Facial Recognition Regulations: A Review of The Current Legal Restrictions Imposed on The Technology's Use in the United States

An Independent Study
Submitted to the Faculty of
The Department of Electrical and Computer Engineering
Villanova University

By

Grace Hamilton

In Partial Fulfillment
Of the Requirements for the Degree of
Bachelor of Science in Computer Engineering

VILLANOVA
UNIVERSITY

April 16, 2021

ACKONOWLEDGEMENTS

Thank you to my advisor, Dr. Richard Perry for the guidance, support, and assistance reviewing this paper during its creation. Additional thanks to Representative Duane Quam of the Minnesota House of Representatives for his swift response clarifying the need for and the text of his proposed facial recognition legislation.

ABSTRACT

Facial Recognition is a new and developing technology whose technical aspects and limitations are not fully understood by the general public and whose future implications for widespread public use are not yet known. This paper explains a concise technical overview of the technology, a brief look into its limitations and real-world implementations, and reports on the currently passed and pending legislation for facial recognition in the United States, both at the federal and state level.

TABLE OF CONTENTS

Chapter 1

Introduction

1.1 WHAT IS FACIAL RECOGNITION

Facial recognition is a computer-based system that takes a photograph of an unknown individual and compares it to photos of known persons, returning the identity of the unknown person to the user. It uses computer algorithms to pick out distinct details on a person's face [1]. These can include the distance between your eyes or the distance from forehead to chin [2]. Using these distinct features, a mathematical formula is run and compared to the results of other photos in a database who have identities matched to them, returning the closest matches [2]. Many systems return several potential matches instead of one guaranteed match [1]. Facial recognition hinges on having a database of known images, or images that already have a known identity associated with them. Thus, when the system returns that an unknown subject closely matches the subject of a photo in its database, the end user will have a name to go with the face.

1.2 SHORTCOMINGS OF FACIAL RECOGNITION TECHNOLOGY

With the ubiquity of crime shows and police dramas on television, it can be difficult to remember that not all modern evidence collection and analysis programs are completely foolproof. Facial recognition technology is chief among them, touting a largely racially and gender biased system favoring white men of European descent. According to a report from the National Institute of Standards and Technology (NIST) of many facial recognition programs developed by a wide variety of companies, the results on people of African nationalities showed some of the highest false match results some more than two orders of magnitude higher than the values for Eastern Europe [3]. The false match results were highest between countries such as Somali and Ethiopia, with the next highest rates occurring between countries such as Ghana, Liberia, and Nigeria in West Africa [3]. These countries do not share borders, so the physical distance separating the citizens of the countries would insinuate a development of more distinct characteristics for each country. This makes the high error rate between those countries slightly more concerning. NIST also found that the false match rate was elevated between West Africa and the Caribbean, West and East Africa, especially West Africa and Kenya, as well as East Asia, giving high false match results both within the countries and between countries in the region [3]. NIST reviewed how the algorithms ran on United States mugshots and found that the rate of false matched results was highest in Americana Indians [3]. The NIST report showed a high rate of false positive matches among groups of people of color, while people of European descent saw a much lower number. This is likely because the datasets used to train the algorithms are biased, underrepresenting people of color and minorities. IJB-A, a

NIST sponsored benchmark for facial recognition hosted a test program that consisted of approximately 80% light skinned individuals [4], a gap that only serves to exacerbate the skewed nature of these algorithms.

In addition to the racial hurdles these facial recognition algorithms must overcome, there exists a sexist element to the recognition as well. The aforementioned NIST report concluded that, during their study of United States mugshots, there was a higher false match result rate in women, especially in Asian and Black women [3]. Overall, women's results were less accurate, but the report noted that the results were particularly less accurate in women of color with high false positive identification rates in Black women [3]. In fact, the same IJB-A dataset is estimated to only be 24.6% female. Gender Shades, a third-party audit that focuses on comparing the results of facial recognition programs between different subgroups such as men and women found that women have an error rate of anywhere from 2.7 to 21 times as large as men [5]. The study focused on existing programs such as those put forth by Microsoft, IBM, and Adience [4]. The independent audit found, as did NIST, that there were higher error rates amongst African countries and much lower in European countries [4].

