DEFECTIVE DETECTION

Allaa Tayeb*

TABLE OF CONTENTS

* JD, Florida State University College of Law, 2022. Licensed to practice in Florida.

I. INTRODUCTION

"This is not me," Robert Williams told police after they showed him a picture of a suspect accused of stealing $3,800 in watches from a retail store called Shinola.[1] The officers detained Robert and held him for thirty hours after using facial recognition software to "match" surveillance footage of the accused thief to a database of images.[2] "The computer says it's you," the officer told Robert.[3] But unfortunately for Robert, the image really was not him. That day Robert became one of the many people wrongfully arrested due to misidentification, a not so uncommon fate created by increased use of facial recognition technology.

Based on this story, and the many others out there, it might not be hard to imagine the contours of potential harms created by this technology against vulnerable communities. Take this fictional story for example: one quiet morning in Newark, New Jersey, 23-year-old Nadia Ahmed awoke to the sound of knocking on the door by several police officers. The officers arrested Nadia on the spot, accusing her of shoplifting over $3,000 worth of merchandise, including a TV, several phones, and some furniture from a local Walmart. They claimed they caught her on camera two nights earlier committing the crime. Nadia immediately broke down in tears—she knew they had the wrong person. The night the crime was committed, Nadia attended a dinner party with at least twenty other guests that could attest to her attendance. She pleaded with them to let her go, asserting she had a reliable alibi. Sadly, the officers remained unpersuaded by this point. Unbeknownst to Nadia, her local police station and Walmart received a free trial to use a software that matches faces to a database of more than three billion images. Both Walmart and the police station used this software to "match" Nadia's face to the face of the alleged shoplifter and the police used

---

[1] Ella Torres, *Black Man Wrongfully Arrested Because of Incorrect Facial Recognition*, ABC NEWS (Jun. 25, 2020), https://abcnews.go.com/US/black-man-wrongfully-arrested-incorrect-facial-recognition/story?id=71425751.

[2] *Id.*

[3] *Id.*

this as evidence to obtain an arrest warrant. Nadia spent a week in jail and paid over $2,000 in legal costs to defend herself. Eventually, the prosecutor dropped the charges due to a lack of evidence, but the shame and fear of Nadia's detention will forever haunt her.

Like Nadia, our real-life victim Robert also had an alibi that the police never checked. Robert and Nadia have another thing in common too: they are both Black. Unfortunately for Nadia and Robert, the tools that caused their arrests are incapable of accurately reporting matches on darker-skinned people. Moreover, our fictional character Nadia's identity adds an additional layer of nuisance to the mix: she wears a hijab, a veil worn by Muslim women to cover their head and hair. As a result, the technology is even less accurate at correctly matching her face and faces like hers.

The tool that caused the tragedies against Nadia and Robert falls under a narrower category known as a facial-scanning system, but this specific tool is better known as facial-recognition technology. This technology is near ubiquitous, from the unlocking of an iPhone to the use by the US government for identifying and arresting criminals. Fortunately for our character Nadia, her story is fictional. However, it nonetheless highlights the potential trouble that facial recognition technology poses to women with identities like hers. For the purpose of this Article, Nadia and Robert's stories will be used to illustrate the ways that facial-recognition technology misidentifies and harms certain people.

Clearview AI, a small start-up company based in New York, is at the center of the controversy. Clearview came under scrutiny by privacy advocates for its use and dissemination of facial recognition technology. The company collected more than three billion images from Facebook, YouTube, LinkedIn, Venmo, and other websites to create a database used by law enforcement to identify criminal suspects.[4] Clearview's algorithm, and others like its kind, "misidentifies people with darker skin and contributes to police bias against Black communities."[5] Such an influence gives extraordinary power to government actors and raises potential First, Fourth, and Fourteenth Amendment concerns. In the hands of private actors, facial-recognition technology erodes consumer trust and may cause loss of opportunity, economic loss, loss of liberty, and social detriment to consumers.[6]

These privacy invasions may go unremedied due in large part to a lack of comprehensive federal privacy laws in the United States regulating these

---

[4] Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, NY TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[5] Shira Ovide, *A Case for Facial Recognized*, NY TIMES (Nov. 11, 2020), https://www.nytimes.com/2020/11/11/technology/facial-recognition-software-police.html.

[6] *See infra* note 136 and accompanying text.

practices. This Article will examine the individual harms of facial-recognition technology to privacy rights and propose that Congress pass a federal ban on the use of facial-recognition technology and other forms of biometric surveillance, rather than rely on piecemeal federal and state responses. Limited authority from the Federal Trade Commission (FTC) and the ongoing threat to civil liberties this technology poses makes a regulatory response impractical. A federal ban will better preserve individual privacy rights and protect against this wide-ranging and Big Brother-like surveillance.

Part I of this Article offers an overview of the technology, how it works, and discusses Clearview AI, as an exemplar. Part I also surveys the potential Constitutional violations of facial-recognition technology, with an emphasis on how the technology discriminates against darker-skinned people, women, and people in the LGBTQ+ community. Tied to these observations is a discussion of the ethical harms associated with facial recognition's general use. Part II conducts a cost/benefit analysis of facial recognition in schools, homes, airports, and as used by law enforcement. It concludes that this tool's benefits do not outweigh the harms, both because of its bias against certain people as well as the ethical harms on everyone. Part III scrutinizes the current legal frameworks that purport to control the damages of its use, including the Federal Trade Commission's case-by-case adjudication, tort law, and proposed legal regulations issued by the United States Senate and Amazon. Lastly, Part IV proffers a draft statute that bans facial recognition technology. Part IV also contemplates the key considerations and implications of a ban. While there is really no escaping surveillance in the current digital age, a more comprehensive legal framework will perhaps protect privacy rights for everyone and ensure that people like Nadia and Robert are not subjected to such an invasion.

II. FACIAL RECOGNITION IN THE AGE OF THE DIGITAL

A. What is Facial Recognition Technology?

In recent years, facial recognition technology has seen growth in almost every sector of life—including promising to increase efficiency, improve diagnosis, and lead to more criminals apprehended by law enforcement. Despite the purported benefits this technology provides, many privacy advocates are concerned that the technology is too invasive to be available to law enforcement and private actors for use at their whim.

Facial recognition technology is a digital matching technology that

breaks down digital images of faces into identifiable components.[7] It is a form of facial scanning systems and works by verifying and identifying faces.[8] Other forms of facial scanning, such as facial detection, work by simply detecting faces— for instance, when you look into your phone camera the camera simply detects your face.[9] Facial characterization on the other hand, purportedly uses facial analysis to detect emotion.[10] This form of facial scanning also purports to identify gender, age range, and emotional indicators.[11]

Facial recognition is the most controversial form of facial scanning. Through a "point-based" design, this technology creates a template from the facial structure of a person and matches it against a database of photos. Simply put, this form of facial scanning creates a "faceprint," or a digital representation that maps the unique features of an individual's face.[12] Facial Recognition Technology (FRT)[13] works by comparing a data subject's captured image against images already in a database. Specifically, FRT "has two components that work in tandem: a database of known photo templates and a software capable of comparing these templates to the geometry of the subject's face, identifying up to 30,000 facial landmarks."[14] FRT was once performed unreliably, by just measuring distances between facial points.[15] Recent advancements in artificial intelligence have improved the

---

[7] Note, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1871 n.14 (2007).

[8] EVAN SELINGER & BRENDA LEONG, *The Ethics of Facial Recognition Technology*, OXFORD HANDBOOK OF DIGITAL ETHICS 1–2 (2022).

[9] *Id.* Personal identifiable information is defined by the Department of Labor's "Guidance on the Protection of Personal Identifiable Information (PII)" as "[a]ny representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." *Guidance on the Protection of Personal Identifiable information*, U.S. DEP'T OF LABOR, https://www.dol.gov/general/ppii (last accessed Feb. 26, 2022). PII also is defined as information: "(i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individual in conjunction with other data elements, i.e., indirect identification." *Id.*

[10] SELINGER & LEONG, *supra* note 8.

[11] *Id.*

[12] *Id.*

[13] The acronym 'FRT' refers to facial recognition technology will be used throughout this Article.

[14] *About Face ID Advanced Technology*, APPLE (Sept. 19, 2019), https://support.apple.com/en-us/HT208108.

