12-15-2020

# Law Enforcement's Use of Facial Recognition Software in United States Cities

Samantha Jean Wunschel
*Bridgewater State University*

# Law Enforcement's Use of Facial Recognition Software in United State Cities

Samantha Jean Wunschel

Submitted in Partial Completion of the

Requirements for Departmental Honors in Criminal Justice

Bridgewater State University

December 15, 2020

Dr. Jamie Huff, Thesis Advisor

Dr. Emily Brissette, Committee Member

Dr. Michael King, Committee Member

Abstract

Facial recognition software is something we every day, whether it's a suggested tag on our Facebook post or a faster way to unlock our phones. As technology becomes increasingly pervasive in our lives, law enforcement has adapted to utilize the new tools available in accessory to their investigations and the legal process. In a perfect world where facial recognition was reliable one hundred percent of the time, this new software would only face a constitutional and moral debate of when, or whether it can at all be used. Unfortunately, this technology is still fairly new and already there are cases of inaccurate results due to algorithmic errors, amongst other inaccuracies such as the ability to read the faces of certain races, mainly African Americans, less reliably than others. Due to the issues of accuracy and debates around privacy, many cities have opted not to use the technology. There are concerns that facial recognition software may violate individuals' civil rights by providing false positive identifications and leading to wrongful arrests.

This purpose of this research is to analyze cities whose law enforcement departments are using facial recognition software in comparison to those that are not, to trace a pattern of potential dangers of using facial recognition software in the context of law enforcement. The technology is fairly recent so there is not much data on the widespread use or aversion to it. This paper seeks to gather information that is currently available about the use of facial recognition software being used by law enforcement in the United States and compile it into one comprehensive analysis.

*Keywords*: facial recognition software, facial recognition technology, open-source

**Law Enforcement's Use of Facial Recognition Software in United States Cities**

As technology expands and is further developed each year, we are continuously faced with the question of whether it is appropriate, legal or productive for law enforcement to be able to access and make use of these advances. The development of facial recognition software is no exception. Imperfections or flaws with an otherwise promising technological advancement could have dire consequences if they are not corrected before law enforcement utilizes the technology. The work that officers do has a direct and often dramatic impact on the individuals they cross paths with through investigations, inquiries or arrests. As with any tool utilized by law enforcement, there are numerous possibilities for regulating or restricting it in varying degrees. Many cities in the United States have chosen to ban law enforcement's use of the technology entirely, while others have sought to create policies within their police department to outline proper use of the technology. These regulations must be dependent also upon how law enforcement seeks to use facial recognition technology.

The potential applications of facial recognition software's use by police officers range greatly. The technology could be used similarly to a fingerprint scan, where existing image or video captured of someone committing a crime is used to scan through a facial database of mug shots to identify if someone who has previously committed a crime is involved in their current case. It could also be used as a tool of surveillance, verifying a suspect's whereabouts and movement through the use of public and business cameras. It could even be used to find an individual if that same video of someone committing a crime is applied to local public cameras and video feeds rather than a database of mug shots.

Questions of privacy rights will undoubtably arise due to the nature of facial recognition. In order to complete a facial recognition scan there must first be a captured image to try to

match, as well as a database or video to search for a match within. As we move into unchartered technological waters, the choices we make will create a precedent for future advancements. Future privacy and legal decisions about the ways in which city governments and law enforcement departments may seek the use of newly developed technological advances will be based on the policies and laws that are created to restrict or outline proper practices for law enforcement's use of facial recognition software.

In this thesis I will analyze facial recognition software as it is used by law enforcement agencies in the United States. I will examine six cities as case studies, three of which utilize facial recognition software and three that have banned law enforcement's use of facial recognition software. Using these case studies, I will draw a conclusion about the current use or banning of facial recognition software, as well as form a summary of issues that United States law enforcement should consider and prioritize in relation to facial recognition software moving forward. A brief definition of key terms will follow to outline the basic terminology used throughout the course of this thesis.

**Definition of Keywords:**

**Facial recognition software** is used in this paper to reference specific programs used by law enforcement. **Facial recognition technology** is defined in this project as a broader category of facial recognition software, made up of the many facial recognition programs available. Programs that are "**open-source**" publish their source code online for other developers and the general public to see and access. This allows a larger group of individuals to use or suggest changes to be made to the program. Building off of the use of these terms, broader concepts will be explored in the following sections of this thesis.

## Literature Review

### How It Works

Facial recognition software is designed on the principle of face matching. In face matching the subject being tested, whether that be a machine or a human, is presented with two faces at the same time and asked whether they match without relying on the subject's memory at all. This differs from face recognition, where the subject would be presented with one face to learn and then separately shown a series of other faces and asked whether they are the same or not without having the two side by side to compare (Stacchi, Huguenin-Elie, Caldara & Ramon, 2020). A face is made up of several standard identifiers. These help a person, or a computer recognize that what they are seeing is a face in the first place. From there each identifier has a slight variation between different individual's faces. A nose could be long, short, hooked, or upturned. Lips can be full or shallow, close to the nose or far away. Facial recognition software tries to measure these different variations in facial features in order to match one face to another.

Humans have been matching faces for decades in law enforcement. In general humans have a better memory for faces than events and a faster recall for them as well. Facial matching is not something that can be taught or learned with practice, however, there is a percentage of the population that recognizes and can match faces with a greater accuracy than average. In fact, these "'super recognizers' perform at well above normal levels on tests of unfamiliar face matching, with degraded as well as high quality images" (Robertson, Noyes, Dowsett, Jenkins & Burton, 2016).

Each individual facial recognition software's algorithm is likely different, but the basic steps the program follows would be similar to the five steps outlined in the article "How Facial Recognition Systems Work" by Kevin Bonsor and Ryan Johnson. The steps are Detection,

Alignment, Normalization, Representation, and Matching. In the first step the program tries to find something that is a face, looking for the basic shapes and features that it has learned make up a face from its training data. Once it finds a face, it moves on to alignment. This is the process of determining the head's position, size and pose. A face needs to be turned at least thirty-five degrees toward the camera for the software to be able to recognize it as a face (Bonsor & Johnson, 2001). Once the image is aligned properly, an image of the head goes through the process of normalization, where it is rotated and scaled into the proper position to be read and measured by the program. From there the data of the measurements and location of facial features are translated into a unique code. This process is called representation, and it allows the stored facial data and the newly acquired facial data to be compared more easily. The last step is where the matching occurs. During this matching step, the new facial data is compared to the stored data to determine if a match exists.