With studies conducted by both government agencies and in affiliation with accredited universities such as MIT showing that facial recognition technology has major shortcomings that adversely affect already marginalized members of our society, it calls into question a tool used by many law enforcement agencies for investigations as well as private corporations for targeted advertising.

1.3 INVASION OF PRIVACY

One of the key arguments against facial recognition technology is that its ubiquitous use in public spaces is an invasion of our personal privacy. The first step to this assertion is defining what privacy is in a public setting. Is an action private if it is anonymous or is the action private if it is invisible? Addressing the first option, anonymity in our actions would provide a sense of privacy because even if someone knew the action had occurred, there would be no way to trace it to you. Therefore, public actions would be private. The idea of private browsing operates in a similar fashion: using incognito mode on a browser to visit a website will not record the website in your browser's history and will not give the website any information such as accounts that had been logged in and remembered or cookies from previous visits. However, the server hosting the website still registers the connection despite not being able to trace the connection back the user. The browsing session is anonymous, and thus private. Assuming the definition of privacy in a public space is anonymity, facial recognition violates that expected privacy. With automatic facial recognition, anyone on film in a public area can be easily identified, meaning no anonymity in public and no assumption of privacy. However, privacy can also be argued to be invisibility instead of anonymity. Invisibility assumes that the action cannot be seen, and therefore cannot be attributed to any individual, offering that individual privacy. Privacy by invisibility in public spaces is common, for example bathroom stalls and private dining rooms, which are technically publicly available spaces that can be occupied by an individual or individuals whose actions are then unseen and private. Assuming this definition of privacy is implemented, facial recognition technology also violates the assumed privacy of the public space. For facial recognition to work, images must exist to be fed into the neural network. If images exist of the person performing the action, the action is no longer invisible, and

the expectation of privacy is violated. No matter which way a person defines privacy, facial recognition technology violates the expectations.

While the concepts of anonymity and invisibility apply well to public ventures such as leaving one's house, they don't transfer as well to platforms like social media. Here, our names and images are publicly displayed and linked to our identities, making it impossible to go unseen or unknown. Therefore, what expectations of privacy, if any, can we expect from these platforms? There can be some expectation of privacy with private profiles, or profiles on public sites whose content can only be viewed by those we allow to view them. This practice does not always protect our names and profile pictures from being viewed publicly, but rather the content posted to individual profiles, so the private mode is not infallible. Should any unauthorized user gain access to a private profile, whether intentionally or unknowingly, the expectation of privacy has been violated. The photo scraping practices performed by facial recognition app Clearview AI blatantly violated the terms of service of companies such as LinkedIn [6] and Facebook [7]. Scraping images from these sites to form a database of photos is against the terms of service and violates the expected and allowed use of these platforms. The use of photos scraped from these sites is a violation of the expectation of privacy the public has in these public forums, and therefore contributes to the issue of facial recognition invading expected privacies.

Chapter 2

LAW ENFORCEMENT USE

2.1 Potential Benefits

Facial recognition technology can offer many benefits for law enforcement. Traditionally, police work, if they were lucky, could turn up a photo of a suspect on a security camera or a witness who could provide a description for a sketch artist. This image would then be distributed to the public in the hopes someone would see the face and recognize the person and call the investigators to identify them. Using facial recognition, law enforcement can take any clear image gleaned during an investigation and determine the identity of the individual, or at the very least, several of the most likely identity matches. This cuts down on time, allows police to play key information close to the vest during an investigation, and offers investigators more plentiful and solid leads when searching for a perpetrator.

2.2 Facial Recognition Failures

However, as previously discussed, even something as potentially useful as facial recognition can have its pitfalls. In a quote attributed to Benjamin Franklin, “It is better that one hundred guilty persons go free than one innocent man should suffer.” If facial recognition can cause innocent people to pay for the crimes of the guilty, it is a flawed tool that should not be relied upon by law enforcement. Facial recognition’s aforementioned shortcomings have caused problems with false identifications of suspects, a situation which disproportionally affects minorities and can cause serious issues for the people misidentified as perpetrators of a crime they had nothing to do with.