[15] Kashmir Hill, *Your Face is Not Your Own*, NY TIMES (Mar. 18, 2021), https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html?action=click&module=Top%20Stories&pgtype=Homepage.

technology's capabilities significantly.[16] These advances, however, have not changed the accuracy for facial-scanning systems. One study by the ACLU even falsely matched twenty-eight members of Congress with mugshots using Amazon's Rekognition, a FRT software that is available on the market.[17]

The National Institute of Standards and Technology (NIST) has found significant errors in its FRT tests, with problems arising from "intrinsic and extrinsic factors, including the way in which photos are captured and the complexities of facial features and human movement."[18] Part of this stems from the implicit bias surrounding human interactions. Disparate results are unavoidable where real-world bias "seep[s] into artificial intelligence."[19] Joy Buolamwini, a researcher studying bias in FRT, found that "bias reflecting social inequities in training data can embed unintended bias in the models that are created."[20] Her research revealed that the error rates for facial-recognition programs is never higher than 0.8 for light-skinned men, but has a 20–34% error rate for darker-skinned women.[21] Due to these higher error rates, Buolamwini suggests that to ensure complete accuracy, benchmark datasets must be diverse and intersectional.[22] The system is only as good as its training data— if the dataset contains less women, but more men, or less Black people, but more white people, it will produce a largely inaccurate result for those unrepresented classes. Moreover, as Buolamwini mentioned during the Conference on Fairness, Accountability, and Transparency, "our benchmarks, the standards by which we measure success, themselves can give us a false sense of progress."[23] Without a balanced model and accurate benchmark, not only will the programs misidentify certain people, but might

---

[16] *Id.*

[17] Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (Jul. 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

[18] Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1169 (2021).

[19] Steve Lohr, *Facial Recognition is Accurate, if You're a White Guy*, NY TIMES (Feb. 9, 2019), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

[20] Joy Adowaa Buolamwini, Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers (Dec. 6, 2017) (Masters thesis, Massachusetts Institute of Technology) (on file with the Massachusetts Institute of Technology library archive).

[21] Larry Hardesty, *Study Finds Gender and Skin-Type Bias in Commercial Artificial Intelligence Systems*, MIT NEWS (Feb. 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

[22] *Id.*

[23] *Id.*

also imply equality between classes where there is none.

B. Controversy with Clearview

Clearview AI, a prominent provider of FRT, articulates a simple mission: to provide a research tool for law enforcement agencies to "identify perpetrators and victims of crimes."[24] This company snuck into the world of facial recognition quietly— not many people knew of Clearview's existence outside of law enforcement officials.[25] This quiet beginning was a tactic to avoid "tipping off would-be criminals."[26] Perhaps this was a good idea because with Clearview's technology, some criminals were, in fact, apprehended. For instance, in May 2019 the Department of Homeland Security used Clearview's algorithm to identify a sexual abuser.[27] A Department of Homeland Security (DHS) agent sent a photo of the alleged abuser to investigators all around the country.[28] One investigator ran the photo through Clearview's app and found a match in an Instagram photo of a female fitness model and man at a bodybuilding expo—but the bodybuilders were not actually the "match" the app pointed the investigator to.[29] In the background of the photo was a man standing behind a counter of a booth selling workout supplements; Clearview's app identified him as the match. The agent was shocked, especially because the image of the man was no bigger than a "fingernail."[30] Moreover, Clearview's facial recognition app saw a spike in use following the January 6 insurrection on the U.S. Capitol. Police departments across the country used this system to help the FBI identity the rioters that stormed the Capitol.

This is not the only time law enforcement was able to identify dangerous criminals using the app. In fact, Clearview's website boosts this statement by a detective in a sex crimes unit: "Clearview AI is hands-down the best thing that has happened to victim identification in the last 10 years. Within a week and a half of using Clearview AI, [we] made eight identifications of either victims or offenders through the use of this new tool."[31] Clearview's mission statement continues by proclaiming that "law enforcement is able to catch the most dangerous criminals, solve the toughest

---

[24] CLEARVIEW.AI, https://clearview.ai/ (last accessed Feb. 26, 2022).

[25] Hill, *supra* note 15.

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] CLEARVIEW.AI, *supra* note 24.

cold cases and make communities safer."[32] Since developing Clearview, over six-hundred law enforcement offices have used the technology.[33]

Once folks caught wind of what and how Clearview operated, people started questioning the accuracy of its algorithm. Critiques of Clearview's algorithm centers on roughly three issues: (1) the nature of its uses—including the fact that not only law enforcement has access, but that it was available to private entities as well; (2) the methods the app uses to identify faces – such as an algorithm that is not racially neutral; and (3) where these images were taken from. To start, Clearview developed its app by scraping[34] over three billion images from Facebook, YouTube, Twitter, Venmo, and other websites to create its database.[35] Facebook, LinkedIn, Venmo, and Google issued cease-and-desist letters to the company for violating its terms of service, but Clearview argued it has a First Amendment right to consume these public photos. Essentially the app works in this way: "you take a picture of a person, upload it and get to see public photos of that person, along with links to where those photos appeared."[36]

Additionally, most FRT is not racially neutral. As mentioned earlier, an inclusive benchmark dataset is necessary for an error-free algorithm.[37] The National Institute of Standards and Technologies (NIST) is tasked with testing the capabilities and accuracy of FRT, among other things.[38] However, Clearview's algorithm has not been tested by NIST. Tests conducted by NIST on FRT suggest differences in accuracy across race, gender, and other demographics. In fact, results from a 2011 study by NIST suggests that "conditions in which an algorithm is created—particularly the racial makeup of its development team and test photo databases— can influence the accuracy of the results."[39] As Joy Buolamwini puts, "for human-centered computer vision . . . transparency [should] provide information on the demographic and phenotypic composition of training and benchmark

---

[32] *Id.*

[33] Hill, *supra* note 4.

[34] Scraping is a process that copies data from documents and web applications; Clearview scrapped images from various social media websites.

[35] *Id.*

[36] *Id.*

[37] *See supra* note 22 and accompanying text.

[38] *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies*, *Hearing Before the H. Comm. On Homeland Sec.*, 116th Cong. 2–3 (2020) (statement of Charles H. Romine, Dir., Nat'l Inst. Standards and Tech.)

[39] Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, ATLANTIC (Apr. 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/the-underl.

datasets."[40] Without a fully transparent and diverse algorithm, companies like Clearview cannot verify that their technology is completely accurate.

Earlier in 2021, news that Clearview filed a patent application surfaced. The patent was specifically for transacting with non-governmental customers and detailed ways that this technology can benefit the public, including running rapid background checks on people based on a person's face.[41] While Clearview announced early in 2021 that it will stop doing business with companies not working with law enforcement,[42] the chilling effects of its former availability to private companies remains. Likewise, without federal guidance, the choice not to allow private entities access to it is entirely discretionary—there is nothing stopping another company from creating FRT and doing business with companies since Clearview backed out of this practice.

However, when this technology was readily available to private companies, reports indicated that Clearview licensed access to its technologies to Macy's, Kohls, Walmart, and even the NBA.[43] Clearview's actions have been challenged by many privacy advocates, including the American Civil Liberties Union (ACLU). The ACLU filed a class action in Illinois under the State's Biometric Information Privacy Act, and cited this as its primary concern:

> By building a mass database of billions of faceprints without knowledge of consent, Clearview has created a nightmare scenario that we've long feared and has crossed ethical bounds that many companies have refused to even attempt. Neither the United States government nor any American company is known to have ever compiled such a massive trove of biometrics.

As of now, privacy advocates' concerns with this technology are difficult to solve, mostly due in large part to the lack of comprehensive

---

[40] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classifications*, 81 PROCS. ON MACH. LEARNING RSCH. 1, 12 (2018).

[41] Carolina Haskins, et al., *A Clearview AI Patent Application Describes Facial Recognition For Dating, And Identifying Drug Users and Homeless People*, BUZZFEED NEWS (Feb. 11, 2021), https://www.buzzfeednews.com/article/carolinehaskins1/facial-recognition-clearview-patent-dating.

[42] Steven Musil, *Clearview AI to Stop Providing Facial Recognition to Private Companies*, C|NET TECH (May 7, 2020), https://www.cnet.com/tech/services-and-software/clearview-ai-to-stop-providing-facial-recognition-to-private-companies/.

[43] Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1, 2 (2020).

guidelines that can hold government and private actors accountable for using—or in the case of Clearview, developing—the technology. Some jurisdictions, however, including states like Illinois and cities like San Francisco, have passed bans and moratoriums on FRT to preserve privacy rights for its citizens.

Equally problematic as Clearview, companies like Amazon and Google have also started developing and selling FRT. In fact, Google's marketing team hired contractors to stroll Atlanta and take scans of volunteers to improve its software. Unfortunately, many of the people that Google's contractors targeted were Black homeless people.[44] Part of the issue with Google targeting a community of Black homeless people is that it is exploiting an already vulnerable community and using them for commercial gain. Moreover, these vulnerable communities cannot fully appreciate the gravity of rights they forgo by allowing their face to be scanned. As this article will demonstrate, without federal oversight, companies like Google can essentially do as they please with the data they collect.

III. COST AND BENEFIT ANALYSIS

Part of the consideration of whether FRT should ever be readily available is whether there are any benefits to its use. This Part will consider the benefits of using FRT and weigh them against the costs.

