement, much like any other technological development. However, it must be used in a way that the constitutional rights of citizens are not threatened as a result.

A. Maintain the Distinction Between Searching and Suspicion

One of the most challenging aspects of discussing the use of facial recognition technology by law enforcement is defining what exactly makes its use problematic, as opposed to more conventional means of recognition. To put it another way, if a police officer managed to recognize a wanted criminal in a photo of a busy street, no one would say that the criminal's rights have been violated. Keeping this in mind, what would be the difference if facial recognition technology managed to recognize a wanted criminal in a photo of a busy street?

One of the main differences that sets apart the use of facial recognition technology is the systemic nature of the search. When a police officer recognizes someone in the crowd, that is the kind of law enforcement behavior that we as a society should want to encourage. After all, we want law enforcement officers to be able to recognize faces, whether that means being able to recognize wanted criminals or simply being familiar with the inhabitants of the communities that they police. However, this dynamic changes with the introduction of facial recognition technology. The act of recognizing someone in a crowd has been systemically altered through this technology and that recognition may now rise to a point where constitutional rights are being threatened.

Another aspect that sets facial recognition technology apart is how some uses of this technology can be inherently invasive. The Court in *U.*

[106] Laird v. Tatum, 408 U.S. 1, 16 (1972).
[107] Hassan v. City of N.Y., 804 F.3d 277 (3d Cir. 2015).
[108] *Id.* at 290 n.2.

S. v. Jones dealt with the use of a similar technology, GPS tracking, and its use by law enforcement.[109] In that case, federal agents placed a GPS tracking device on the undercarriage of a car registered to a suspect's wife and tracked its movements for nearly a month, outside of the date range granted by the warrant, before an arrest was finally made.[110] The court made it very clear that the planting of this GPS tracker was a "physical occupation" of private property on behalf of the government, and that any information obtained as a result of the tracker should be treated as the result of a warrantless search as defined by the Fourth Amendment.[111] The government also contended that it had not violated any kind of reasonable expectation of privacy, as government agents only accessed the exterior of the jeep in planting the surveillance device and only recorded its movements along public roads.[112] In turn, the Court rejected the idea that a citizen's Fourth Amendment rights might suddenly disappear when they no longer have a reasonable expectation of privacy.[113]

B. Adapt and Improve Existing FRT Related Guidelines

As has been brought up multiple times throughout this Note, facial recognition technology is a relatively new arrival on the legal scene, and as a result, there are little to no laws and organizational guidelines governing its use on a national scale. However, there have been some developments on the state level. Illinois and Texas have both adopted the Illinois Biometric Information Privacy Act, which focuses on governing the use of biometrics, including facial recognition technology. This Act requires "(i) notice and opt out provisions; (ii) limitations on the commercial use of FRT data acquired; (iii) destruction of the data after three years in Illinois and only one year in Texas; (iv) industry standards of care must be employed to protect private data."[114] It is unlikely that Illinois will be the last state to pass such a law, as Washington and California have both proposed similar pieces of legislation.[115]

Additionally, lawmakers may wish to take a page from the private sector's book. On June 22, 2016, the US National Telecommunications and Information Administration (NTIA), an organization under the umbrella of the US Department of Commerce, released a set of best practices for the commercial use of FRT. The NTIA's best practices are based on the widely accepted Fair Information Practice Principles (FIPPs) framework and according to the NTIA, the best practices reflect an evolving and flexible

[109] United States v. Jones, 565 U.S. 400 (2012).

[110] *Id.* at 403.

[111] *Id.* at 404.

[112] *Id.* at 406.

[113] *Id.* at 406.

[114] 740 ILL. COMP. STAT. 14/ (2008).