In some places, law enforcement is already using facial recognition software. In 2018 Department of Public Safety Officials in Utah applied facial recognition software the state's driver licenses databases. Using the technology officials found several state-issued license IDs that were created with false information. These IDs allowed minors to take part in "age restricted activities … and individuals [to apply] for lines of credit with someone else's information" (Salt Lake Tribune 2018). The Chicago police department has entered into a two-year contract with Clearview, a facial recognition software company, to use the software in criminal investigations. The CPD states that the technology is not used for surveillance or "keeping tabs on protestors," but rather it can only be used "in conjunction with an active criminal investigation" (Schuba 2020). In practice, the Chicago police department says that Facial recognition Software allows police to find a lead or narrow down a lead when all that they have to go off of is a photo. Detroit

also uses the technology after passing a policy that only allows "facial recognition to be used on still images of people suspected of violent crimes or home invasion" (Cwiek 2019).

**Flaws in the Technology**

While this software is used by law enforcement across the United States, there are some flaws that have already arisen. One such problem is a result of the "other race" effect. The other race effect is an effect that was recorded throughout psychological research that "indicates that humans recognize the faces of their own race more accurately than faces of other races" (Phillips, Jiang, Narvekar, Ayyad & Otoole, 2010). Statistically, humans struggle to match or compare faces of races other than their own, but they still perform better than computers do with matching or distinguishing faces of other races. Computers preform with the same bias to recognize faces of their native race better than foreign races. These biases are amplified, however, due to the algorithms written into the software. The process for how the computer sees and compares faces, is created by humans and therefore it is possible for biases to be introduced into the code itself. Further, in cases where the software learns what markers make up a face through training data, bias can be introduced if the human supplied training data is not diverse. The software developed in one region may be somewhat reliable in matching faces native to that region, but it is likely that it will not perform as well when faced with a foreign face. This is because the software was developed to recognize features outlined by humans from that region and was likely fed test images of native faces as well.

Facial recognition algorithms can be tested for the other race effect. Algorithms are often given a series of faces as training data. These faces and the races represented in them may allow the algorithm to be better equipped to recognize one race over another in the same way that human infants begin learning faces they frequently encounter, usually their own race, and don't

recognize faces of other races as easily (Phillips, Jiang, Narvekar, Ayyad & Otoole, 2010). As with any new technology or software, there is the probability of human error interfering and causing a technical error in the performance of the software. This is because the software can only make decisions, for example whether a face is the same as the face in another image or not, as well as it is instructed to by the humans creating it. "The engineer that develops an algorithm may program it to focus on facial features that are more easily distinguishable in some races than others" (Garvie, 2016). This could be entirely unintentional on the engineer's part but is nearly unavoidable. Whether the influence comes from the test data fed to the software or from the process it uses to take in the data of each face, there are infinitely many places where human influence on the algorithm could influence it to make a biased decision or to have sub-par performance when attempting to match faces of other races than its native race.

There has been research into the effect of different algorithm's ability to read faces at different angles and in different lighting and weather. There also have been a limited number of studies focusing on an algorithm's performance in its home area versus in other racial areas and settings but testing for the other race effect has not been considered as thoroughly. (Phillips, Jiang, Narvekar, Ayyad & Otoole, 2010).

**Legislation & Interpretation**

Just as facial recognition software is currently developing and growing in use, legislation around the use of facial recognition software and technology is in an equally changing state. One such piece of legislation that is currently in development is the Facial Recognition Technology Warrant Act of 2019. This act has only been introduced and then referred to the Committee on the Judiciary.

***Facial Recognition Technology Warrant Act.***

The Facial Recognition Technology Warrant Act seeks "to limit the use of facial recognition technology by Federal agencies, and for other purposes" (Facial Recognition Technology Warrant Act of 2019). It proposes to do this by requiring law enforcement to gain similar permissions before using facial recognition software in an investigation to what would be required of a physical search, a warrant. If passed, this "rule would apply to any surveillance activities lasting more than 72 hours" (Corrigan 2019). In the language of the bill there are some proposed situations where the law enforcement officers would be able to forgo this requirement as well if they are able to prove probable cause.

In this case the officer could use the software without a search warrant if they determine that there are "exigent circumstances" that would require the use of the software more immediately than obtaining a warrant would allow. In order to use the software, they would also need to determine that a judge would grant a warrant if the officer did present the current circumstance to them. Then the officer would be required to gain a warrant within forty-eight hours in order to "engage in ongoing surveillance" (Facial Recognition Technology Warrant Act of 2019). Ongoing surveillance, according to an article about the bill written by Jack Corrigan in 2019, is defined as circumstances where an individual is surveilled using facial recognition software for more that seventy-two hours either in real time or by digitally going through data that had previously covered more than seventy-two hours.

It is important to consider the repercussions of not having a system in place to limit and regulate law enforcement's use of facial recognition software. While the goal of law enforcement as an establishment has been conceptualized as a means to protect the public, in reality, specific law enforcement agencies may suggest and encourage that the role of law enforcement is to stop

crime and catch "bad guys." The difference is that of a due process or crime control model of policing.

A due process model values the public's rights and privacy as outlined by the constitution by placing limitations on law enforcement and the state in order to keep their powers from becoming excessive. In a due process model, it is most important for law enforcement to follow proper procedure (i.e., Getting warrants and having sufficient evidence to do so) before invading an individual's personal privacy. These procedures create a clear outline for police to follow to protect the public's civil rights. By specifying under what circumstances an officer must get a warrant the court is able to define which police actions would be in violation of the public's rights without a warrant. This ensures that civil rights are respected.

In contrast, a crime control model values just that, controlling and stopping crime. This model is more ought to overstep some privacy boundaries and follow a jump first ask questions later mentality. A crime control model focuses and puts so much value on catching criminals that there is a perspective change that occurs in law enforcement officials. This perspective change between protecting the public, and by extension their rights, or catching law breakers to reduce crime overall, is key. If the role of law enforcement is protection, as it is in a due process model, then it can be assumed that most people are innocent citizens who are to be protected. If the role of law enforcement is to stop wrong doers, as it is in a crime control model, then an officer's job becomes searching for criminals and finding them amongst the public. This means that they may view all individuals as guilty until proven innocent instead of the more appropriate innocent until proven guilty.

This change in mindset is important to keep in mind when considering how facial recognition software could be potentially used by law enforcement officers. There is always the

chance that, while having the right intentions, law enforcement officers my use facial recognition software in a way that does not respect and preserve the rights owed to all citizens as stated by the constitution. In their haste to protect the public from, or to catch, someone that is perceived by officers to be a threat, the rights of that individual could be forgotten. As a society we may be quick to say that we do not care about those who would be categorized as a perceived threat or as having the potential to break laws. It would be wrong to make this assumption, however, because upon considering the types of individuals coming under this scrutiny— political activists, social activists, individuals attending protests— it becomes increasingly likely that you either are, or know someone who is, in one of these categories when it comes to one area of their life or another. In that case you, your friends, your coworkers, or family members may be tracked and surveilled using this technology without any restriction. This would be due to an action, on your part, that you would view as a basic right owed to you as a citizen of the United States.