A. Benefits to Private Entities Using Facial Recognition Technology

Many businesses in the United States have already implemented the use of facial recognition technology (FRT). The wide-ranging purposes of FRT's use present interesting arguments about the benefit of imposing regulations rather than a ban. If many consumers already enjoy the luxuries of FRT without complaint, why prevent its continued use by businesses?

1. Use in Businesses

Proponents of FRT cite a range of purposes that increase efficiency for businesses and consumers. For example, DeepScore, a Tokyo-based company, created a facial- and voice-recognition app and claims the app can "determine how trustworthy a person is in just one minute."[45] The app works by having the person look into their phone camera and answer a few short

---

[44] Hill, *supra* note 15.

[45] Todd Feathers, *This App Claims It Can Detect 'Trustworthiness.' It Can't*, VICE (Jan. 19, 2021), https://www.vice.com/en/article/akd4bg/this-app-claims-it-can-detect-trustworthiness-it-cant.

questions.[46] The app then analyzes muscular twitches in the person's face and any changes in the person's voice to assess whether they should be approved for a business loan or coverage for health insurance.[47] The technology aims to revolutionize the way that companies use credit scores to assess consumer trustworthiness and allows consumers without a credit history to qualify for loans or health insurance.[48] This form of technology is like the pseudoscience of phrenology, the study of skull shapes as an indicator of mental abilities.[49] The researchers that created phrenology in the early 1800s did so to suggest that white men's minds were different than Native American and African American people.[50] Despite the racial basis for this idea's development, apps like DeepScore suggest that, somehow through phrenology, accurate assessments of individuals can be made. Most research actually indicates that facial expressions cannot accurately assess mental state or personal intentions.[51]

Although this technology is primarily used in Japan, Indonesia, Vietnam, and the Philippines, there is no clear regulatory framework that bans its use or the development of similar apps in the United States. This fact should raise concerns among US consumers, especially given the discriminatory effect of facial-recognition technology on people of color, children, and women that was mentioned earlier in the Article.[52] Aside from the demonstrated algorithm bias present in FRT, there is also "no reliable science to indicate that these peoples' facial expressions or the inflections of their voices are proxies for their internal mental and emotional states."[53] Again, the racial implications and history that the pseudoscience of phrenology should be enough to suggest that these technologies are wholly inaccurate for everyone, but specifically for people of color. As a result, it is nonsensical to believe that an app can ever truly discern whether an individual is "trustworthy" enough to deserve health insurance or a loan. Moreover, algorithmic biases may cause unintended inequities and harms to darker-skin users and women.[54] Say for example, Nadia or Robert enter a bank that uses

---

[46] *Id.*

[47] *Id.*

[48] *Id*.

[49] Andrew Bank, *Of 'Native Skulls' and 'Noble Caucasians': Phrenology in Colonial South Africa*, 22 J. OF S. AFR. STUD. 387, 402–03 (1996).

[50] *Id.*

[51] *See, e.g.*, Tayla Rachel Meyers, *Why Our Facial Expressions Don't Reflect Our Feelings*, BBC (May 10, 2018), https://www.bbc.com/future/article/20180510-why-our-facial-expressions-dont-reflect-our-feelings.

[52] See *supra* Part I.C.

[53] Feathers, *supra* note 45.

[54] *See infra* Part II.D (discussing "ethical harms").

this software. Because of Nadia and Robert's darker skin color, the system might inaccurately assess their level of trustworthiness to receive a loan or health insurance, thereby possibly denying them access to it. Such a resolution leads to unintended consequences for people like Nadia and Robert—without access to health insurance or a loan to purchase a home or car, both these people cannot fully take part in the luxuries of social progress.

2. Use in Shopping Centers and by Employers

Many U.S. shopping centers have started using the facial features of consumers—captured from cameras installed throughout the stores—to detect an individual's path of travel and then mine the data collected to "determine traffic patterns, worker performance and consumer reaction to displays and marketing."[55] Centers using FRT suggest that this will provide better service and support to consumers.[56] Even more, shopping centers can use this technology to identify and catch shoplifters.

In the employment sector, software programs developing FRT promise to identify personality traits of job candidates based on facial expressions and physical differences like wearing glasses or a headscarf.[57] This study of this software program assessed personality traits in five dimensions: openness, conscientiousness, extraversion, agreeableness, and neuroticism.[58] The results varied depending on the outfits worn by each candidate, but the developer of the software remarked that "the impression that a person makes on other people is part of the concept" and that "the algorithm is trained to measure the impression of people, so how people judge someone's personality from observation."[59] This AI's assessment of personality has a 90 percent accuracy compared to those of a group of human observers.[60]

Here, like in every other instance of FRT's use, the discriminatory effect of biased algorithms may cause disparate harms to darker-skinned and female customers. Robert is a clear example of this—the Michigan State police inaccurately matched Robert's face to the face of the actual shoplifter.

---

[55] Esther Fung, *Shopping Center Exploring Facial Recognition in Brave New World of Retail*, WALL STREET J. (Jul. 2, 2019), https://www.wsj.com/articles/shopping-centers-exploring-facial-recognition-in-brave-new-world-of-retail-11562068802.

[56] *Id.*

[57] Elisa Harlan & Oliver Schnuck, *Objective or Biased: On the Questionable Use of Artificial Intelligence for Job Applications*, BAYERISCHER RUDFUNK (Feb. 16, 2021), https://web.br.de/interaktiv/ki-bewerbung/en/.

[58] *Id.*

[59] *Id*.

[60] *Id*.

It is important to consider the impact this will have on the perception of people of color as well; if the software continues to misidentify people of color like Robert as perpetrators of crimes they did not commit, perhaps it will impact the public's perception and cause unintended stereotypes to resurface. This software also reports a higher level of trust associated with people wearing a head covering, but this all still begs the question of how accurate a software is that can be tricked depending on the clothing a person wears.

More concerningly, in the employment context, FRT can adversely affect access to opportunities for people affected by these disparate harms. In *Ethics of Facial Recognition Technology*, Evan Selinger and Brenda Leong point out these potential adverse effects—namely that there is an obvious loss of opportunity related to employment when an employer misuses FRT and decides whether to hire an applicant solely off FRT's assessment of their qualifications. An example of this is "an employer us[ing] a biased facial scanning system during an interview to evaluate the applicant for characteristics of friendliness or other aspects that would make her a 'good fit' for company culture, and ultimately treat[ing] this analysis as the deciding factor over her resume, performance and other qualifications."[61] For people like Nadia and Robert, access to employment may be limited if facial scanning systems inaccurately report them as being a poor fit for a company's culture.

3. Use in Schools

Some schools have already used FRT in classrooms for a range of purposes, including as a security measure to restrict certain adults from entering campus. The technology works by alerting administrators if FRT finds a match between an adult and a restricted adult in a database.[62] Another software manufacturer has proposed using the technology to identify and track potential school shooters. School administrators will receive an alert if a student or adult trespasses on campus. More recently, a tablet, GoSafe, developed by the company OneScreen, can scan foreheads of students and teachers for elevated temperatures and can even detect when students are not wearing a mask.[63] GoSafe's benefits go beyond a pandemic-riddled world;

---

[61] SELINGER & LEONG, *supra* note 8.

[62] Emily Tate, *With Safety in Mind, Schools Turn to Facial Recognition Technology. But at What Cost?* EDSURGE (Jan. 31, 2019), https://www.edsurge.com/news/2019-01-31-with-safety-in-mind-schools-turn-to-facial-recognition-technology-but-at-what-cost.

[63] Gregory Barber, *Schools Adopt Face Recognition in the Name of Fighting COVID*, WIRED (Nov. 3, 2020), https://www.wired.com/story/schools-adopt-face-recognition-name-fighting-covid/.

schools can also use it to take attendance and prevent intruders from entering campus.[64]

Pressing concerns of FRT's use in schools mostly revolve around collecting, using, and disclosing minors' personal information and biometric identifiers. More than this, the same risks of inaccurate reporting against children of color are an important concern. One argument against its use discusses a threat to children's right to "privacy, free expression, and association."[65] The fear is that constant surveillance of children may cause them to censor their actions and will discourage "spontaneous and playful" association between friends and siblings that the school regards as "troublemakers."[66] Evan Selinger and Brenda Leong call this a "social detriment."[67]

For example, consider this: one day our fictional character Nadia takes a test that uses software that records and assesses whether she cheats or not. The software purports to detect and flag signs of cheating and send teachers a report as well as video footage of each student taking the exam. Unless the software flags a student for cheating, the teacher does not really review the video footage. Due to the inaccurate algorithm, the exam cannot correctly detect Nadia's face or assess her emotions and as a result, flags her several times for cheating. The school places a hold on Nadia's grade pending an investigation of the video taken of her during the exam. This happens to Nadia, and other students of color, quite often, causing each student unnecessary fear and stress while taking exams. These students also predict that administration will have to review the video surveillance each time they sit for an exam, causing them to experience less of an expectation of privacy than their white peers.