2.2.1 Robert Julian-Borchak Williams

In January of 2019, Robert Julian-Borchak Williams was contacted by the Detroit Police to turn himself in, since he had a felony warrant out in connection to a larceny case [8]. Assuming it was a joke, Williams returned home, where the police arrived and promptly arrested him in front of his family [8]. He was brought in as a suspect in a robbery of a local upscale boutique in which approximately $3,800 of goods had been stolen [8]. He informed the police that he hadn’t been to the store in question since approximately 2014 [8]. Williams had been brought in due to a faulty facial recognition match on surveillance footage from the crime scene made by DataWorks Plus, a service that offers a range of products to law enforcement spanning from iris scanning to inmate tracking to digital crime scene evidence management [9]. Williams expressed to the police interrogators that he looked nothing like the man in the photo. Even despite this, he was only released after posting $1,000 bond [8]. This arrest and Williams’ time in jail broke a four-year streak of perfect attendance at his job [8]. It was later discovered that a private Instagram post could account for Williams’ whereabouts at the time of the crime [8].

2.2.2 Michael Oliver

In July of 2019, Michael Oliver was driving near his home in Michigan when he was pulled over by police [10]. After being informed that there was a felony warrant out for his arrest, Oliver was taken into custody [10]. He had been identified as the suspect in a larceny case by a facial recognition program called DataWorks Plus [10]. His photo was matched with a single screen from a cell phone video from an eyewitness [10]. However, when his case was presented before a judge, even the judge agreed that the photograph did not resemble Oliver [10]. The suspect in the photo even lacked the easily identifiable neck tattoos that Oliver had [10]. The case was thrown out. This false accusation, however, was catastrophic for Oliver's life. After missing numerous days of work for court dates, Oliver lost his job. Without a job to pay for home or car payments, he eventually lost both as well [10].

2.2.3 Nijeer Parks

In January of 2019, police were called to the Hampton Inn of Woodbridge, NJ to deal with a shoplifting claim. When they arrived, police were directed to a man dealing with a rental car contract in the hotel lobby who had been accused of taking snacks from the hotel gift shop without paying [11]. The man apologized to police and gave officers a driver's license that turned out to be a false identification card. The officers claimed to have a seen a plastic bag full of suspected marijuana on the man's person. The suspect made a run for it, hitting a police car as he drove off [11].

The following month, Nijeer Parks was taken into custody on the charges relating to the incident [11]. Parks had also been misidentified by a facial recognition program and falsely accused. Parks spent 10 days in jail and spent $5,000 in defense fees despite having been 30 miles away at the time of the incident in Haledon, NJ with bank records to confirm it [11]. Finally, in November of 2019, the case was dismissed for lack of evidence [11].

Chapter 3

FEDERAL LAW

3.1Policies and Hearings

At the federal level, no current legislation exists to govern facial recognition, save the ideas of privacy introduced by the Fourth Amendment. In May of 2019, the Congressional Committee on Oversight held a hearing on the topic of facial recognition, with several expert witnesses testifying before the committee and offering insights on legislative measures [12]. The tone of the witness testimony was overwhelmingly critical of facial recognition. Joy Buolamwini, founder of the Algorithmic Justice League called on Congress to enact a moratorium on facial recognition due to its threats to civil liberties and its propensity to cause negative outcomes for already marginalized groups [12]. Professor Andrew Gunthrie Ferguson studies big data and its interactions with the freedoms guaranteed to use by the Fourth Amendment [12]. He implored Congress to implement regulations now, since the world of mass surveillance is changing so rapidly that dealing with privacy issues on a case by case basis will be insufficient to protect citizen's rights. Ferguson states that the Fourth Amendment alone will not stand up to the challenges posed by facial recognition [12]. Neema Singh Guliani, a representative for the American Civil Liberties Union, called for the committee to take steps to stop facial recognition use by law and immigration enforcement, ensure that the FBI and ICE are publishing the information on how they use facial recognition, and to investigate private companies that sell facial recognition for law enforcement use [12]. Clare Garvie of the Center on Privacy and Technology at Georgetown Law warned that facial recognition gives law enforcement power they've never before wielded, and that power is flawed and a threat to due process [12].

