Facial Recognition in Public Safety

How Public Officials Can Ensure This Controversial Technology Is Used For Good

Author: Jamison Mercurio

Advisor: Mihir E. Kshirsagar

CITP Technology Policy Clinic

Introduction:

The goal of this paper is to determine recommendations to government officials regarding the implementation of facial recognition in public safety; specifically examining the areas of data storage, algorithm transparency, and categories of crimes pursued using this groundbreaking technology (abbreviated FRT: Facial Recognition Technology). By creating detailed advice for policymakers, it's our hope that they can use this information when drafting key legislation, as well as to better inform debates and public hearings that may accompany this process. Ethical concerns abound, but as this paper will describe, FRT has many advantages in the field of public safety that simply cannot be cast aside.

One important note: This paper deals with the usage of facial recognition in non-real time. That is, the topics covered will not be dealing with live police body cameras, or FRT's potential for live surveillance usage on public video feeds – both of which involve many other serious ethical issues that must be considered. Instead, this paper's policy recommendations focus on police using FRT to identify criminals after a crime has been committed. For example, using FRT on a store's security camera screenshot of a suspect. Thus, ACLU's recently voiced concerns about live surveillance using FRT – i.e. "People should be free to walk down the street without being watched by the government"[17] does not apply, as this paper is discussing FRT's usage for identifying criminals after the fact.

The current problem that this legislation advice addresses has three key sections. First, decisions on the data used in FRT by government agencies can vary greatly. Many states engaging in the usage of FRT utilize DMV photos. However, there's plenty of other sources at the disposal of police officers. Social media, look-alike photos of celebrities, and even police sketches can be used to try and identify criminals – but accuracy can certainly become the limitation to supporting large scale adoption of such practices. Also, it's not just photos that can be used for facial recognition: It's been proven that identifying people in videos - such as suspects in security camera footage – is much easier through FRT when done with stored, trusted video (rather than through a driver's license picture). Additionally, it's not simply the kind of data that's stored, but who has access to it. At the moment, image data is siloed off among states and regions - with regard to local and state police department usage. Should a centralized, nationwide system exist for such data?

Moreover, algorithm transparency is an essential, yet currently unregulated aspect of FRT in public safety. Local police departments are kept in the dark as to how the FRT of federal agencies operates, only receiving the results of the algorithm rather than seeing the entire identification process at play.[1] This secrecy can also be seen within larger police departments such as the NYPD, who have "resisted efforts to reveal their methods and the details of their searches", and many times will not inform suspects that facial recognition was used in identifying them for arrest.[3] Some may argue that this makes sense – if criminals understand how they're being identified through FRT, they might act to make it more difficult for law enforcement. Yet, "NYPD and other agencies have also used 3D modeling software to fill in missing facial data …this means that a photo showing 60 percent of a suspect's face could be given a 95 percent confidence rating".[10] How can we as Americans regulate these serious lapses and “rounding” in identification that take place in our criminal justice system, when there is no oversight on FRT algorithms?

Finally, we must consider what crimes can be deemed suitable for FRT usage by police departments. There is demonstrated need in small towns for FRT in cases like armed robbery – as interviews with suburban police chiefs has determined that they have no other way of identifying a suspect other than through “manual” facial recognition – i.e. distributing photos of the offenders on social media and asking the public to call in with the person’s name.[1] At the moment, courts have deemed FRT as legal with regard to identifying a suspect in a crime, and specifically for identity theft crimes, although further evidence is needed to convict them.[8] Yet, Americans do have to draw the line somewhere. Many have condemned China’s extensive use of facial recognition for petty crimes such as traffic violations, with nonprofits describing it as creating a paranoid “panopticon effect” that could needlessly instill fear and worry into American’s daily lives.[3]

Police Department Interviews:

In order to understand the issues at play from a police department perspective, I first interviewed two leaders in the Western New York area. Police Chief Shane Krieger is from the small town of East Aurora, New York. Police Captain Jeff Rinaldo leads the City of Buffalo, NY’s Police Department.