Regrettably, this system is actually real and sold on the market; it is known as Proctorio, a proctoring platform that claims to use "state-of-the-art technology" to "ensure the total learning integrity of every assessment, every time."[68] Proctorio works by observing test takers for over 20 behaviors and preparing a report with 'flags,' or suspicious behaviors picked up during the session. Yet, students still report cheating on almost every exam administered

---

[64] *Id.*

[65] *Facial Recognition Technology in US Schools Threatens Rights*, HUMAN RIGHTS WATCH (Jun. 21, 2019), https://www.hrw.org/news/2019/06/21/facial-recognition-technology-us-schools-threatens-rights.

[66] *Id.*

[67] SELINGER & LEONG, *supra* note 8, at 8.

[68] Gabriel Geiger, *Students Are Easily Cheating 'State-of-the-art' Test Proctoring Tech*, VICE (Mar. 5, 2021), https://www.vice.com/en/article/3an98j/students-are-easily-cheating-state-of-the-art-test-proctoring-tech.

through Proctorio with relative ease.[69] Even a Teaching Assistant tested the system and found that it mostly flagged students for benign audio violations and nothing more.[70] What this tells us is that these technologies purport to do more than they actually can. Worse, and much like the example given, it allows certain groups to get away with more and causes others to reap greater harms. Also notable is that this system and others like it create unnecessary invasions into student privacy by video recording students in the privacy of their homes and then cherry-picking without any degree of reliability certain students to review in-depth.

4. Use in Homes

One of the most personal uses of FRT is the recent use of "smart homes." In Miami, a developer designed condominiums with a "passive facial-recognition system" that alerts the concierge of the resident's arrival and "use[s] facial-recognition or a fob to get to the private landing of [the] unit."[71] This means that even if your key fob is lost or stolen, you can always access your unit. This also increases security by preventing home invaders from entering. This technology is based on algorithms that collect unique codes based on the resident's biometric identifiers. The code is matched against the real bio-identifier when the user touches a scanner or looks into the digital cameras throughout the home or complex.

Users of "smart home" technology are concerned over the various parties that will have access to the biometric system information, including their fingerprints and faceprints.[72] Fortunately, some companies have implemented encryptions that can help protect that information. Unfortunately, the inaccuracy of FRT algorithms may still present disadvantages for "smart home" users that have darker-skin and who are women. For example, Nadia might face a greater difficulty entering her home simply because her skin and hijab will present difficulties for this faulty system. It is possible that with this difficulty, Nadia and Robert, might again be misidentified as an intruder in their home and made a suspect by police.

B. Benefits of Government Use of Facial Recognition Technology

The United States government is the largest consumer of facial

---

[69] *Id.*

[70] *Id.*

[71] Antonio Pacheco*, High-end Homes are going Biometric*, ARCHINECT NEWS (Jun. 24, 2019), https://archinect.com/news/article/150143031/high-end-homes-are-going-biometric.

[72] Rowe, *supra* note 43, at 5.

recognition technology.[73] Government agencies use FRT for a range of purposes, from criminal justice to airport security, to use by law enforcement.

1. Use by Airport Security

FRT has many benefits to airport security and increasing efficiency with boarding passengers. Airlines like JetBlue have started using FRT to speed up boarding and "sift through security threat[s]."[74] When a JetBlue customer arrives at the airport and goes through the first security checkpoint, a facial image is "grabbed."[75] When the passenger boards the flight, another image is taken of their face and is compared against the image taken at the first checkpoint to ensure the correct passenger is boarding.[76]

JetBlue is not alone in its use of FRT. In fact, FRT has been used by Customs and Border Protection in over three million instances since June 2017.[77] Some airports even require travelers to take a photo with an iPad at departure gates and then use that photo to compare against a database of images pulled from the Department of Homeland Security.[78] The image will either flash green or red– green indicates a person is clear to board and red indicates the person should be pulled aside for additional screening. In a post-9/11 America, increased airport security is often understood as an essential element to ensuring national security. One article points out that "when people know they are being watched, they are less likely to commit crimes."[79] In airports, the prevalence of facial surveillance technology may deter individuals that intend to commit national security breaches.

However, algorithmic inaccuracies will likely lead to misapprehending individuals or missing suspicious behaviors that the technology is not designed to detect. Even without facial recognition software, people like Nadia are often made suspect by airport security and

---

[73] *Id.* at 6.

[74] Francesca Street, *How Facial Recognition is Taking Over Airports*, CNN TRAVEL (Oct. 8, 2019), https://www.cnn.com/travel/article/airports-facial-recognition/index.html.

[75] *Id.*

[76] *Id.*

[77] Rowe, *supra* note 43, at 22.

[78] Lori Aratani, *Facial-Recognition Scanners at Airports Raise Privacy Concerns*, WASH. POST (Sept. 15, 2018), https://www.washingtonpost.com/local/trafficandcommuting,/facial-recognition-scanners-at-airports-raise-privacy-concerns/2018/09/15/a312f6d0-abce-11e8-a8d7-0f63ab8b1370_story.html.

[79] Bernard Marr, *Facial Recognition Technology: Here Are the Important Pros and Cons*, FORBES (Aug. 19, 2019), https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/?sh=292db61514d1.

subjected to increased surveillance through so-called "random" selections. It is indeed possible that with support of an inaccurate algorithm that may identify people like Nadia as "suspicious," the implicit biases that already exist against Arab Americans and Muslims traveling through U.S. airports, will only get worse.

Supporters of its use in airports report that the scans are optional for United States citizens, but unless airports better communicate the right to refuse a scan, many people may still unintentionally submit to it. This is because most people do not really read the signs around the airport that discuss these rights, but even if they had, uninformed individuals cannot be expected to fully appreciate the invasion this technology poses. One reason for this is that "people do not and largely cannot possess an appropriate level of knowledge about the substantial threats that facial recognition technology poses to their own autonomy."[80] Discussing the enforceability of privacy agreements in the online context, Wayne Logan and Jake Linford theorized that consumers "only have a duty to read contractual language when they have a reasonable opportunity to read it and when the language is understandable."[81] While this is not a contract or privacy agreement, the argument still stands: travelers cannot fully comprehend the rights they forgo when they submit to scans where the only notice is signs strewn in small places throughout a busy airport. This notice also requires the consumer to understand what it means to give up scans of their facial identifiers, but the average layperson is not an expert on the risks and benefits of FRT.

2. Use by Law Enforcement

Law enforcement can greatly benefit from the use of FRT. Most notably, it can enable law enforcement agencies to conduct efficient investigations, help gather reliable evidence, identify criminals, locate missing persons, and deter crime.[82] For example, in New York police officers apprehended an assailant accused of threatening a woman with rape at knifepoint within 24 hours of the incident.[83] Additionally, in cities with high crime rates and not enough police officers to fight crime, businesses can take matters into their own hands by installing the technology and catching shoplifters on their own.[84] The primary benefit is clearly crime-prevention.

---

[80] Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 33, 104 (2019).

[81] Wayne A. Logan & Jake Linford, *Contracting for the Fourth Amendment Privacy Online*, 104 MINN. L. REV. 101, 138 (2019).

[82] Marr, *supra* note 79.

[83] *Id.*

[84] *See infra* p. 22.

Here, like with benefits to airport security, FRT can deter criminals from committing crimes in the first place if there is an imminent fear of constant surveillance.[85] Other U.S. security agencies, like U.S. Immigration and Customs Enforcement, believe using FRT will help prevent border crossing too.[86]

However, in no other context is FRT more dangerous than in the hands of law enforcement. The possible misuses and abuses have the potential to cause detrimental effects on individuals, with harms ranging from "loss of liberty," "societal detriment," and constitutional violations.[87] One need only look to our real-life example, Robert, as proof of this. For Black men like Robert, there is already an inherent fear attached to police interaction.[88] In fact, Robert's attorney called her client "lucky" despite his trouble, because the situation did not escalate any further.[89] Robert also reported feeling humiliated after his arrest—his boss even advised him not to tell anyone at work and he chose not to share this information with his mother.[90] Had Robert's detention lasted any longer, it is possible he might have lost his job, his family, and his social circle. FRT's use by law enforcement largely implicates the First, Fourth, and Fourteenth Amendment violations mentioned earlier in this Article.[91]

C. The Harms of Widespread Use of Facial Recognition Technology

As mentioned throughout Part I, the harms of Clearview's technology and other forms of FRT are massive. This section will address constitutional harms, ethical harms, and tangible harms, such as discrimination, over-policing, and misidentification.