***A Reasonable Expectation of Privacy.***

Drawing on the well know case of *Katz*, the debate becomes whether we have a reasonable expectation of privacy when it comes to our faces. The supreme court has argued that you cannot expect that your face or person would not be observed within a public space, however, it was decided in the case of *Katz* that "the fourth amendment protects people, not places" (Katz v. United States. (n.d.)). To that end surveillance drones are allowed to record and scan a public area from one hundred feet away. It is not assumed that our faces can reasonably be kept private because of the space we are in, as well as the fact that the details of our appearance are visibly on display wherever we go. Overtime the presence of cameras around us has steadily become a normal part of our daily lives. There are cameras on our phones, in our stores, on our traffic lights, in parking garages, inside and outside of apartment buildings, and in and around

our city government buildings. Facial recognition software has grown out of the new societal norm where cameras record us in our daily movements, for the most part without our notice. This presence creates a wealth of data for technology like facial recognition software to utilize.

While our faces may not be kept private while in public spaces, it is the information that a scan of our faces would supply that is concerning many people. Any passerby may be able to see your face when you're walking down the street. They cannot tell, however, how old you are, where you live, work and go to school. Facial recognition software allows us this possibility when it matches our face to a database of information. "Under Katz, an expectation of privacy is not reasonable if the information at issue was "knowingly expose[d] to the public"" (Hirose, 2017). It might be assumed that this interpretation would protect the public from unknowing scans of their face. The information that would be gleaned from such a scan can be very personal in nature and is not "knowingly exposed to the public" through the act of showing your face in public. This too is allowed and legal, however, because the supreme court argues that the same information that is provided by a facial recognition search could be gleaned by an officer's in-person surveillance of an individual paired with a manual search through database records.

Arguments Supporting warrantless use of facial recognition software compare the technology to a license plate look up. The glaring difference between the two, however, is the nature of the thing being recorded scanned and matched against a database of information. License plates, while publicly displayed are, by nature, meant to identify and record personal information. The owner of the plates knowingly registers them with the government and is aware that their record will be recorded under the plate numbers (Hirose, 2017). Individuals do not self-register their faces with the government in a similar way. They also do not operate under the

assumption that their face carries with it a record of personal information throughout their daily travels in public spaces.

Hirose, writing for the Connecticut Law Review, observes that people may not expect that their appearance and physical actions are kept private when they are in a public space. They do expect, however, that their personal information is kept private. It makes sense that one would assume that personal details such as an individual's address, age, income, and career are kept private when moving about in public spaces. Facial recognition technology, Hirose argues, acts against this expectation of privacy because, when applied to a database of information, a scan and match of an individual's facial features could reveal all this personal information.

***Fundamental Values of Democracy.***

When discussing constitutionality, the when and where of facial recognition software's application matters. Facial recognition software could restrict or interfere with more than one of the fundamental values of democracy as they are protected by the bill of rights. Outside of the fourth amendment, which is largely concerned with investigative searches, some of the fundamental democratic values at risk of being interfered with are freedom of speech in reference to the right to anonymous speech, and freedom of movement. These are integral rights that make up the foundation of our liberties outlined by the United States Constitution. The reason that freedom of speech and the freedom of movement are prioritized so highly is that they not only are important to us on a personal level, but also democratically. These foundational rights allow for us to interact with the government, law enforcement and each other in a way that fundamentally supports civil democratic society. If these rights are ignored or lost, the basic principles of our society will fail and crumble.

Protests throughout Hong Kong of late are plagued by a steady change in policing in their area. "Many protesters now cover their faces, and they fear that the police are using cameras and possibly other tools to single out targets for arrest" (Mozur, 2019). Facial recognition software and video surveillance are being used increasingly in a similar fashion to the way in which these tools are utilized in China. As police have begun to pair this surveillance with the act of concealing their identity as law enforcement agents' tension is rising (Mozur, 2019). Protesters are tracked using video surveillance of protests and activist are tracked down based on this information.

It is not a far reach to imagine that facial recognition software could be misused in the United States similarly. The fear that law enforcement might use facial recognition software to track protesters and activists, like they do in China and have begun to do in Hong Kong, is not unfounded. These countries can be categorized under a crime control model. Law enforcement agencies in the US that do already use facial recognition software use it to track individuals and place them at specific locations at certain times. These actions imply a crime control model as well. Officer's want to keep track of "potential risks" in order to prevent crime. This intention of risk prevention, however, is the very thing that pushes United States policing from a due process model, as intended, to a crime control model.

If we believe that individuals are innocent until proven guilty, then we do not need to keep an eye on people who exercise their freedom of speech. A due process model of policing assumes that these individuals will act appropriately and legally within their rights. In the event that someone does break or cross any laws or legal restrictions police investigation, with or without facial recognition software, may be warranted. The technology has been designed to find individuals based only on their face, so it can easily be used to find and track down individuals

that have been caught on tape at a protest or seen leaving a meeting place or known frequented location of activists or protestors. This kind of usage goes against the very foundation of our rights as citizens of the United States of America as defined in the Constitution's Bill of Rights.

*Right to Anonymous Speech.*

The first Amendment of the Bill of Rights states that "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 the people peaceably to assemble, and to petition the Government for a redress of grievances" (U.S. Const. amend. I). Hirose brings up the concern that the application of facial recognition software on crowds during protests and rallies could interfere with this right. The use of this technology could be used to dissuade individuals from exercising their right to free speech and peaceful assembly (Hirose, 2017).

Their identities, in theory, would be recorded and could be used against them simply by attending to show their support or interest. If a law were to be made allowing law enforcement agencies to use facial recognition software in these instances, it would allow officers to not only know who is in attendance at these events, but also to gather a record of information of the individual were to attend multiple events like this. This data could be used to the ends of building a case against an individual that they are a political radical, when in fact they may only be passionate about a civil rights movement and acting within their legal rights. The officer would also have access to many of the individual's personal details which, if revealed, could cause issues or threaten the individual's career and personal relations.

*Freedom of Movement.*

There is also the potential for facial recognition technology to be applied to public area and used as a tool for mass surveillance by law enforcement. In this way, when tracking a

suspect or just in the gathering of data for a searchable database, it would be possible to create a record of where an individual travels each day, public places they frequent, or a list of individuals entering a certain area. Hirose alludes to the potential for this type of surveillance to impede the free movement of individuals as they would effectively be tailed wherever they traveled, and this data would be accessible at any point in history after its implementation (Hirose, 2017).

## Methods

This project will used mixed social methods common to legal analysis. In particular, the project will primarily rely on case studies of how differing law enforcement institutions use facial recognition technology. Case study methodologies have long been used in qualitative social science projects to analyze law and policy. Case studies "involve the nonstatistical comparative analysis of a small number of cases…the study of two or more instances of a well-specified phenomenon that resemble each other" (George & Bennet, 2005, pg. 151). George and Bennet outline the case study method as a useful way of determining and evaluating the factors that shape legal and policy outcomes.