Current FRT Usage:

When asked about his experience with FRT, Krieger said the following[1]:

> *Interviewer:* “Does your department look into facial recognition during attempts to gather evidence?”
>
> *Krieger*: “I haven’t looked into using facial recognition. We do not have the resources [for that] right now… I imagine it would require extremely high costs of implementation and maintenance.”
>
> *Interviewer:* “Are there other departments nearby that use [FRT]? Additionally, do you know of any educational programs for local PDs on FRT?
>
> *Krieger:* “I do not know any departments that use [FRT]. I don’t know where I would even start.

We can see from this conversation that the main concern of small police departments is the sheer cost of implementing FRT. In their minds, it requires a significant amount of installation and upkeep costs.

Additionally, I went on to speak with another PD – Police Captain, Jeff Rinaldo.[2]

> *Interviewer:* "Does your department look into facial recognition during attempts to gather evidence?"
>
> *Rinaldo:* "We do not use [FRT] at all currently."
>
> *Interviewer:* "What seems to be the limiting factor here?"
>
> *Rinaldo:* "I see the technology as being in its infancy at the moment. I'm familiar with it, in that I've used it when going through US-Canadian customs before. However, it wouldn't be useful [or] effective for us".

After speaking with this captain, it appears the city's concern is not cost – it's the effectiveness of FRT in identifying suspects, given current police department assets and evidence.

Current PD Tactics for Face-based Suspect Identification:

When confronted with the problem of identifying suspects today, both departments utilize the same general strategy catch criminals. They referred to it as "manual facial recognition, AKA facial recognition, without the technology."[1] As described to me, it has three parts:

1. They post pictures of the suspect on their police department social media platforms (i.e. Facebook, Twitter, Instagram).

2. They send the same photos to the local news organizations and agencies, who then publish them on their own websites, in addition to airing the photos on television.

3. They circulate the picture(s) to numerous local police departments in the Western New York area.

All three of these tactics are entirely reliant on either a member of the public or a fellow police officer recognizing the suspect and calling into the station with the person's identity.

Finally, I was able to obtain an approximate success rate for this technique: <u>40%</u>, according to Jeff Rinaldo.[2]

Why Does Facial Recognition Matter?

We can see that Police Departments are worried about both the effectiveness of facial recognition, in addition to costs of implementation. Let's look at some examples to demonstrate why these concerns are misplaced.

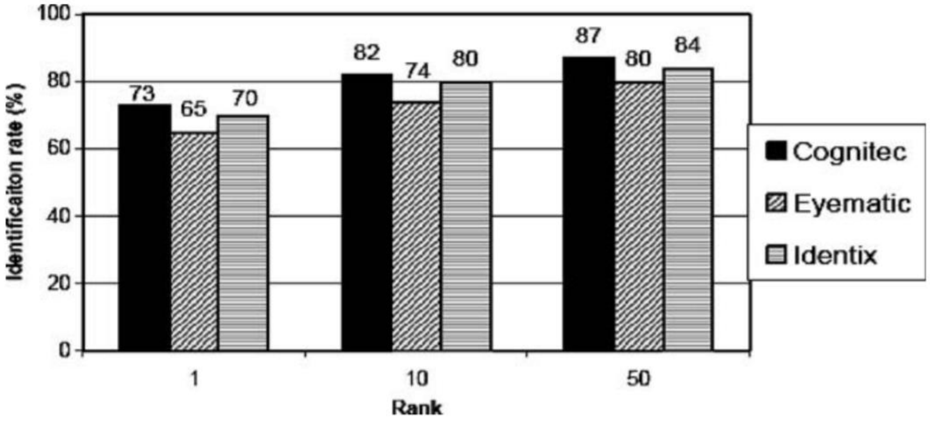
Facial Recognition Works:

In 2017, an investigator in Colorado hit a complete "dead end" in her felony-level theft case at a small-town bowling alley.[3] She had surveillance footage of the thief, but not much else – he had not left any fingerprints, and witnesses could only remember his first name. After months of the case sitting on the shelf, she tries out the department's new Facial Recognition software created by a company called Lumen, and almost immediately finds the culprit. "This is huge" she exclaimed.