1. First Amendment Violation

A potential First Amendment violation of FRT may appear more predictive than current, however, it is nonetheless a vital piece to explore. The First Amendment of the Constitution reads:

---

[85] *See infra* p. 22.

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

[87] *See supra* Part I.C.

[88] Kashmir Hill, *Wrongfully Accused by an Algorithm*, NY TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[89] *Id.*

[90] *Id.*

[91] *See supra* Part I.C.

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of people peaceably to assemble, and to petition the government for a redress of grievances.[92]

Privacy advocates specifically note that there is an inherent right to anonymity that is attached to the First Amendment. This idea holds that without some degree of freedom to walk around without consistent surveillance, people are less inclined to be their authentic selves—especially when an individual's identity is tied to a potentially controversial affiliation. This idea impacts the right to religious association, speech, and right to protest the most. Advocates broadly define anonymity 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."[93] While the right to anonymity is not entirely supported by all courts, the courts that do recognize this right as inherent to the Constitution also recognize a "vital relationship between freedom to associate and privacy in one's association."[94]

Tied to First Amendment rights is the fundamental right to privacy from government surveillance of a person's movements. Consistent surveillance of people in the most intimate portions of life, *i.e.*, at protests, political rallies, and places of worship stifles free speech because the "awareness of being watched affects individual's behavior regardless of whether they intend any wrongdoing."[95] In fact, "[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 . . . and on and on."[96] All things considered, the right to freely associate should not be undermined by allowing the government to freely surveil and identify people.

---

[92] U.S. Const. amend I.

[93] Kimberely N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 412 (2014) (citing DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 5 (2008)).

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

[95] SELINGER & LEONG, *supra* note 8, at 11.

[96] 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, 114 (2017).

2. Fourth Amendment Violation

Possibly the strongest argument against government actors using FRT to identify, track, and ultimately arrest criminals is baked into the Fourth Amendment privacy rights. The Fourth Amendment guarantees that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated," and asserts "no warrant shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the places to be seized, and the persons or things to be seized."[97] The Supreme Court in *Katz v. United States* established that the Fourth Amendment protects a reasonable expectation of privacy and advanced a two-part test to determine whether an expectation of privacy has been violated by the government.[98] Some privacy scholars worry that current Fourth Amendment jurisprudence is not sufficient to address the sophistication necessary to assess FRT's potential Fourth Amendment abuses caused by FRT.

Recent cases that concern technology or unwarranted surveillance by police officers say very little about advanced forms of facial scanning, like facial recognition technology. The two most pertinent cases to this discussion are *Kyllo v. United States*.[99] and *Illinois v. Lidster*[100] In *Kyllo*, police used a thermal-imaging device to scan the defendants' home to determine if the amount of heat emanating from the roof is typical for marijuana growth.[101] The court in *Kyllo* held that the use of sense-enhancing technology that normally could not have been obtained without a physical intrusion to the home violated the reasonable expectation of privacy and therefore is a search under the Fourth Amendment.[102] In *Lidster*, police set up a highway checkpoint to obtain information about a hit-and-run accident that occurred a week earlier.[103] The officers stopped each vehicle for 10 to 15 seconds, asked them some questions, and handed them a flyer describing the situation and requesting information.[104] The court in this case discussed issues related to unwarranted public surveillance and held that the Fourth Amendment does

---

[97] U.S. Const., amend. IV.

[98] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

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

[100] Illinois v. Lidster, 540 U.S. 419 (2004).

[101] *Id*. at 30.

[102] *Id.* at 40.

[103] *Illinois,* 540 U.S. at 421.

[104] *Id.* at 422.

not protect against police surveillance at highway checkpoints.[105] The court reasoned that the "relevant public concern was grave . . . and the stop advanced this concern to a significant degree."[106] After the decision in *Lidster*, Judge Posner remarked 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."[107]

These two cases highlight the current jurisprudence's deficiency to answer whether police use of FRT violates the Fourth Amendment. While these holdings are informative, neither case considers how evolving technology fits into the picture. It is important to note that plenty of plaintiffs, including Robert Williams, have brought Fourth Amendment claims against government actors that use FRT.

However, none of those cases have produced actionable guidance. Until a court considers FRT specifically, or a technology similar to it, there is no official guidance on whether and to what extent this technology violates the Fourth Amendment.

With this in mind, even if courts were to better define how the Fourth Amendment applies to newer technology, there is still a lasting fear that use of FRT might still be abused under the exceptions to the exclusionary rule of the Fourth Amendment. The good faith doctrine in particular can lead courts to excuse a police error if the officer acted under good faith belief that they were in accordance with legal authority. Courts shouldn't be able to apply a good faith to FRT because these errors are different from those committed by police—FRT errors are system errors, not police errors. In *Hein v. North Carolina*, the court stated, "[t]o be reasonable is not to be perfect, and so the Fourth Amendment allows for some mistakes on the part of government officials."[108] Important to this is the language "on the part of government officials"—a statement that highlights that human action is sometimes excusable if individuals, not computers, acted in good faith.

Additionally, cases like *Byrd v. Lamb* accentuate the idea that courts are not particularly sensitive in evaluating police abuse. The defendant in *Byrd* brought a *Bivens* action[109] against a federal agent that allegedly used

---

[105] *Id.* at 428.

[106] *Id.*

[107] RICHARD POSNER, NOT A SUICIDE PACT: THE CONSTITUTION A TIME OF NATIONAL EMERGENCY 91 (Oxford Univ. Press, 2006).

[108] Ferguson, *supra* note 18, at 1192.

[109] "A Bivens action generally refers to a lawsuit for damages when a federal officer who is acting in the color of federal authority allegedly violates the U.S. Constitution by federal officers acting." *Bivens Actions*, LEGAL INFORMATION INSTITUTE,

excessive force to perform an unlawful seizure.[110] The court in *Byrd* refused to extend *Bivens* to defendant's claim, citing precedent that did the same.[111] Judge Don. R. Willett, writing for the concurrence, expressed concern that with *Bivens* essentially "off the table," victims have really no judicial forum to complain of police misconduct. While the court did not explicitly renounce *Bivens*, consistently refusing to hold police accountable can cause distrust in the legal process.

Law professor Andrew Guthrie Ferguson discusses two insights helpful for future Fourth Amendment analysis. First, the court typically defers to human decision-making, but "programmatic" decision-making is different and should be different under constitutional scrutiny.[112] Second, the Supreme Court often forgives good faith and isolated errors from officers, but systemic or recurring errors[113] are not forgivable.[114] New systems of FRT are better examined with these insights in mind should a case involving FRT reach the Supreme Court.

Companies like Clearview are private actors and therefore not bound by the Fourth Amendment. However, under the entanglement exception to the State Action Doctrine, private conduct is considered state action if the state authorizes, encourages, or facilitates private conduct that if it were a state action would violate the Constitution.[115] The question then is whether police action using Clearview's system violates the Constitution. At issue in the litigation against Clearview is whether the images the company collected were public or if Clearview violated the website's terms of service by collecting them. This also implicates the "third-party doctrine," a doctrine that holds that there is no reasonable expectation of privacy in information willingly exposed.[116] For this reason, law enforcement agents might argue that the images in Clearview's database were willingly put online by users and as a result, not deserving of Fourth Amendment protections.

In *Carpenter v. United States*, the Supreme Court addressed whether long-term data collection used to track a person's movements constituted a search. The court held that it did and "redefined" the reasonable expectation

---

https://www.law.cornell.edu/wex/bivens_actions (last accessed Mar. 12, 2022).

[110] Byrd v. Lamb, 990 F.3d 879, 880 (5th Cir. 2021).

[111] *Id.* at 882.

[112] Programmatic decision-making here simply refers to the way that facial recognition technology processes data from the database of images to produce a match. *See* Hao-Fei Cheng, et al., *Explaining Decision-Making Algorithms through UI: Strategies to Help Non-Expert Stakeholders*, CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (2019).

[113] *See infra* Part II.C.

[114] *See supra* text accompanying notes 95–105.

[115] Burton v. Wilmington Parking Auth., 365 U.S. 715, 716–18 (1961).

[116] Smith v. Maryland, 442 U.S. 735, 749 (1979).

of privacy test in the digital age to say that people have a reasonable expectation in their movements even if the CSLI data collected was turned over by a user to the cell phone service provider. Applying this understanding to whether the images Clearview scraped implicate the third-party doctrine, it is reasonable that people preserve an expectation of privacy in images they post online. This is because people do not fully predict that when they post a photo to Facebook or Instagram, it might end up in a government database. Moreover, the argument here is that the potential for ubiquitous FRT could create a long-term tracking system for everyone – one that might allow someone to 'plug' in and see where you are each time you step before a camera. Much like in *Carpenter*, this sort of tracking of movements has lasting effects and courts should be reluctant to allow it. That said, *Carpenter* does not fully apply to FRT, in part because the Court in *Carpenter* did not fully renounce the third-party doctrine.[117] Still, it provides insightful guidance on how deep-rooted the issue is and why legislation is the best bet at addressing its harms.