The cases analyzed in this project will include a total of six cities where facial recognition software's use by law enforcement is either accepted, banned, or a topic of controversy. They are Salt Lake City, New York, Detroit, Somerville, San Francisco, and Cambridge.

Case study methods allow the comparison of policies with attention to their similarities and differences. Drawing from Yin's (2012) *Applications of Case Study Research*, this project will compare eight cases by identifying core factors shaping the development and use of facial recognition technology. Cases will be analyzed for concerns about privacy, false positives, biased

algorithms, and other factors that are of concern for departments considering facial recognition technology.

Data on each case's use of facial recognition software will be obtained from news sources, government documents (when available), and interest group and nonprofit reports on the use of the technology. Many departments do not make their formal facial recognition technology policy information available to the public directly, but information about the use of the technology appears in media reports and reports from relevant non-profit agencies such as the American Civil Liberties Union.

As facial recognition technology is a fairly recent development there is not a wealth of prior research on the topic to draw upon. Facial recognition software and its use by law enforcement is a developing subject and therefore, data is limited and in a nearly constant state of change. This project seeks to compile currently available data as well analyze both theoretical and practical advancements and obstacles as they occur.

## Case Studies

### Salt Lake City

In Utah, Salt Lake City started using facial recognition software in 2008. Before this, "people were able to apply for and obtain a valid, government issued identification card under a false name or birth date" (Wood, 2019). The concern at the time was that this meant that people were able to apply for credit and financing under false credentials and underage minors were able to take part in age-restricted activities. Using facial recognition software, city officials planned to scan the database when an individual applies for a license in order to verify that there are no other licenses given already to that same person. To confirm this, the software would need a photo of the individual applying for the ID and have access to the state's database of licenses to

scan their images and check for a match to the new applicant. If there are no matches the application goes through as usual and the person receives their license following the usual course of action. If there is a match found in the system, however, the application would be rejected thereby preventing citizens from applying for a second license under false credentials.

Using facial recognition software as a new tool also allowed "immigration and law enforcement officials to pore through all Utah driver license photos to identify criminals, witnesses or others of interest" (Wood 2019). The ability to apply facial recognition software on the database of driver's licenses has been the center of dispute for the past few years in Utah. Privacy concerns are the center of this debate as law makers argue that access to the database of driver's licenses effectively puts every registered resident under police scrutiny as a potential criminal without their knowledge or consent. There has been no legislature created to limit or control the way in which officials are permitted to utilize the facial recognition software in the state of Utah.

**New York**

The New York City Police Department has been using facial recognition software since 2011. While no legislation has been created or proposed in the area, the New York City Police Department made the first policy in association with facial recognition technology after almost a decade of using it (Agrawal, 2020). The policy outlines a four-step procedure for New York police officers to follow when using facial recognition software as part of their investigation. The steps are as follows: the investigator submits a request to the Real Time Crime Center, the request is approved, an officer of the Real Time Crime Center runs the image against a database containing only arrest and parole photograph, and finally the officer sends the report to the case investigator. The center compiles and has access to New York State criminal, parole, and

probation records, New York City criminal complaints, emergency calls and summonses, national crime report records and public records. The goal of the Real Time Crime center is to create "a centralized data hub that rapidly mines information from multiple crime databases and disseminates that information to officers in the field" (New York City Global Partners, 2010). Facial recognition software used by the New York Police Department would have access to these databases.

While a policy that seeks to manage law enforcement's use of facial recognition software is a good idea upon inception, there have been some concerns that the procedure outlined by the New York Police Department is not a sound procedure and could be weak to corruption and misuse. Methods of oversight or disciplinary actions for the policy are not outlined in the press release or public records (New York City Police Department, 2020). Critiques have said that facial recognition software has "limited effectiveness" because matches are not always accurate and need to be verified by an officer (Agrawal, 2020).

While method may be better than relying solely on the software, it does not account for human bias. In order to confirm the software's results a human, who is susceptible to biases and human error, must look through the leads offered by the computer. This introduction of human influence could lead to further false identifications or accusations. There also has been speculation that it is not clear who can request to use the can request to use facial recognition software through this process and also that there is unclear phrasing as to the scope of the database, state or city, that officers will have access to (Agrawal, 2020).

**Detroit**

Detroit's law enforcement has been using facial recognition software since 2017 (Rahal & Ferretti, 2017). In September of 2019, Detroit's Board of Public Commissioners voted to

approve an update to their policy for the use of facial recognition software. The Detroit Police Department's previous policy regarding facial recognition software had allowed for more extensive use of the technology, including live scans using facial recognition on public areas in the event of a terrorism threat. Under the new policy, requests to use the technology must be submitted to the Crime Intelligence Unit to be reviewed and either approved or denied (*Detroit P.D. manual,* 2019). The new policy also outlined punishments for officers who misuse the technology. In the new section of Detroit's Police Department manual there is a section titled "Discipline" which states that suspected violations to the facial recognition policy will be reported within twenty-four hours of the violation. The suspected "misuse of facial recognition software will be investigated and reviewed for criminality" and officers found guilty of violating the policy will be dismissed from the Detroit Police Department (*Detroit P.D. manual,* 2019).

Detroit's city council voted to approve a proposal that would renew the city's contract with Dataworks Plus, the company that creates and supplies the facial recognition technology used by Detroit law enforcement, from October 1, 2020 to September 30, 2022 (Ferretti & Rahal, 2020). In the past years, there has been public debate and protest expressing Detroit residents' dissatisfaction with law enforcement's use of facial recognition software. Most recently, was a protest this fall in September of 2020. In this protest "members of the Detroit Will Breathe coalition led a 10-car caravan protest over facial recognition through the city's East English Village neighborhood" (Ferretti & Rahal, 2020). Protesters criticized the racial bias of facial recognition software.

**Somerville**

In Somerville, the tone towards facial recognition technology is equally critical. Residents and city officials worry that the technology's function and abilities are developing at a

faster pace than the public can comprehend. In 2019, the Somerville City Council voted unanimously to ban law enforcement and local government's use of facial recognition software. With this decision, "Somerville became the first community on the East Coast to ban government use of face surveillance technology" (Lannan, 2019). In a Boston Globe article by Sarah Wu, Somerville City Councilor Ben Ewen-Campen mused that many residents of Somerville work in STEM and technology fields and are more familiar with the technology than other cities and communities might be and are more conscious of the need to regulate its use.