Moreover, down in Florida, Pinellas County Sheriffs received a federal grant to test out FRT back in the late 1990s. Since then, Sheriff Bob Gualtieri has described how "the technology has changed policing almost entirely for the better, allowing investigators to identify bank robbers, missing persons, even people who've been killed in car crashes. 'We solve crimes we otherwise wouldn't have solved!' he explained."[3] His descriptions have been part of the reason that major cities including Los Angeles, San Diego, Chicago, and New York adopted this technology.

Furthermore, Maryland Police used FRT to directly to identify and arrest a mass shooter last year.[4] It was initially quite a predicament – they were faced with a suspect who had no identification, was refusing to cooperate, and his fingerprints were not in their database. However, running a photo through Maryland's Image Repository System provided a match, one that they were able to follow up on before arresting the suspect in question.

In fact, there's numeric evidence to back up the capabilities of FRT. According to a study by Lancaster University, facial recognition's indoor success rate was 73%, far and above that 40% "manual facial recognition" statistic from earlier.[6] An experiment cited in this study conveyed how effective the software actually is in practice, displaying the likelihood of the right suspect showing up in the first X search results (called "Rank"), as follows.



The best FRT on the market has its first search result correct about 73% of the time – and if we broaden our search to include the top ten search results, that accuracy rate increases to about 82%. The most shocking aspect of this information, however, is that the experiment was conducted in 2002! Today, Facebook's FRT can hit 97.25% in ideal conditions, while Google's has recently been shown to reach 99.63% accuracy.[7] Certainly, the accuracy of this tech demonstrates its value over current identification techniques.

It’s Cost Effective:

Second, FRT is effective relative to other identification methods for its price. Unlike DNA identification, in which police departments are required to pay a significant fee every time it’s used, Facial Recognition software is usually paid for via a fixed installation cost, and a small monthly subscription. This means that police departments do not have to hesitate to use FRT for a crime – a past problem that Police Chief Krieger mentioned to me regarding DNA testing.[1]

To put this in perspective, in setting up Amazon’s Rekognition software, Washington County spent about $700 to upload its first big haul of photos, and pays about $7 a month for all its searches.[5] Amazon even offers free trials of their Rekognition software. As supported by the press, “Rekognition is easy to activate, requires no major technical infrastructure, and is offered to virtually anyone at bargain-barrel prices.”[5] Prior to this and other modern tech company software, most FRT required the hiring of contractors that charged much more for “building [proprietary] systems.”[5]

Along the same lines, FRT systems are easily sharable. That same Pinellas County Sheriff’s office in Florida shares their system with almost 300 other law enforcement agencies, all through a federal grant.[3] This helps explain why the Georgetown Center for Privacy and Technology demonstrated that “at least one in four police agencies could run facial recognition searches, either through a system they’d purchased themselves or one owned by another agency”.[3]

Policy Recommendation 1: Overcome Misinformation

Educate Police Departments on the benefits and the cost-effectiveness of facial recognition technology. For example, establish training classes for your territory’s police chiefs on how it can be used properly. Based on our research, it’s clear that some PD’s do believe that FRT is either too expensive, or not effective – and neither of these should be reasons why they avoid the usage of facial recognition when apprehending criminals.

More Resources:

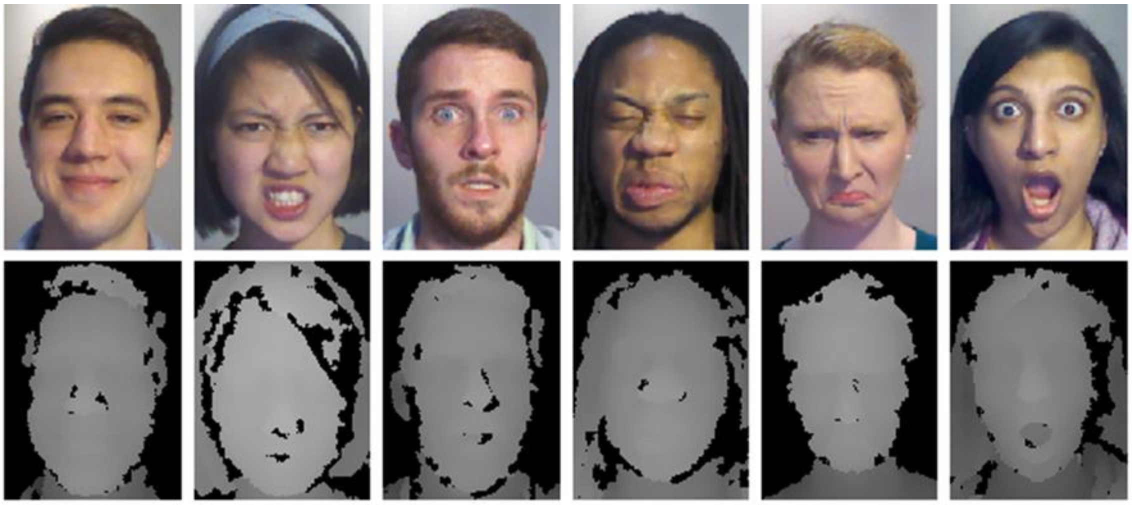
Facebook’s DeepFace FRT Closing the Gap to Human Performance Levels: https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/