The Congressional Research Service, a group who researches topics relating to potential legislation and reports factual findings to Congress to inform their policy making, released a report on facial recognition on October 27th, 2020 [13]. The group reported that the full extent and frequency of facial recognition use by federal law enforcement is unknown [13]. The FBI engages in two main facial recognition programs: Next General Identification-Interstate Photo System (NGI-IPS), which supports state and local law enforcement, and Facial Analysis, Comparison, and Evaluation Services Unit (FACE), which supports FBI investigations [13]. In general, the two programs do not provide a one-to-one match, but rather a gallery of suspects to facilitate investigations [13]. NGI-IPS mainly compares photographs from an investigation to a database of criminal mugshots, however the search can be extended to facial images collected for non-criminal background checks performed by the FBI [13]. The results returned from a search of those databases typically takes the form of a gallery of 2-50 individuals [13]. Those results are only returned to trained individuals, are not conveyed as positive identification, and are not suitable cause for an arrest [13]. FACE Services Unit runs facial recognition against both NGI-IPS accessible databases and federal databases [13]. Department of Homeland Security uses the service to run facial recognition on people entering and leaving the country [13]. Through the Traveler Verification Service (TVS), facial recognition is used by Customs and Border Patrol and the Transportation Security

Authority at 27 airports, 7 seaports, and 5 boarder locations in the United States [13]. While US citizens may opt out, currently images of 60% of departing foreign nationals aged 14-79 are captured for the program, as well as 20% incoming [13]. CBP's goal is to capture 97% of travelers by 2022 [13]. The FBI claims to audit the systems regularly and report that none of their audits have found noncompliance with their guidelines [13]. The FBI is also required to share information on facial recognition systems through public reports [13].

The study also looked at how the technology is viewed by the American public. Just over half of Americans reported trusting law enforcement to use facial recognition responsibly, and having more trust in law enforcement use of the tech than in private company use [13]. Older, white Americans tended to have more trust in law enforcement than other demographics [13]. The study encouraged policy makers to consider how gender, race and age may play into community-police relations with the use of facial recognition, as well as the accuracy and interpretation of results, restrictions for law enforcement, and privacy and security concerns [13].

The Federal Trade Commission, or FTC, published guidelines for the commercial use of facial recognition. The FTC encourages companies to design their systems with consumer privacy in mind, as well as develop security protections for the personal information they keep as well as public retention policies for the data [14]. Companies should consider the sensitivity of the situation when implementing facial recognition, with the example given being that it should not be implemented in a place where children congregate [14]. Under these guidelines, consumers should have little trouble opting out of facial recognition programs, and for those who opt in, companies should not use biometric data differently than they said they would [14]. The FTC has even handled a public settlement with a company employing facial recognition services over misuse and misrepresentation of the services. In January of 2021, Everalbum, a cloud photo storing application, introduced a "Friends" feature that would run facial recognition on user's photos to allow the user to tag their friends in photos and help group photos together [15]. This feature was automatically enabled for all users except those in the European Union, Texas, Illinois, and Washington state, where laws protect against the collection of biometric data without consent [15]. Everalbum was accused of lying about the retention of photos of deactivated accounts, as well as using user photos to develop models and algorithms to better their facial recognition systems [15]. Furthermore, it was alleged that the company used the photos not just for their "Friends" feature, but also for facial recognition services sold to enterprise customers [15]. As part of the settlement, Everalbum must delete any photos from deactivated accounts, as well as the models and algorithms created which used data that was collected without consent [15].

3.2 Pending Legislation

While there is no current law on the books for regulations at the federal level, there are a few proposed and pending bills in Congress that attempt to tackle the issue. Senate Bill 4084, titled the Facial Recognition and Biometric Technology Moratorium Act of 2020, proposes a ban on biometric surveillance systems unless an act of congress authorizes its specific use, as well as banning any use of information gained by such systems in federal investigations [16]. The bill was proposed June 25th, 2020 and referred to committee. An earlier bill introduced in November 2019, Senate Bill 2878, otherwise known as the Facial Recognition Technology Warrant Act of 2019, forbids federal agencies from using

ongoing facial recognition based surveillance without a court order as well as outlines the requirements that must be met in order to issue such a court order [17].

Even before these two bills were proposed to attempt to introduce regulations on law enforcement use of the technology, Congress introduced the Commercial Facial Recognition Privacy Act of 2019 in March of that year [18]. The bill would prohibit private entities keeping or using facial recognition data unless they both provide documentation on the limitations and capabilities of the facial recognition system and obtain explicit consent from the end user [18]. The data that such entities would be able to collect would not be allowed to be used for discrimination, unreasonable uses outside of the uses specified when consent was gained from the user, sharing data with third parties, or conditioning the use of a product with consent from the end user [18].