Law enforcement officials in Somerville worry that bans on facial recognition technology "could impede police departments' efforts to maintain public safety" (Wu, 2019). Law enforcement officials and police officers are more likely to assume the technology will be used appropriately. This is because, as officers of the law, they do not view themselves as likely to misuse the technology and extend this assumption to all officers.

**Cambridge**

Following Summerville's decision to ban facial recognition software in September of 2020, Cambridge, Massachusetts's "City Council unanimously approved [a] measure, prohibiting any city departments from intentionally accessing or using face recognition technology — as well as any information obtained from such technology" (DeCosta-Klipa, 2020). Amongst the city departments included in the ban was the city's law enforcement department. Prior to this vote, Cambridge officials were permitted to use facial recognition software as long as they had first gained the City Council's approval. City Councilor Marc McGovern pointed to other cities in the United States using facial recognition as evidence that Cambridge should ban the technology (Geller, 2020). Being a more technologically conscious community, Cambridge is also more ought to keep up with the ways in which advances in

technology are being used or misused elsewhere. This is evident as the push to ban facial recognition in Cambridge became more insistent after an example of the technology being misused was clearly seen in the way "the Chinese government [used] it to target protesters in Hong Kong" (Geller, 2020).

Notably, Cambridge City Council officials clearly state that it was not a question of their law enforcement's morals or ability that led to the ban, but rather the examples of facial recognition software being misused elsewhere. The concern in Cambridge is not that their law enforcement will misuse the technology, but that the technology itself has the potential to be flawed. Seeing facial recognition misused in other areas was enough, in this case, for officials to unanimously vote to ban the technology. As of 2019, a poll by the American Civil Liberties Union (ACLU) showed that ninety percent of Massachusetts "voters think the state should regulate government use of face surveillance technology, and 79% support a moratorium until the state does" (Szaniszlo, 2019). Following this logic, Cambridge too seeks to ban facial recognition software in its early phase in response to evidence of flaws in the software and misuse in other areas.

**San Francisco**

San Francisco was the first city in the United States to ban the use of facial recognition software. The act bans city officials and police from using facial recognition technology and also requires any future use of the technology to be approved by the city council (Lee, 2019). Law enforcement officials in San Francisco expressed concerns that the ban will prevent the city from ever using facial recognition, even when the technology is more developed and less flawed. The language in the "ban forbids city departments from buying or using facial-recognition technology for any purpose" (Metz, 2019). The ACLU of Northern California, however, commended San

Francisco on its decision. San Francisco's decision to ban law enforcement's use of facial recognition software was ultimately based upon the failings of several popular facial surveillance systems. In general, facial recognition technology has proven to be inaccurate when attempting to match female or African American faces. The ACLU warns that without some form of structure and oversight, "the technology could easily be misused to surveil immigrants or unfairly target African-Americans or low-income neighborhoods" (Conger, Fausset, & Kovaleski, 2019).

## Analysis & Discussion

### Fundamentals of Facial Recognition

With today's wealth of online knowledge and resources, it is not difficult to find articles detailing the basic principles that facial recognition technology must follow in order to find and determine a match between a given image and a database of faces. This base knowledge can help the general public become more familiar with the technology and its limitations as law enforcement's use of facial recognition software increasingly becomes a topic of discussion in the United States. Overtime, an increased transparency of facial recognition software's accuracy and its blind spots could only improve the public's understanding of what they are agreeing to when they allow their law enforcement to use facial recognition software without regulation.

The way in which future facial recognition technology is developed also will affect the resulting software that is produced. There are currently a series of larger companies developing facial recognition software. There are also a series of free open-source facial recognition programs (Miller 2020). Programs that are "open-source" publish their source code online for other developers and the general public to see and access. This allows a larger group of individuals to use or suggest changes to be made to the program.

One example of an open-source facial recognition software is "OpenFace" (OpenFace – Home, n.d.). OpenFace's website is directly linked to GitHub, allowing anyone with a free account to access and suggest changes to its code. Open-source facial recognition software may benefit from this variety if developers are conscious of the need to minimize racial bias within the system. Being open source would allow a greater number of culturally different individuals to work on the project with ease. In contrast, private companies that do not share their source code will need to concern themselves with diversity in their team as well as in their code.

**Flaws in the Technology & its Algorithms**

The most concerning aspect of facial recognition software is its relatively new age. "Facial recognition technology was first developed in the mid-1960s" (Kahn, 2019). Any technology is bound to have flaws in its first iterations. It is not common, however, for law enforcement to seek use of relatively new technology without proper testing and proof of reliability. "The law, as is usual in the field of privacy and emerging technologies, is lagging behind-no clear set of constitutional rules constrains law enforcement's use of this powerful technology" which, with a lack of testing and oversight, may actually exacerbate the issue and its ability to do harm (Hirose, 2017).

In a brief TED talk, MIT grad student Joy Buolamwini describes her first-hand experience with facial recognition software's shortcomings. Joy first encountered facial recognition when working on an assignment for school. She needed to use technology that recognizes a face in order for her project to work, but when Joy stepped in front of the webcam the software could not detect her face. At first, she simply borrowed one of her friends to help her complete her assignment and assumed that the problem would be fixed by someone else. On a study abroad trip later in her education, however, Joy encountered this problem again. The

same free facial recognition software she had used in her assignment was being used in a demonstration in an entirely different country (Buolamwini, 2016).

That was in 2016, now, in 2020 the same flaws are still a huge problem in facial recognition technology. Seeing these issues with facial recognition software's racial bias in and outside of law enforcement was one of the reasons Cambridge officials decided to ban the technology from the start (Geller, 2020). Facial recognition technology works with up to ninety-nine percent accuracy on Caucasian men. The software has a much harder time recognizing and matching individuals with darker skin and women, being accurate only "up to nearly 35 percent for images of darker skinned women" (Lohr, 2018). The problem could lie in the images used as training data for the software.

Using facial recognition software, computers can learn how to recognize a face based on data that they are fed (Buolamwini, 2016). The computer learns from the images used as training data what traits faces have such as eyes and a nose. This can also mean that a computer can become accustomed to certain features and skin tones if that is the only set of inputs it receives in its training data to the point of not recognizing a face that is made up of features that are different from what it has learned is a "normal" face. This is why a relation between the algorithm's accuracy also has been shown to correlate to whether it is matching a face of the same demographic as the majority of the location where it was developed (Phillips, Jiang, Narvekar, Ayyad & Otoole, 2010) By adding in more culturally diverse faces to training data, the accuracy of facial recognition software may improve.

Improving the accuracy of facial recognition software is an important step towards the software becoming a viable option for United States law enforcement to consider. It would not, however, be the only hurdle to get past. Even if facial recognition software were accurate across

all races and genders, there would still remain the question of how the software is being used by law enforcement. Once accurate, the technology has the potential to be used to target these same groups that it currently cannot accurately match. If facial recognition can be used on racial minorities it could be used as a means to track racial minorities. If police are allowed to use facial recognition software to surveil individuals attending protests or frequenting suspicious areas, what is to stop them from surveilling individuals of a racial minority and the neighborhood they live in? It is important that we are aware of the consequences of any use of facial recognition software by law enforcement as any of the ways we allow the technology to be used may have an impact on citizens privacy and personal rights.