Law professors, Jake Linford and Wayne Logan, addressed *Carpenter*'s narrow holding and point out that state and federal courts are filtering out or rejecting the use of the third-party doctrine in Fourth Amendment cases that concern the internet age.[118] They argue instead that courts must be skeptical of interpretations of contract that waive Fourth Amendment rights in any situation where a consumer is likely to be on notice that the waiver occurred. This is because user privacy expectations are far removed from the conduct of online platforms, and consumers have weaker bargaining power, meaning they cannot fully comprehend the rights they forgo when they agree to an internet platforms terms of service.[119] Rather, "courts should reasonably understand that users might have consented to certain commercial exposure without necessarily waiving fundamental constitutional rights."[120]

In the case of FRT, it is unlikely that a user understood that posting a photo on Facebook meant it might be scraped by a company and used to power facial-recognition technology for use by the police. Even worse, nobody expects that merely walking in the background of a photo means forgoing Fourth Amendment rights. People do not possess the requisite knowledge necessary to appreciate the threat that FRT poses to their "autonomy," and due to that, people do not forgo their rights simply by

---

[117] Logan & Linford, *supra* note 81, at 103.

[118] *Id.*

[119] *Id.*

[120] *Id*. at 105.

posting photos of themselves and their family online.[121]

3. Fourteenth Amendment Violation

A program biased against people of color, women, and people who are transgender potentially violates the Equal Protection Clause of the Fourteenth Amendment as well. The Equal Protection Clause ensures that no state can "deny any person within its jurisdiction equal protection of laws."[122] Under this right, no state shall draw classifications between people unless the action satisfies a particular level of judicial scrutiny. Such a protection is vital to preserving civil rights because it prevents the government from discriminating against persons unless, at minimum, a rational governmental objective exists.[123]

Imagine, for example, that Newark, New Jersey, the city where Nadia was arrested, adopts a practice where it uses FRT to scan criminal suspects. Here's a refresher on Nadia's case: A local Walmart is robbed of over $3,000 worth of merchandise, including a TV, several phones, and a bunch of furniture. Luckily, surveillance footage caught the perpetrator on camera. The officers used the FRT they have on hand to run the footage against the database provided by the app. Unfortunately for Nadia, she has a public Twitter account and often updates her followers with photos of herself. Clearview scrapped one of her photos and included it in the database. The app matches Nadia to the image of the person that robbed Walmart and the officers use this as evidence to obtain an arrest warrant. Nadia is arrested, detained for hours, but eventually let go. Any claim she brings against the government for her wrongful arrest might involve an Equal Protection claim. Under the Equal Protection Clause, "[r]acial and ethnic distinctions of any sort are inherently suspect and thus call for the most exacting examination."[124] When the law is facially neutral, the claimant must show that the policy or law is enforced in a discriminatory manner. This examination requires proving discriminatory effect and discriminatory purpose. Without more than a mere disparate harm, however, it is unlikely a court will see that strict scrutiny, the highest and most difficult level of judicial scrutiny, applies.[125] Even under rational basis review, the government

---

[121] Selinger & Hartzog, *supra* note 80.

[122] U.S. Const. amend. XIV.

[123] Washington v. Davis, 426 U.S. 229, 239 (1976).

[124] Kelsey Y. Santamaria, CONG. RSCH. SERV., R46541, FACIAL RECOGNITION TECHNOLOGY AND LAW ENFORCEMENT: SELECT CONSTITUTIONAL CONSIDERATION 24 (2020) (quoting Univ. of Cal. Regents v. Bakke, 438 U.S. 265, 291 (1978) (plurality opinion)).

[125] United States v. Carolene Prods. Co., 304 U.S. 144, 152 (1938).

will have great difficulty establishing a rational interest in misidentifying certain classes of people.

Nadia might also argue that the law violates a fundamental right to privacy under the Equal Protection Clause. While this right is not unenumerated in the U.S. Constitution, the Supreme Court already recognized the right to privacy as fundamental in *Griswold v. Connecticut*.[126] Having satisfied the question of whether the right is fundamental, Nadia next must prove whether there is an infringement of this fundamental right or whether the policy significantly interferes with the right.[127] Here, the use of FRT to identify suspects infringes on that right both because it has unintended bias consequences against certain classes of people and because it enables the government to easily surveil an individual.

It is important to observe that the typical equal protection framework revolves around human decision-making, while FRT involves mostly algorithmic bias.[128] Due to this, the circumstances which with a court might evaluate such a claim are largely unknown.

D. Ethical Harms

Besides the constitutional harms of FRT, in the hands of both private entities and law enforcement, FRT poses significant ethical harms. Even if they operate correctly, the "right to be let alone" idea, advanced by Warren and Brandeis, is still under threat.[129] Specifically, misuse and abuse by public and private actors can lead to a "shift in phenomenological perspective as dehumanizing because an intrinsic aspect of their person, such as their unique faces that have deep connections to their life experiences, is translated into things that only have instrumental value."[130]

On an individual level, the harms advanced by Evan Selinger and Brenda Leong include a loss of opportunity, economic loss, loss of liberty, and social detriment.[131] The loss of opportunity concerns "informational injuries [mostly] related to employment, insurance, social benefits, housing, [and] education."[132] An example of this is a biased facial scanning system that determines insurance benefit eligibility. Economic loss includes losses

---

[126] Griswold v. Connecticut, 381 U.S. 479, 495 (1965).

[127] Zablocki v. Redhail, 434 U.S. 374, 383 (1978).

[128] *See supra* text accompanying notes 13–20.

[129] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[130] SELINGER & LEONG, *supra* note 8, at 13.

[131] *Id.* at 8.

[132] *Id.*

to "credit, differential pricing, and narrowing of choice."[133] Loss of liberty concerns mostly the "negative effects of surveillance, such as suspicion [and] incarceration."[134] Social detriment is brought on by development of "filter bubbles and confirmation bias, stigmatization of groups leading to dignitary harms and stereotype reinforcement."[135]

Even opting out of participating in certain social media platforms to protect your privacy lends its own set of harms—there is an inherent loss of opportunity, especially during an age where even connecting with work employers through online platforms like LinkedIn are considered the norm. Even so, certain systems can infer information about users that do not participate in these platforms, as evidenced by Clearview's ability to discern a person's identity in the background of a photo they were unaware was taken.[136]

IV. INSUFFICIENCIES IN CURRENT LEGAL FRAMEWORK

Current legal approaches are insufficient address the harms of FRT. This part of the Article will discuss current legal remedies that fall short of addressing the harms of FRT's use by government and private actors. While the Federal Trade Commission has authority to penalize unfair competition and deceptive trade practices, this authority will likely fail to prevent or correct the harms from FRT's use. Likewise, tort law addresses harms after they occur, an approach that can never sufficiently protect individuals harmed by surveillance.

A. Federal Trade Commission (FTC) Lacks the Necessary Authority

The Federal Trade Commission (FTC) was established in 1914 to address unfair competition in commerce.[137] By 1995, the FTC had jurisdiction to prohibit "unfair and deceptive acts or practices" and "unfair methods of competition" against consumers.[138] Section five of the FTC Act, 15 U.S.C. section 45(a)(1) is the primary source of FTC authority; the section authorizes the FTC to protect consumers by "preventing persons, partnerships, or corporations . . . from using . . . acts or practices in or

---

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] *See supra* p. 8.

[137] J. Howard Beasles III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, FTC (May 30, 2003).

[138] F.T.C., PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, REP. TO CONGRESS 10, 3–5 (2000).

affecting commerce."[139] In assessing this, the FTC must consider whether an act or practice: (1) caused consumers, competitors, or other businesses substantial injury; (2) offended public policy as established by statute, the common law, or otherwise; and (3) was immoral, unethical, or unscrupulous.[140]

Some critics of the FTC believe that its investigations are too slow, and that the agency is overall a "[l]ow-[t]ech, [d]efensive, [and] [t]oothless."[141] Other privacy experts believe the FTC is a formidable government authority to address privacy protection. Daniel J. Solove and Woodrow Hartzog believe that the FTC has developed, through a "gradual process" a "federal body of privacy law."[142] They express extreme hope that the future direction of the FTC will move toward focus on consumer expectations.[143] While Solove and Hartzog are correct that the FTC rulings provide the closest thing the U.S. has to comprehensive federal privacy regulations, the fact this process has been "gradual" is exactly why the FTC is an inadequate authority to address FRT harms. The FTC's ex post adjudication necessitates waiting for a harm to occur, conducting a lengthy investigation, and creating rules that only stop that specific company from its harmful practices. It offers guidance, at best, to other companies creating and distributing FRT. Unless the action has the FTC's attention, there is not true oversight. Given the overall unfairness of FRT—*i.e.,* the systemic inaccuracies[144] and ethical harms,[145] slow FTC authority over this matter is not enough of a remedy to address these complex harms. Solove and Hartzog also suggest that a focus on consumer privacy expectations will produce "bolder steps toward developing a thick, meaningful, and broad approach to regulating privacy in the United States."[146] But as mentioned earlier in this article, consumers do not possess the requisite level of comprehension when it comes to FRT.[147]

Recently, in *AMG Capital Management, LLC v. FTC*, the Supreme Court restricted FTC authority to award monetary relief under section

---

[139] 15 U.S.C. § 5.