[115] Sam Castic, Shea G. Leitch, Aravind Swaminathan & Antony P. Kim, *Biometrics: A Fingerprint for Privacy Compliance, Part I*, , ORRICK TRUST ANCHOR (Mar. 4, 2016), http://blogs.orrick.com/trustanchor/2016/03/04/biometrics-a-fingerprint-for-privacy-compliance-part-i/ [https://perma.cc/HF35-DPAJ].

approach to FRT uses. These principles encourage covered entities to publish policies or disclosures describing their collection, storage, and use of facial template data.[116] This includes reasonably foreseeable purposes for collecting and sharing the data; data retention and de-identification practices; and individual's ability to review, correct, or delete facial template data.[117]

Covered entities should also develop internal facial template data management practices that consider: whether the enrollment is voluntary or involuntary; sensitivity of non-facial recognition data also being captured and stored; how they store and use the data; whether the entity will use facial template data to determine a person's eligibility for, or access to, employment, healthcare, financial products or services, credit, housing, or insurance; risks and harms to the individual; and reasonable consumer expectations regarding the data's use.[118] Finally, entities should give individuals the ability to control the sharing of their facial template data with unaffiliated third parties; implement reasonable safeguards to protect facial template data; take reasonable steps to maintain the data's integrity and accuracy; and establish processes for individuals to contact them about the use of their facial template data.[119]

These principles were not universally adopted, with a number of entities withdrawing from the process.[120] Despite this, these principles could serve as an excellent starting point for drafting more in-depth legislation that would outline the boundaries of the use of FRT by law enforcement agencies. In another example, the International Biometrics & Identification Association released the "Privacy Best Practice Recommendations for Commercial Biometric Use" in August 2014.[121] The main points of these recommendations were as follows: (1) FRT operators should obtain and publish privacy policies.[122] The privacy policy should specify the purposes of the data captured, whether any non-biometric data is also collected that can be used to associate with the biometric data, and how long the data will be maintained.[123] (2) Businesses should provide notice that they are implementing these technologies.[124] (3) Firms should

[116] NAT'L TELECOMM. INFO. & ADMIN., *Privacy Best Practice Recommendations for Commercial Facial Recognition Use* (June 17, 2016), https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf [https://perma.cc/N7XB-XE3K].

[117] *Id.* at 2.

[118] *Id.* at 2-3.

[119] *Id.* at 3.

[120] Jennifer Lynch, *EFF and Eight Other Privacy Organizations Back Out of NTIA Face Recognition Multi-Stakeholder Process*, ELEC. FRONTIER FOUND. (June 16, 2015), https://www.eff.org/deeplinks/2015/06/eff-and-eight-other-privacy-organizations-back-out-ntia-face-recognition-multi [https://perma.cc/Y56H-VXXF].

[121] *See* INT'L BIOMETRICS & IDENTIFICATION ASS'N, *Privacy Best Practice Recommendations for Commercial Biometric Use* (Aug. 2014), https://www.ntia.doc.gov/files/ntia/publications/ibia_privacy_best_practice_recommendations_8_18_14.pdf.

[122] *Id.* at 2.

[123] *Id.*

[124] *Id.* at 1.

have sufficient cybersecurity to protect against any potential malfeasance.[125] And (4) firms should provide the consumer with a mechanism to retrieve their own data upon request, and have a method for implementing any necessary corrections to the data.[126]

The US Federal Trade Commission issued its own report regarding the privacy implications of FRT.[127] The Commission recommended that companies using FRT design their services with privacy and security in mind through the implementation of certain principles:

> 1. Privacy by Design: Companies should build in privacy at every stage of product development.
> 2. Simplified Consumer Choice: For practices that are not consistent with the context of a transaction or a consumer's relationship with a business, companies should provide consumers with choices at a relevant time and context.
> 3. Transparency: Companies should make information collection and use practices transparent.[128]

It may also be wise to look beyond the United States' borders for examples on how regulation of facial recognition technology might be accomplished. In the European Union, regulation of FRT falls under general regulations that apply to most forms of data collection. Any organization, public or private, that collects data from European citizens must respect their rights as data owners under EU law.[129] The most recent version of these rights can be sourced from an agreement reached by the European Parliament, the Council, and the Commission regarding data protection.[130] These data owner rights include the right to rectification and "to be forgotten,"[131] the right to consent to the processing of personal data,[132] easier access to personal data,[133] the right to object to uses of the data, including to the use of personal data for the purposes of profiling,[134] and the right to data portability from one service provider to another.[135]

It should be apparent by this point that we are a long way off from any sort of consensus regarding how the implementation of FRT should be governed. However, there are still certain principles that echo throughout

[125] *Id.* at 2.