**Law Enforcement's Take**

No matter where you look, law enforcement generally views "facial recognition technology [as] an important tool in solving crime, increasing public safety, and bringing justice for victims" ("NYPD Announces Facial Recognition Policy", 2020). This is apparent not only in cities where facial recognition software is used by police, but also in cities where it is banned. After Cambridge banned facial recognition software, state police spokesman David Procopio spoke about the values of facial recognition software as an investigative tool (Geller, 2020)/

Despite the technology's flaws and potential for misuse, law enforcement seems to believe that the benefits are worth the risk. In San Francisco officers worry that a ban will prevent law enforcement from ever using the technology, even with legislature and oversight conducting their use of the technology (Metz, 2019). In cities where law enforcement has a policy for the use of facial recognition software, officials feel that the technology can do no harm. In a March 2020 press release, the New York City Police Department stressed that "A facial recognition match is merely a lead; it is not probable cause" ("NYPD Announces Facial

Recognition Policy", 2020). This idea is not unique to New York either. The language of Detroit's policy for the use of facial recognition software uses similar language, stating that "the result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT" (*Detroit Police Department Manual.* 2020).

These passages are intended to address the public's concerns with the accuracy of the software. If an individual asks about the repercussions of a false positive match and its potential to lead to the arrest of an innocent individual, the department can point to this clause and reaffirm that facial recognition matches are only used as leads not deciding factors in arrest. While this is better than using facial recognition without any such restrictions, it still doesn't fully address or solve the racial bias issue with facial recognition software. By using a piece of technology knowing that it has a flaw in the form of racial bias, law enforcement sends the message to the tech industry developing facial recognition technology that this is not a fatal flaw. In other words, the developers do not need to prioritize this issue because the company can still sell the product, facial recognition software, in its current form. This behavior could impede the speed at which accuracy amongst different demographics is prioritized and improved as facial recognition software continues to be developed.

Law enforcement's use of facial recognition software in its current state also can lead to a waste of resources on many fronts, even without the added cost to purchase a contract with a facial recognition development company and maintain the software overtime. Funding will also need to be allocated to training individuals to use the technology, and if a separate division will be created strictly for running facial recognition scans this department must be staffed and trained. Resources also would go towards time spent reviewing each request to use the software

as well as to review and verify the results. Further, a false positive might lead investigators down the wrong path, wasting precious time and resources to follow up a lead that proves to be invalid and fruitless.

Even with these precautions, a false positive match may indirectly lead to the arrest of an innocent individual, though the intention was not to do so. In Detroit, a man was arrested and held in jail overnight after a facial recognition search returned his person as a match to a suspect in a larceny investigation (Hill 2020). This account is proof that, even with the intention of using facial recognition matches as a lead, it is possible for police to be led astray by a false match. This opens up the department to liability and gives the impression to citizens that law enforcement trusts an algorithm more than their own investigative skills. When the man in question held up the surveillance camera image that had been deemed a match for his face it was clear that the two were not the same individual. In the time since this story was printed in The New York Times, the county prosecutor has commented saying that he "could have the case and his fingerprint data expunged" from the record (Hill 2020). If police continue to use facial recognition software with its current racial bias, this incident is sure to become a pattern.

Another issue with law enforcement's use of facial recognition software is a lack of government policy to regulate the extent of law enforcement's access and ability to use the technology. New York and Detroit do have policies in place, but not at the state or local government level. The policies in place are, in fact, police department policies put in place by the commissioners of the city's police department. This allows for a greater level of discretion on the part of law enforcement. Police department policies make up a set of protocols for officers to follow. Having policies in place not only makes it easier for officers to know what the correct decision should be when they are under pressure, they also protect the department from lawsuits

by clearly outlining proper procedures ("Four Crucial Law Enforcement Policies", 2020). Law enforcement policies can change overtime as new officials are elected or promoted, effectively rewriting the interpretations of an individual's rights and the extent of personal privacies.

**Legislation & Privacy Concerns**

As technology grows and expands along with our society, new advancements often walk a thin line between helping us and encroaching upon our individual rights and liberties. Facial recognition software is a clear example of this. The potential for the software to do great things, once perfected, ranges from aiding in criminal investigation to predicting whether a person is ill. These benefits also come with an enormous responsibility for us as a democratic country. In order to protect individual rights, specific language must be carefully developed in our policies and laws to limit the freedom of the use of these technological advances in order to increase the freedom of American citizens.

Local bans on facial recognition are a start when it comes to preventing the unregulated use of imperfect software, but they are only temporary fixes to a larger issue. It is important that we develop legislature to tell us how often facial recognition can be used, under what circumstances and in what settings. Today there are cameras in most stores, apartment buildings, and schools and even built into many streetlights as traffic cameras. A question that has not been discussed at length in the forefront of any prior research, is whether law enforcement should be able to access these public spaces through the application of facial recognition software on the recordings of a public space. If public spaces may be used in this way, there is a potential to track individuals throughout their day whether they are in public spaces or not.

Creating clear policies about when the use of facial recognition software is permissible lessens the potential for human error to interfere. Without any restrictions law enforcement is

expected to make decisions about when and where facial recognition scans might be useful and ethical. Proposed laws like the Facial Recognition Technology Warrant Act could lessen the demands and pressure put on officers and police departments to decide, in a case-by-case way, whether facial recognition will infringe upon citizens' rights. Instead, there would be a clearly outlined protocol to detail when and how officers may seek the use of facial recognition software. Local bans will "press pause on face surveillance," but they also put a pause on the development and improvement of facial recognition software as well as halt any attempt for city and state governments to begin the process of creating legislature around facial recognition (ACLU 2020).

The Facial Recognition Technology Warrant Act also would not solve all of the problems facing law enforcement's use of facial recognition software. The language of the bill proposing the Facial Recognition Technology Warrant Act is specific to federal law enforcement. This may create a precedent for states to follow, however, discretion will still be given to individual states when following or choosing not to support this ideal. The bill also only seeks to protect individuals from "ongoing surveillance" and stipulates that it does not seek to limit "instances where facial recognition technology is utilized for a single identification or attempted identification of an individual" as long as the technology is not used to track the individual's movement after being identified (Facial Recognition Technology Warrant Act of 2019). Due to these exceptions the Facial Recognition Technology Warrant Act does not address the issue of false identifications due to racial bias or the kinds of databases or systems that officers should be allowed to search for a match.