[140] *Id.*

[141] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600 n.62 (2014) (citing Peter Maass, *Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless*, WIRED (Jun. 28, 2012), http://www.wired.com/threatlevel/2012/06/ftc-fail/all/).

[142] *Id.* at 624.

[143] *Id*.

[144] *See supra* pp. 6–9.

[145] *See supra* pp. 15–17.

[146] Solove & Hartzog, *supra* note 141, at 676.

[147] *See supra* note 112 and accompanying text.

13(b).[148] FTC Chair Rebecca Kelly Slaughter criticized the ruling: "The Supreme Court ruled in favor of scam artists and dishonest corporations, leaving average Americans to pay for illegal behavior."[149] Without this authority, and in the case of FRT's use, people like Nadia or Robert that are misidentified are left alone to deal with the costs accrued from their wrongful arrest and detention.

B. Tort Law Cannot Redress the Harms of Facial Recognition Technology

Privacy torts stem from the initial scholarly analysis advanced by Warren & Brandeis in their paper "The Right to Privacy," but catalogued by Prosser. Privacy torts fall under one of four categories: (1) intrusion into one's private life and affairs; (2) public disclosure of embarrassing private facts; (3) unwanted publicity of private individuals; and (4) misappropriation of a name or likeness for financial advantage.[150] The "right to be left alone," is a right to "one's personality and peace of mind."[151] Prosser's four privacy torts are arguably the backbone of privacy torts today, and the torts with which Nadia and Robert might seek redress under had they gone to court. These torts include: (1) intrusion upon seclusion; (2) public disclosure of embarrassing facts; (3) false light publicity; and (4) appropriation of the others' likeness.[152] While these privacy torts are important and valuable at protecting privacy rights for Americans, they are insufficient to address the complexity of FRT because surveillance by law enforcement and private entities does not fall into any current privacy tort categories.

The first tort, intrusion upon seclusion, involves one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, in a way that is highly offensive to a reasonable person.[153] This tort is not suited to address the harms associated with FRT because it does not address information publicly displayed, like pictures on social media. The tort of public disclosure of private facts is similarly deficient. This tort requires that the tortfeasor publicized certain information about an individual without their

---

[148] AMG Capital Management, LLC v. Federal Trade Commission, 141 S. Ct. 1341, 1344 (2021).

[149] Leah Nylen, '*The Supreme Court Ruled in Favor of Scam Artists,' FTC Chief Says After Gut Agency's Powers*, POLITICO (Apr. 22, 2021), https://www.politico.com/news/2021/04/22/9-0-supreme-court-ruling-guts-ftcs-ability-to-seek-redress-for-consumers-484194.

[150] Warren & Brandeis, *supra* note 129.

[151] *Id.*

[152] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 398–401 (1960).

[153] *Id.*

permission.[154] Like the tort of intrusion upon seclusion, this tort is difficult to apply in the context of public exposure of already public information. The third tort, false light, is also insufficient. This tort involves "a false statement about the plaintiff that affects the way third parties view her, and thereby harms the plaintiff."[155] This tort is still unhelpful at addressing a "widespread broadcast of one's image on online social media platforms."[156] Lastly, for the tort of appropriation, a defendant must show that the voice, likeness or name of the plaintiff was used for a commercial purpose.[157] Zahra Takhshid calls this tort inadequate because "[t]he exposure and spread of images on social media platforms are unlike anything imaginable."[158]

Instead, Takhshid argued for the recognition of a new privacy tort, called the "tort of unwanted broadcasting."[159] This new tort would allow a person whose image was shared without permission to recover damages.[160] For instance, under an unwanted broadcasting tort, a person in Clearview's database can recover damages from the company, but not from the law enforcement officers or private entities that possess and use the photos. This tort is important, but it does not fully address the invasion of FRT and will only hold the company's collecting the photos accountable and not the individual's using the systems. Such a tort still falls short of addressing a grave harm like misidentification mostly due in large part to the constitutional and ethical harms attached. Tort law is designed to make a person whole, but when you have stripped a person of their dignity, misidentified them, and left these inaccurate scans in the database, the remedy lacks real accountability.

The complexity of FRT makes creating an effective tort difficult, largely because privacy torts cannot ever fully repair individuals from the harm of online exposure. Once photos are online there is reason to believe getting the photos back will be difficult—in the case of Clearview, it seems unlikely that if an individual were to bring a tort claim against the company, an injunction against Clearview could reach every party that used the app and accessed these photos. An injunction could stop Clearview from accessing these photos again, but it could never undo the harm associated with the past photos they used.

---

[154] Zahra Takhshid, *Retrievable Images on Social Media Platforms: A Call for a New Privacy Tort*, 68 BUFF. L. REV. 139, 157 (2020).

[155] JOHN C.P. GOLDBERG & BENJAMIN C. ZIPURKSKY, THE OXFORD INTRODUCTIONS TO U.S. LAWS: TORTS 331 (1st ed. 2010).

[156] Takhshid, *supra* note 154, at 158.

[157] *Id*.

[158] *Id* at 157.

[159] *Id.* at 139.

[160] *Id.*

C. The Flaws of Current Proposed Regulations

In June, 2020, two senators[161] and two representatives[162] introduced bicameral legislation to stop government use of facial recognition technology and other biometric technology.[163] The Facial Recognition and Biometric Privacy Moratorium Act asks that leading technology companies pause the sale and development of FRT until the technology has been better studied and the systematic inaccuracies and biases are remedied.[164] Senator Markley remarked that, "facial recognition technology doesn't just pose a threat to our privacy, it physically endangers Black Americans and other minority populations in our country."[165] The bill would also create a Congressional commission to study the technology and correct these racial and gender biases. The proposed legislation also prohibits states or local governments from using federal funds to purchase technology.

Even Amazon has expressed concern over FRT. Amazon's CEO Jeff Bezos announced that the company developed laws to regulate facial recognition technology that it hopes to share with federal lawmakers. The news of this came shortly after Amazon faced public scrutiny over its FRT called Amazon Rekognition. Rekognition allows customers to match photos and videos of people to a database of photos of peoples' faces—this technology, however, is not without fault. As mentioned earlier in this Article, a study from the ACLU found that FRT tested on members of Congress disproportionately misidentified congresspeople of color.[166] Without a completely accurate and unbiased technology, no regulation can sufficiently remedy the potential harms it produces. While some may argue that FRT might reach a time where its accuracy is improved, the technology itself is still invasive with harms still looming in the distance.

---

[161] Senators Edward Markey and Jeff Merkley.

[162] Congresswomen Pramila Jayapal and Ayanna Pressley.

[163] Edward Markey et. al., *Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology*, SENATE.GOV (Jun. 25, 2020), https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology.

[164] *Id.*

[165] *Id.*

[166] *See supra* p. 11; Jason Del Rey, *Jeff Bezos Says Amazon is Writing Its Own Facial Recognition Laws to Pitch to Lawmakers*, VOX RECODE (Sept. 26, 2019), https://www.vox.com/recode/2019/9/25/20884427/jeff-bezos-amazon-facial-recognition-draft-legislation-regulation-rekognition.

V. THE FRAMEWORK THAT WILL SAVE PRIVACY RIGHTS

The ethical and constitutional harms posed by FRT severely outweigh any benefits of its use. Even if algorithms are "fixed" to prevent racial biases or inaccuracies, the threat of constant surveillance by private and government entities will stifle free expression in almost any context. This is because, as put by Evan Selinger and Brenda Leong, "awareness of being watched affects individuals' behaviour regardless of whether they intend any wrongdoing."[167] The greatest harms to free expression will impact people with personalities, conditions, or behaviors that deviate from norms, including minorities, people with disabilities, and even individuals that wish to "challenge the status quo."[168] To summarize, Part III of this article discussed, at length, current legal approaches that can address harms of FRT and why they fall short. These approaches include the FTC's lack of necessary authority, the ex-post nature of tort law, and the flaws in each proposed regulatory legislation advanced by Congress.