[126] *Id.* at 3.

[127] FED. TRADE COMM'N, *Facing Facts: Best Practices for Common Uses of Facial Recognition Technology* (Oct. 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

[128] *Id.* at 2.

[129] *Protection of Personal Data*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/ [https://perma.cc/5BM3-LJP3] (last visited Nov. 11, 2016) ("Everyone has the right to the protection of personal data.").

[130] Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU); Council Directive 2016/680, 2016 O.J. (L 119) 89 (EU); Council Directive 2016/681, 2016 O.J. (L 119) 132 (EU).

[131] Council Regulation 2016/679, 2016 O.J. (L 119) 65 (EU).

[132] Council Regulation 2016/679, 2016 O.J. (L 119) 32 (EU).

[133] Council Regulation 2016/679, 2016 O.J. (L 119) 39 (EU).

[134] Council Regulation 2016/679, 2016 O.J. (L 119) 60 (EU).

[135] Council Regulation 2016/679, 2016 O.J. (L 119) 68 (EU).

these various guidelines and regulations. For example, each one emphasizes the importance of maintaining a citizen's privacy when subjecting them to facial recognition technology. Despite their differences, these various guidelines can help serve as a starting point for drafting further legislation on a national scale.

C. Require a Demonstration of an Appropriate Need

One of the main methods that could be used to limit abuses of FRT databases would be to treat them the same as other police databases that contain substantial amounts of personal and private information, so that legislation such as the Justice For All Act of 2004 that limited access to the national Combined DNA Index System (CODIS) database and provided stiff penalties for misuse[136] would apply to these databases as well. Law enforcement officers should show that they have some sort of special need before being granted such substantial access to a citizen's personal data. We have seen the courts come to similar conclusions in the past, in cases such as *Carpenter* and *Jones*.

An additional principle that might be incorporated in the use of FRT by law enforcement would be an obligation to technically improve and test the system before it is broadly implemented. This principle would be especially welcome in the wake of the General Office of Accountability's (GOA) findings that the FBI had substantial room for improvement in many technical and principle-related issues, including issues that came with deploying facial recognition systems that had not been rigorously tested.[137]

CONCLUSION

It is apparent that facial recognition technology is not going away any time soon. The commercial potential of the technology alone is enough to ensure its longevity and advancement, and law enforcement agencies will undoubtedly be interested in adapting FRT for their own use. To a certain extent, this is undoubtedly a good thing. We want our law enforcement officers to be good at their jobs, and proper use of FRT would certainly help them keep our citizens safe. That being said, the technology is also ripe with the potential for abuse, and both citizens and legislators alike need to be aware of the threat to constitutional rights of Americans. With that mindset, they can begin to take steps to limit the potential constitutional harms that this technology could cause, without completely hamstringing the use of FRT.

[136] U.S. DEP'T OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, FS 000311, OVC FACT SHEET: THE JUSTICE FOR ALL ACT (2016), http://ojp.gov/ovc/publications/factshts/justforall/fs000311.pdf [https://perma.cc/NVA7-ZJ3M].

[137] *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-621, FACIAL RECOGNITION TECHNOLOGY: COMMERCIAL USES, PRIVACY ISSUES, AND APPLICABLE FEDERAL LAW 3-38 (2015), http://www.gao.gov/assets/680/671764.pdf.

As law enforcement agencies get more and more comfortable with the use of facial recognition technology, courts and legislatures must be vigilant in ensuring that the rights of citizens are maintained in the face of this new technology. A balance must be struck between law enforcement's need for information and the duty our lawmakers have to preserve the rights enshrined in the Constitution.