Even the very nature of associating facial recognition with the requirement of a warrant for surveillance should call into question every other aspect of the technology's use as well. For

law enforcement to use a tool that can be used in such a multitude of ways, from searching through a database of mug shots to tracking an individual in real time, it should be considered that there is a potential for it to be misused. While law enforcement officials repeatedly assure the public that identification of a suspect through the use of a facial recognition scan will only be treated as a lead not probable cause for arrest, we have seen examples to the contrary. In the case of the Detroit man who was arrested and held overnight the basis of the arrest seemed to revolve around a computer program stating falsely that his face was a 99.9% match for the stranger caught on tape committing a crime (Hill 2020).

**Moving Forward**

Reviewing the compilation of case studies, both of cities that use or have banned law enforcement's use of facial recognition software, it is clear that certain patterns arise. Law enforcement's general attitude towards facial recognition software is hopeful. City law enforcement officers in cities across the country believe that facial recognition software could be a valuable tool to aid in investigations. Whether you're looking at a city like Detroit that uses facial recognition, or Somerville which wants very little to do with the technology at this stage, the public's opinion of facial recognition software seems to be aligned. Concerns about the software's accuracy and ability to wrongfully accuse innocent individuals in police investigations are widespread.

Privacy concerns also exist due to a lack of regulation or restriction of law enforcement's use of facial recognition software. As seen throughout the case studies, facial recognition software has the potential to be used in many different ways from identifying an individual to surveilling them. Because of this malleable potential, it is possible that the software could be used in ways that overstep or infringe upon some of our basic constitutional rights. These rights

are foundational not only to us as citizens of the United States, but also to our country as a democracy. It is important that the many potential uses of facial recognition are considered as laws and policies are developed. Proposed laws like the Facial Recognition Technology Warrant Act seek to limit the duration of law enforcement's use of the technology in each individual investigation, they do not account for they kinds of ways law enforcement may use the technology. It is important to limit the extent of specific applications of the technology such as extended surveillance, however, it is also important to consider which applications of the technology are to be permitted. Can law enforcement run facial recognition scans in public places? Should they be able to apply the technology to protests to identify individual protestors? Questions like these much be explored further before we can accurately codify any proper usage of facial recognition software by law enforcement.

In order for facial recognition software to be more viable for use by law enforcement in the United States we would first need to make a few changes to the things we prioritize. First, the technology must be further developed and tested more extensively. In order to be a useful tool for law enforcement, facial recognition technologies' racial bias needs to be addressed. There is no sense in using a tool that is accurate sometimes for some people, and drastically targets minority groups when it falls short. Furthermore, cities currently using facial recognition software in police investigations should cease using the technology until such a time when testing under various circumstances consistently shows accurate results in matching a diverse cultural demographic of faces.

Finally, and most importantly, cities, states and the country as a whole need to begin to talk more about privacy rights in a world of technology that easily can break down barriers that our country's founders could never have imagined. Until we have proper legislature detailing

how facial recognition software can be used without disregarding or overstepping the bounds of our fundamental rights, using it can only bring more division. Even in a future where facial recognition software can accurately and reliably identify and match faces of all races, it is paramount that restrictions are placed upon law enforcement's use of the technology. Even if facial recognition software was entirely accurate law enforcement would still have the potential to abuse it. Facial recognition software that can positively match the faces of minority groups, could also be used to track these individuals in the same way that police could track protestors.

Facial recognition software is a relatively new technological development. As such, it is something that should be watched and considered as it is further developed, and its usage becomes more widespread. Facial recognition software may be a powerful tool in many industries, but as it is by nature a technology that relies upon cameras, images, and recordings it is important to consider when, where, and how we will allow this technology to be utilized. Law enforcement officers are ideally the guardians and protectors of our country, but they are also human. This fact may be overlooked when new technologies are considered as tools for law enforcement. If all officers are entirely unbiased, unflawed, and never put in a spot where every choice has dramatic consequences, they might be allowed a greater arsenal of technological tools. The reality is, however, that officers of the law are still human. As such, it is highly probable that some are biased, some seek to abuse the system that gives them power, and some simply have different values and morals that deem their actions as honorable when others will see them as invasive.

Because law enforcement is built upon the premise of protecting and serving the public but composed of human actors, the rules and restrictions we place on it as an institution are the only thing that can narrow this chance for abuse and misuse of technological resources such as

facial recognition software. The more rules and restrictions we create to outline the allowed use of facial recognition software, the less choices about its appropriate use are left up to individual states, cities, precincts and individuals. Facial recognition software may be a viable tool for law enforcement, or it may be an unnecessary power with a potential for abuse. It is through these guiding restrictions that we may decide what the proper course of action is for our country in this and future cases of technological advance.

## Tables

Table 1. U.S. Cities Using Facial Recognition Software

| | Salt Lake City | New York | Detroit |
|---|---|---|---|
| Year Adopted | 2008 | 2011 | 2017 |
| Use | driver's license database | Arrest & parole database | Public scans previously, then through request |
| Public Opinion | citizens placed in lineup | Misuse & inaccuracy | Ongoing protests |
| Law/Policy | none | Police Policy | Police Policy |

Table 2. U.S. Cities Banning Facial Recognition Software

| | Somerville | Cambridge | San Francisco |
|---|---|---|---|
| Year Banned | 2019 | 2020 | 2019 |
| Ban | No use by city of law enforcement officials | No use by city departments | No use by law enforcement or city officials, future use needs city council approval |
| Public Opinion | awareness leads to caution | F.R.S. misuse elsewhere leads to caution | Concerned about bias and misuse |
| Law Enforcement | Investigation will be impeded | Not suspected, but not taking a chance | May never be able to use technology in the future |

References

ACLU. (2020, July 02). Press Pause on Face Surveillance. Retrieved from https://www.aclum.org/en/campaigns/press-pause-face-surveillance

Agrawal, A. (2020, March 16). NYPD announces its facial recognition policy. *MEDIANAMA*. Retrieved from https://www.medianama.com/2020/03/223-new-york-police-ffacial-recognition-policy/

Bonsor, K., & Johnson, R. (2001, September 04). How Facial Recognition Systems Work. Retrieved from https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm Conger, K., Fausset, R., & Kovaleski, S. F. (2019, May 14). San Francisco Bans Facial Recognition Technology. The New York Times. Retrieved from https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Corrigan, J. (2019, November 15). Lawmakers Propose Bill Limiting Government's Use of Facial Recognition. Retrieved from https://www.nextgov.com/emerging-tech/2019/11/lawmakers-propose-bill-limiting-governments-use-facial-recognition/161327/

Cwiek, S. (2019, September 19). Detroit police commissioners approve facial recognition policy. Michigan Radio | NPR. Retrieved from https://www.michiganradio.org/post/detroit-police-commissioners-approve-facial-recognition-policy

DeCosta-Klipa, N. (2020, January 14). Cambridge becomes the largest Massachusetts city to ban facial recognition. Retrieved from https://www.boston.com/news/local-news/2020/01/14/cambridge-facial-recognition#:~:text=In a 9-0 vote,information obtained from such technology.