Amazon Rekognition Software Pricing Model: https://aws.amazon.com/rekognition/pricing/

How Does Facial Recognition Technology Work?

Facial recognition is a relatively recent technology that allows a computer to take a given image, and using a set of images, return one (or a few) that appears to be a match.

Identifying a Face: It first uses differences in pixel color and intensity in the image to pick out points and edges. Then, the software will use these points and edges to identify features (ex. a nose, an ear, a mouth) that it sees in the images. It also saves geometric measurements – the distance between each of these features. This results in a person's "facial signature".[14]



Aly, S., Trubanova, A., Abbott, A.L., White, S.W., & Youssef, A.E. (2015). VT-KFER: A Kinect-based RGBD+time dataset for spontaneous and non-spontaneous facial expression recognition. *2015 International Conference on Biometrics (ICB)*, 90-97.

The FRT will compute the facial signature of every photo it has in its database. Then, given a photo of a face to search, it compares that photo to each stored facial signature and determines which of them have similar (or identical) facial signatures, before returning a list of results to the user.

Finally, there are a few key terms used throughout the rest of this paper that must be understood:

- A dataset is the set of photos, videos, or other visual data that is used as a baseline by FRT. For example, a dataset could include all of the New York State Department of Motor Vehicles driver's license photos.
- A probe image is the photo that is fed into an FRT system, that the software then compares to its dataset for matches. For example, this could be a screenshot from security camera footage of a bank robber's face.
- A false positive is a situation where the FRT claims that it has a match of a suspect (from the dataset) with the probe image, but it is incorrect.

More Resources:

Norton's Explanation of How FRT Works: https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html

HowToGeek's FRT Explanation: https://www.howtogeek.com/427897/how-does-facial-recognition-work/

Proper Data Storage and System Design:

Our goals for establishing appropriate standards here are threefold. First, the visual data in the FRT database must be effective, in allowing police department FRT systems to accurately identify criminals. Next, the system must be one that is affordable for any city police department, and ideally any local PD within the United States. Finally, and most importantly, the data and system must both abide by the constitutional and civil rights of the American people.

Effective Data:

Choosing the right data involves assessing many potential options. For instance, an FRT database could contain a state's DMV photos. It could contain the nation's DMV photos. It could contain mugshots, or arrest photos. On the other hand, the dataset could include public pictures of people on social media, or even private (think: friends-only) ones.

To determine the right data, we first looked at court cases, and found that DMV photos have been approved by the courts as usable in FRT-powered investigations. For instance, in *NJ v. Alvarez*, authorities ran facial recognition on their NJ DMV database, against itself. This allowed them to catch those who were committing identity theft by having duplicate driver's licenses from NJ, under different names – and the court validated this practice.[8]

Looking at what is currently used by police departments – mainly DMV photos, in addition to mugshots and arrest photos – only confirmed our recommendation. For instance, The NYPD claims to use arrest record photos, and does not "engage in mass or random collection of facial records from NYPD camera systems, the internet, or social media." [12] Other news articles concur that DMV photos are the main source of FRT data in New York, Florida and other states[10].

<u>Policy Recommendation 2: Datasets</u>

Facial Recognition datasets used by police departments should only contain DMV photos and mugshots. These are voluntary and/or arrest-related, therefore, the individual has consented for the government to have access to such pictures. This differs from a person's private social media account, where they have not directly consented to the government's usage of such image data.