A. A Call to Ban Facial Recognition Technology

As a result of all the harms mentioned throughout this Article, Congress should pass a comprehensive federal ban on the use and development of FRT to best ensure the full protection of privacy rights in the United States. Regulations of FRT's use will not effectively safeguard privacy rights, primarily because this technology is oppressive to people of color and women but also because there is still a concern attached to government and private entities using facial identifiers to assess emotions, thoughts, and levels of trustworthiness. There are certain features of our life and identities that are best left private—the "right to be let alone" is widely understood to mean a right to one's personality and peace of mind.[169]

An effective ban will contain three important features: (1) it will prohibit any private or government actor from acquiring, accessing, possessing, developing, or using biometric systems or information derived from these biometric systems;[170] (2) provide a right of action for individuals to sue the federal government or private companies that violate the statute; and (3) require that the National Institute of Science and Technology

---

[167] SELINGER & LEONG, *supra* note 8, at 11.

[168] *Id.*

[169] Warren & Brandeis, *supra* note 129.

[170] The language of this ban was lifted from the San Francisco Ordinance and the proposed federal regulation developed by the Senate. This language effectively addresses the way to prevent misuse and abuse of FRT. SAN FRANCISCO, CAL. ORDINANCES ch. 107–19 (2018).

investigate and appraise whether and to what effect FRT can be made racially neutral. Even if NIST settles that FRT might be bias-free in the future, it is important to note the ethical harms that will never go away. An effective ban will also list the reasons a ban is necessary. To summarize the reasons already discussed in this Article, the ban must address the following: (1) FRT has the tendency to misidentify women, children, people who are transgender, and people of color;[171] (2) FRT is invasive and raises potential First, Fourth, and Fourteenth Amendment violations; and (3) it is dangerous to the progression of a truly "free" society.

The Facial Recognition and Biometric Technology Mortarium Act of 2021[172] provides effective guidance on how to approach a ban on FRT. Important elements of the Act include: (1) a prohibition on the use of facial recognition technology by federal entities, which can be lifted with an act of Congress; (2) a prohibition on the use of facial recognition technologies, including voice recognition, gate recognition, and recognition of other immutable physical characteristics; (3) condition federal grant funding to state and local entities, including law enforcement, on those entities enacting their own moratoria on the use of facial recognition and biometric technology; (4) prohibit the use of information collected via biometric technology in violation of the Act in any judicial proceedings; (5) provide a right of action for individuals whose biometric data is used in violation of the Act and allow for enforcement by state Attorney General; and (6) allow states and localities to enact their own laws regarding the use of facial recognition and biometric technologies.

However, if a later study reveals that an FRT algorithm can be developed without a systemic effect on people of color, people that are transgender, and women, the legal framework might need to change. Instead, firms that develop FRT must prove that the algorithm contains no bias before it enters the market. While bias exists in almost every context of life, relying on racist algorithms to accomplish the intended goals of its development, is inherently unjust because it has the potential to affect an individual in many different ways.[173] Even if firms are to develop software that is racially neutral, concerns over privacy rights generally will remain, making a complete ban still the best resolution.

---

[171] *See supra* pp. 11–14.

[172] Facial Recognition and Biometric Technology Moratorium Act of 2021, H.R. 3907, 117th Cong. (2021).

[173] *See supra* Part I.C.

B. Draft Statute of FRT Ban

The following draft statute combines the key features discussed in the preceding section. It has been modeled after the San Francisco ordinance "Stop Secret Surveillance" passed on May 5, 2019, and the Facial Recognition and Mortarium Act of 2021. A summary of important parts has been provided below:

SECTION 1. Short Title

This Act may be cited as the "Facial Recognition and Other Forms of Harmful Facial Scanning Systems Act of 2021."

SEC 2. DEFINITIONS.

In this Act:

(1) BIOMETRIC SURVEILLANCE SYSTEM – The term "biometric surveillance system" means any computer software that performs facial recognition or other biometric recognition in real time or on a recording or photograph.[174]

(2) FACIAL RECOGNITION – The term "facial recognition" means an automated or semi-automated process that –

(A) assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating surveillance information about an individual based on physical characteristics of the individual's face; or

(B) Logs characteristics of an individual's face, head, or body to infer emotion, associations, activities, or the location of an individual.[175]

SEC. 3 PROHIBITION AGAINST FEDERAL GOVERNMENTS USE OF FACIAL RECOGNITION TECHNOLOGY

(a) IN GENERAL. – Except as otherwise provided in subsection (b), it is unlawful for any Federal agency or Federal official,

---

[174] Facial Recognition and Biometric Technology Moratorium Act of 2021, H.R. 3907, 117th Cong. (2021).

[175] *Id.*

in any capacity, to acquire, possess, access, or use in the United States –

(1) any facial recognition system; or

(2) information derived from a facial recognition system operated by another entity.

(b) EXCEPTION. – The prohibition set forth in subsection (a) does not apply to activities authorized by an Act of Congress.

SEC. 4 PROHIBITION AGAINST PRIVATE ENTITIES USE OF FACIAL RECOGNITION TECHNOLOGY

(a) IN GENERAL – it is unlawful for any entity or individual to acquire, possess, access, or use in the United States –

(1) any facial recognition system; or

(2) information derived from a facial recognition system operated by another entity.

SEC. 5 CAUSE OF ACTION/ENFORCEMENT

(A) IN GENERAL – Violating this Act constitutes an injury to any individual harmed by this Act.

(B) RIGHT TO SUE – An individual described in (A) may introduce proceedings against the Federal Government or entities and individuals who is alleged to have violated this Act in any court of competent jurisdiction.

Other important sections worth including in the statute is the type of relief the plaintiffs might be entitled to, as well as a part that allocated federal funding to investigate the technology by NIST.

C. Implications and Key Considerations

A practical argument against a federal ban is instead instituting a federal mortarium on the use of FRT. This will give the National Institute of Science and Technology the opportunity to investigate facial surveillance technology, establish standards for development and use, and require companies to "fix" algorithms so that they are racially neutral. However, studies on Machine Learning-based Predictive Policing and FRT generally make it clear that it is not easy to eliminate racial disparities embedded in this technology. This is because the machines use data and information from the "real-world" to work. In this way the technology "can learn to discriminate facially on the basis of race because they are exposed and learn from data derived from the racist realities of the United States criminal justice system—a world in which Black Americans are incarcerated in state prisons at a rate that is 5.1 times

the imprisonment of whites."[176]

Baked into this consideration is an argument requiring law enforcement to obtain warrants before using FRT on suspects. If, for example, instead of an officer immediately getting an arrest warrant, perhaps instead the reports from FRT can serve as probable cause to obtain a search warrant. Even with procedures like a warrant requirement in place, Fourth Amendment concerns will not disappear. Calling on law enforcement to simply obtain a warrant before using FRT still requires defining the areas and circumstances that are constitutionally protected and thus necessitate a warrant.[177] Current Fourth Amendment jurisprudence has been criticized by legal scholars as "a one-way ratchet against privacy," and the concern centers around the idea that "as technology continues to enhance government's power to monitor the public square, citizens' expectations of shielding information from the state's view necessarily diminishes."[178] The overwhelming agreement is that even if the Court defines what constitutes a "constitutionally protected area" in terms of FRT, misuse and abuse by law enforcement is still at issue.[179] Additionally, courts cannot ever truly balance privacy interests against police error because the errors in the case of FRT are computer-generated rather than the result of human intervention.[180]

VI. CONCLUSION

This Article demonstrated that the costs of using facial recognition technology do not outweigh the benefits. The need for a federal ban on its use by government and private entities is necessary with increased use and availability of this technology. Facial recognition technology threatens civil liberties and raises First, Fourth, and Fourteenth Amendment concerns. In the hands of private entities, facial recognition technology poses significant ethical challenges for individuals. Current legal frameworks like case-by-case adjudication by the Federal Trade Commission (FTC) raises concerns over proper notice and lengthy investigation time. Similarly, privacy torts only protect rights after-the-fact, and the damage to privacy rights resulting from FRT are irreparable. Regulations on its development and use will not adequately safeguard privacy protections either.

While there are some benefits to using FRT, these benefits are

---

[176] Renata M. O'Donnell, *Challenging Racist Predictive Policing Algorithms Under the Equal Protection Clause*, 94 N.Y.U. L. REV. 544, 547 (2019).

[177] *See supra* pp. 8–11.

[178] Douglas A. Fretty, *Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights in Public Places*, 16 VA. J.L. & TECH. 430, 440 (2011).

[179] *See supra* p. 10.

[180] *See supra* pp. 8–11.

significantly outweighed by its intrusion on privacy rights. Rather, the most viable solution is a federal ban that prevents government entities and companies from accessing, acquiring, possessing, or using facial recognition technology or anything derived from it. An effective statute will also provide a Right of Action so that individuals can hold parties that do not comply accountable. Without a federal ban, the threat of an Orwellian dystopia fettered with constant surveillance and uncertainty will become too real to ignore.