*Detroit Police Department manual*. (2019). Detroit: The Dept.

Engrossed **Bill of Rights**, September 25, 1789; General Records of the United States Government; Record Group 11; National Archives.

Facial Recognition Technology Warrant Act of 2019, S. 2878, 116th Cong. (2019).

Ferretti, C., & Rahal, S. (2020, September 29). Detroit council OKs controversial contract for facial recognition software. *The Detroit News*. Retrieved November 22, 2020, from https://www.detroitnews.com/story/news/local/detroit-city/2020/09/29/detroit-council-vote-facial-recognition/3563440001/

Four Crucial Law Enforcement Policies. (2020, August 21). Retrieved from https://www.powerdms.com/blog/crucial-law-enforcement-policies/

Geller, S. (2020, January 14). Cambridge city council bans face surveillance technology. *Boston Herald*. Retrieved from https://www.bostonherald.com/2020/01/14/cambridge-city-council-bans-face-surveillance-technology/

Hill, K. (2020, June 24). Wrongfully Accused by an Algorithm. The New York Times. Retrieved from https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Hirose, M. (2017). Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology. *The Connecticut Law Review, 49*(5), 1591-1620. Retrieved September 30, 2020.

Kahn, J. (2019, May 23). Facial Recognition. Bloomberg. Retrieved from https://www.bloomberg.com/quicktake/facial-recognition#:~:text=Facial recognition technology was first,intelligence agencies and the military.

Katz v. United States. (n.d.). *Oyez*. Retrieved November 22, 2020, from https://www.oyez.org/cases/1967/35

Lannan, K. (2019, June 28). Somerville Bans Government Use of Facial Recognition Tech - State House News Service. Retrieved from https://www.wbur.org/bostonomix/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech

Lee, D. (2019, May 14). San Francisco is first US city to ban facial recognition. BBC. Retrieved from https://www.bbc.com/news/technology48276660#:~:text=Legislators%20in%20San%20Francisco%20have,transport%20authority%2C%20or%20law%20enforcement.

Lohr, S. (2018, February 9). Facial Recognition Is Accurate, if You're a White Guy. The New York Times. Retrieved from https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

Metz, R. (2019, July 17). Beyond San Francisco, more cities are saying no to facial recognition. *CNN Business*. Retrieved from https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html

Miller, S. (2020, November 24). The Best 8 Free and Open Source Face Detection Software Solutions. Retrieved from https://www.goodfirms.co/blog/best-free-open-source-face-detection-software-solutions

Mozur, P. (2019, July 26). In Hong Kong Protests, Faces Become Weapons. *The New York Times*. Retrieved October 10, 2020, from https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html?referrer=masthead

New York City Global Partners (Comp.). (2010, April 27). *Best Practice: Real Time Crime Center: Centralized Crime Data System*. New York.

New York City Police Department. (2020, March 13). NYPD Announces Facial Recognition Policy [Press release]. Retrieved from https://www1.nyc.gov/site/nypd/news/pr0313/press-release---nypd-facial-recognition-policy#:~:text=The NYPD today announced the Department's facial recognition technology policy.&text=The NYPD has never arrested,lead in the investigative process.

OpenFace- Home. (n.d.). Retrieved from https://cmusatyalab.github.io/openface/

Phillips, P. J., Jiang, F., Narvekar, A., Ayyad, J., & Otoole, A. J. (2010). An other race effect for face recognition algorithms. National Institute Standards and Technology. The University of Texas at Dallas. doi:10.6028/nist.ir.7666

Robertson, D. J., Noyes, E., Dowsett, A. J., Jenkins, R., & Burton, A. M. (2016). Face Recognition by Metropolitan Police Super-Recognisers. Plos One, 11(2). doi:10.1371/journal.pone.0150036

Rahal, S., & Ferretti, C. (2020, June 25). Metro Detroiter battling 'flawed' facial recognition software. *The Detroit News*. Retrieved November 22, 2020, from https://www.detroitnews.com/story/news/local/detroit-city/2020/06/25/wrongfully-accused-detroit-facial-recognition-software-michigan-aclu/3214958001/

Schuba, T. (2020, January 29). CPD using controversial facial recognition program that scans billions of photos from Facebook, other sites. Chicago Sun Times. Retrieved from https://chicago.suntimes.com/crime/2020/1/29/21080729/clearview-ai-facial-recognition-chicago-police-cpd#:~:text=The Chicago Police Department is,so ripe for abuse that

Stacchi, L., Huguenin-Elie, E., Caldara, R., & Ramon, M. (2020). Normative data for two challenging tests of face matching under ecological conditions. Cognitive Research: Principles and Implications, 5(1). doi:10.1186/s41235-019-0205-0

Szaniszlo, M. (2019, June 18). Poll: Nine in 10 Bay Staters say face surveillance should be regulated. *Boston Herald*. Retrieved from https://www.bostonherald.com/2019/06/18/poll-nine-in-10-bay-staters-say-face-surveillance-should-be-regulated/

Wood, B. (2019, November 20). Use of facial recognition software on driver license photos? Utah lawmakers don't like it. The Salt Lake Tribune. Retrieved from https://www.sltrib.com/news/politics/2019/11/20/use-facial-recognition/

Wu, S. (2019, June 28). Somerville City Council passes facial recognition ban - The Boston Globe. Retrieved from https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html

## Further Reading

As this topic continues to grow and develop, the scope of this research could not cover the entirety of more recently occurring case studies and legislation. Provided below is a list of further readings and sources.

An Act establishing a moratorium on face recognition and other remote biometric surveillance Systems, S. 1385, (2020). Retrieved from https://malegislature.gov/Bills/191/S1385

Flanagan, P. (2020, November 30). Face Recognition Vendor Test (FRVT). Retrieved from https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

Harwell, D., & Cox, E. (2020, February 26). ICE has run facial-recognition searches on millions of Maryland drivers. The Washington Post. Retrieved from https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/

IBM abandons 'biased' facial recognition tech. (2020, June 09). Retrieved from https://www.bbc.com/news/technology-52978191

Massachusetts voters strongly support pausing use of unregulated face recognition technology. (2019, June 18). Retrieved from https://www.aclum.org/en/news/massachusetts-voters-strongly-support-pausing-use-unregulated-face-recognition-technology

Passport facial recognition checks fail to work with dark skin. (2019, October 09). Retrieved from https://www.bbc.com/news/technology-49993647

S.B. 218, 2020 Biennium, 2020 Gen. Sess. (UT. 2020). Retrieved from https://le.utah.gov/~2020/bills/static/SB0218.html