Concession: We did interview renowned FRT expert and Princeton Professor Olga Russakovsky, in order to get a better understanding of what effective data looks like on a technical level. Russakovsky informed us that video datasets are better than photographic datasets in identifying a suspect in a video – such as in security camera footage. However, building these datasets is difficult without violating the privacy rights of the American public – as police officers would need to compile public security footage data of every potential suspect (thus, every person in the United States). This could easily lead to mass paranoia and privacy concerns, as seen in China's current implementation of facial recognition – where public security cameras film and identify individuals 24/7.[9]

System Design:

Currently, no centralized database is used by every police department's FRT. In fact, in many cases, police departments only use datasets provided to them by their state or region. For instance, the Washington County Police Department uses hundreds of thousands of photos – but all of them are mugshots from their county jail.[5] In other instances, such as some localities in Colorado and Florida, they only use their state's DMV photos.[3] This means that if a criminal commits a crime out-of-state, authorities are out of luck with regard to using their FRT system to identify the suspect.

Yet, local public safety officers do have one alternative, as described by small-town Police Chief Krieger. They can reach out to federal agencies, such as the FBI, for assistance in using their (the FBI's) FRT software; however, this is seen as time consuming and is not the usual protocol except for extraordinarily serious crimes.[1] It is reminiscent of DNA lab work, where police departments have to significantly limit their usage of such costly testing.

Policy Recommendation 3: Interstate Databases

With that in mind, we recommend that city and state governments combine their DMV, mugshot and arrest record photos into joint databases, thereby increasing the effectiveness of their FRT analysis. It's demonstrably inexpensive and prevents criminals from avoiding FRT identification by committing crimes in other states.

At the same time, locales should lobby the federal government for a centralized, nationwide dataset that will eliminate this issue of lacking the right data. Moreover, a centralized system will likely cost less, as every department can share the costs. Nonetheless, this lobbying process will likely take time, which is why we recommend creating joint-state databases at first. Additionally, combining datasets will result in only one database will be used more consistently, which will assist in the regulation of appropriate photos – as only one source of data needs to be maintained and updated.

More Resources:

China Building an FR Database Using Public Surveillance Data: https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any

Data Privacy Concerns in China: https://www.cnbc.com/2019/09/06/ai-worries-about-the-dangers-of-facial-recognition-growing-in-china.html

Proper Algorithm Transparency:

Algorithm transparency references the way the algorithm works. It includes the searches that are made, the potential results that show up, the probability of a match that the system predicts, and false positives.

Concerning Behavior:

Some police departments have not been informing suspects that FRT was used to catch them, such as the NYPD.[3] In addition to that, local police departments utilizing FRT are not divulging any information about their searches, as they are not required to by any regulatory body or court system[3] - FRT is not commonly used as evidence in court, so the rulings on it are minimal. Finally, federal agencies like the FBI do not reveal how their algorithms or searches work, including when they assist local police departments.[1]

All of this could potentially be explained. Police Departments do not want to reveal exactly how they go about catching criminals, as they want them to be on their toes – always guessing, and never knowing how the police will approach a crime scene. Additionally, as FRT is not commonly used as direct evidence of a person committing a crime (usually, lawyers use the video footage of the suspect, and show it to the court), police departments might not be violating a person's rights if they don't tell suspects they used FRT to find them.

However, in NYC, police have claimed that a suspect "looked like" a celebrity, in order to generate FRT results. This means that they knowingly use photos of other people (celebrities), in order to find potential suspects – leaving open an obvious opportunity for false positives to arise.[10] Moreover, other police agencies have used 3D modeling software to fill in missing facial data.[10] For example, if the surveillance camera picture is blurry/cropped, they will have a computer 'guess' what the person looks like. This additionally can lead to more false positives, as a photo encompassing 60% of a person's face could result in FRT bringing back a '95%' match – a lenience not applied to other identification data like partial fingerprints.[10]

Another common practice is to feed police sketches in as probe images, and investigate the suspects that the FRT returns.[10] However, this practice is entirely dependent on the accuracy of the sketch, which can vary greatly based on the artist and the witness accounts – also contributing to a higher false positive rate.

Policy Recommendation 4: Counter False Positives

Mandate all FR searches require more evidence before an arrest. This is a common policy in PDs that use FRT, but not a requirement. We do not want to violate an innocent person's civil rights and inconvenience them by arresting them solely on the basis of a false positive facial recognition search. Additionally, police officers require "probable cause" to put out an arrest warrant, and FRT-based identification has not had the necessary studies and tests done within the context of public safety to equate to "probable cause", unlike DNA tests or fingerprints for instance.

Amazon Rekognition's documentation recommends this policy as well: "A human should confirm facial recognition software predictions and also ensure that a person's civil rights aren't violated. For example, for any law enforcement use of facial recognition to identify a person of interest in a criminal investigation, law enforcement agents should manually review the match before making any decision to interview or detain the individual. In all cases, facial recognition matches should be viewed in the context of other compelling evidence, and shouldn't be used as the sole determinant for taking action."[11]

Finally, this has been a serious concern for many facial recognition experts, who "worry that a case of mistaken identity by armed deputies could have dangerous implications, threatening privacy and people's lives."[5] By addressing this issue proactively, FRT will become much less controversial in the mainstream.

Policy Recommendation 5: Police Accountability

Require that the actual searches and results be disclosed to a court if FRT was used to catch a suspect. Part of the reason there are not many court rulings on FRT is because it has been kept secret by police departments, and this will also keep police departments accountable. Additionally, as FRT is challenged in courts and improves, it will bring about more transparent algorithms, accountability for tech companies, and could lead to FRT being trusted as true evidence.

Note: I concur with my partner Jordan Heinzel-Nelson that in order to address bias, independent regulatory agencies should also have a hand in testing these algorithms for racial discrimination, in order to prevent a rise of FRT from exacerbating racial tensions in public safety. In her paper, she goes more into detail about what this would look like in practice.

More Resources:

San Francisco Bans Facial Recognition Outright Due to Lack of Limitations on Public Safety Use: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Department of Justice Facial Recognition Best Practices: https://www.bja.gov/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf

Suitable Crimes

Facial recognition could, in theory, be used by local police departments for all crimes. From violent felonies to jaywalking, this technology can be used to analyze evidence of all sorts. However, the goal is to create a safer community, without instilling a sense of paranoia throughout one's constituency. Studies show that the American people have significantly more faith in law enforcement to responsibly handle FRT than advertisers or tech companies.[13] This paper's policy recommendation will aim to retain that trust.

Crime Types Where FRT Is Ubiquitous:

According to police chief interviews and data online, FRT is utilized by local police departments indirectly for serious, violent felonies and other extraordinarily malicious crimes. Local police will reach out to federal agencies with access to FRT, such as the FBI or the CIA, in order to have suspects identified.[2] This occurs especially if the suspect appears to be from out-of-state and "manual" facial recognition does not produce promising results.[1]

Crime Types Where FRT Is Used by Early Adopters:

This is where the main value of FRT lies – in reenergizing serious investigations that currently "couldn't be solved otherwise".[3] For example, thefts in the hundreds of dollars (or even felony-level) are certainly crimes that police would like to pursue if possible – such as that $400 cash theft at a Colorado bowling alley mentioned at the beginning of this paper. Additionally, missing person investigations and criminals who refuse to identify themselves have also been proven to be cases where FRT is considered transformative for public safety.[4]

Crime Types Where FRT Is Controversial

China uses facial recognition for the public shaming of jaywalkers, toilet paper thieves, and others who commit petty crimes or violations, a tactic that many Americans see as 1984-esque[3]. The worldwide condemnation that China has received for employing these tactics (using FRT for all possible violations) means we should draw the line somewhere. Additionally, US government oversight groups also warn of a paranoid "panopticon effect" that overused FRT would create – the sense that the government is all-seeing and omniscient.[3]

Policy Recommendation 6: Appropriate Offenses

At the start, this paper recommends allowing and encouraging the usage of FRT for violent crimes, in addition to felony-level ones - including thefts. As already described, it's clear that FRT will assist in crimes like these, which it already has in Colorado, Maryland, Florida, and NYC. The alternative for many police departments in crimes such as thefts is simply "manual" facial recognition (posting the suspect's picture on social media and local news), which leads to suspect identification only 40% of the time.

On the other hand, there should be some limitations on FRT. For instance, ban the usage of FRT by police for petty crimes, such as misdemeanors and traffic violations. This will curb the amount of criticism that newfound facial recognition usage will create, and protect the rights and privacy concerns of the public – as the American government does not want to become Big Brother.

More Resources:

Maryland Mass Shooter Identified Through FRT: https://www.nbcnews.com/news/crime-courts/suspect-maryland-newspaper-shooting-had-sued-capital-gazette-defamation-n887626

Cities Ask for ACLU Approval before FRT Is Implemented: http://citris-uc.org/wp-content/uploads/2019/09/Facing-the-Future_Ruhrmann_CITRIS-Policy-Lab.pdf

Conclusion:

Certainly, there are plenty of aspects of FRT that must be considered and regulated before it is provided to every police department across the country. Be it the educational training, stored data, the system design, algorithm transparency, or suitable crimes, each sub-field of facial recognition needs defined parameters and requirements. We must balance the public safety value of this technology with protecting Americans' privacy concerns. Some tech companies such as Microsoft are pleading for government intervention[15], while others are refusing to investigate privacy concerns that their technology is inciting.[16] It is up to government entities like your own to regulate this rapidly growing tool, to ensure it is used in ways that positively benefit Americans nationwide.

Citations

1 - Krieger, Shane. East Aurora, NY Police Chief. Interview conducted by Jamie Mercurio on Nov. 14, 2019

2 - Rinaldo, Jeff. Buffalo, NY Police Captain. Interview conducted by Jamie Mercurio on Dec. 7, 2019

3 - Schuppe, Jon. NBC. "How Facial Recognition Became a Routine Policing Tool in America", https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251

4 – Hawkins, Dereck. Independent UK. "How Maryland police Used Facial Recognition to Catch Annapolis Shooter Jarrod Ramos". https://www.independent.co.uk/news/world/americas/annapolis-shooting-maryland-police-facial-recognition-catch-jarrod-ramos-a8427181.html

5 – Harwell, Drew. Washington Post. "Amazon's Facial Recognition Technology is Supercharging Local Police". https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/

6 - Introna, Lucas. *Disclosive Ethics and Information Technology: Disclosing Facial Recognition Systems*. Lancaster University, 2005

7 – Gemalto. "Facial Recognition: Top 7 Trends". https://www.gemalto.com/govt/biometrics/facial-recognition, 5 December 2019.

8 - *NJ. v. Alvarez.* https://casetext.com/case/state-v-alvarez-136, 4 May 2015

9 - Cheng, Evelyn. CNBC. "Chinese Concerns Over Data Privacy" https://www.cnbc.com/2019/09/06/ai-worries-about-the-dangers-of-facial-recognition-growing-in-china.html

10 - Emerson, Sarah. Vice. "Police Are Feeding Celebrity Photos into Facial Recognition Software to Solve Crimes" https://www.vice.com/en_us/article/xwngn3/police-are-feeding-celebrity-photos-into-facial-recognition-software-to-solve-crimes

11 – Amazon Rekognition Documentation: "Use Cases That Involve Public Safety." https://docs.aws.amazon.com/rekognition/latest/dg/considerations-public-safety-use-cases.html

12 – Bosman, Julie. NYT. "Facial Recognition: Dawn of Dystopia, or Just the New Fingerprint?" https://www.nytimes.com/2019/05/18/us/facial-recognition-police.html

13 - PEW Research Center. *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*. https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/

14 - Symanovich, Steve. Norton. "How Does Facial Recognition Work?" https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html

15 – Smith, Brad. Microsoft. “Facial Recognition: It’s Time for Action.” https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

16 – Reuters. New York Post. “Amazon Will Continue Selling Facial Recognition Tech to Government Agencies.” https://nypost.com/2019/05/27/amazon-will-continue-selling-facial-recognition-tech-to-government-agencies/

17 – Associated Press. New York Post. “Amazon Slammed for Selling Facial Recognition Tech to Cops”. https://nypost.com/2018/05/23/amazon-slammed-for-selling-facial-recognition-tech-to-cops/