As of the writing of this paper, all of these proposed bills remain in committee.

Chapter 4

STATE LAWS

Despite the lack of federal regulations on the technology, some states have implemented their own regulations. States such as Illinois, Texas, and Washington have law currently on the books placing restrictions on commercial use of facial recognition. Despite only three notable examples of facial recognition legislation on the state level, many states have come to see the importance of learning about and implementing proper use procedures for this growing, powerful technology. Most states have proposed bills working their way through committee to either restrict or deny law enforcement use of facial recognition systems, as well as restrictions on commercial entities using the technology for financial gain at the expense of the privacy of state citizens.

4.1 Alabama

In February of 2021, Senate Bill 113 was proposed to the Alabama state senate. The bill outlined a policy that prohibits state or local law enforcement from using facial recognition, with a few exceptions, and would forbid a facial recognition match from being sufficient probable cause for arrest [19]. This sort of bill would be a key step in limiting law enforcement dependence on the technology and would have been able to prevent arrests of misidentified innocent people without further investigation and probable cause.

4.2 Alaska

Alaska's Senate Bill 98 was passed in March 2012 and presents restrictions on the collection of biometric data. It requires that individuals be notified before collecting their biometric data and that the collectors expressly disclose how that data will be used [20]. The individual must give their consent for the collection, which can then be revoked at any time [20]. Exempt from these restrictions are law enforcement biometric data collection and biometric data collected in state licensing databases [20].

4.3 Arizona

Arizona's House Bill 2478 proposed a limit on collecting biometric data, requiring that a person must be notified and give consent before their data is collected [21]. Unfortunately, the bill died back in 2019 [21].

4.4 California

California has had several different anti-facial recognition initiatives. In May of 2019, San Francisco placed a ban on facial recognition use by city agencies [22]. Later that year, in July, Oakland's city council voted unanimously to uphold a similar ban for their city agencies [22]. Both cities have been cited as positive examples in other legislative proposals from other states across the country. California state government voted in October of 2019 to place a 3-year moratorium on facial recognition use on police body cameras, which went into effect January of 2020 [22].

4.5 Colorado

Colorado's Senate Bill 132 was introduced to the senate on February 26, 2021 [23]. The bill seeks to ban "digital communications" platforms from using users' personal identifying data with facial recognition software and allows users who have had their data fed through facial recognition software without consent an avenue to sue [23]. If passed, the bill would go into effect January 1, 2022 [23]. Colorado's law would be a government enforced backing to many currently existing policies employed in big tech company's terms of service, which already limits the ways in which those platforms can use a user's submitted image. Having a law enacted to take strides to protect users who choose to use such digital communications platform can set a precedence and help to protect users of future digital communications platforms who may not see the need to enforce those sorts of policies upon themselves.

4.6 Connecticut

Connecticut has two examples of proposed regulations on commercial use of facial recognition. House Bill 5326 is considered dead in the chamber as of March 30, 2016. Had it been passed, it would have outlined specific guidelines and requirements for businesses that employ facial recognition software on their premises on exactly how to notify the public that a system that captures biometric identifiers is being used in the area [24]. House Bill 5333, which prohibits retailers from using facial recognition for marketing purposes at all, died in January of 2019 [25]. Both bills make an effort to restrict flagrant use of facial recognition by private businesses on an unsuspecting public, however, unfortunately, neither made any real headway.

4.7 Delaware

Delaware is one of the many states that allows the Federal Bureau of Investigations access to its state driver's license database for federal facial recognition requests [26]. Senator Chris Coons, a United States Senator from Delaware, introduced a bipartisan bill to the United States Senate in 2019 that would require that the FBI needed a warrant, and therefore probable cause before asking the state for access to its photo database for facial recognition searches [27].

4.8 Florida

Florida has very little restriction on facial recognition and openly allows its law enforcement to utilize it as an investigative tool. In fact, in Pinellas County sits the headquarters for the state facial recognition operations, which started almost 21 years ago [28]. The system is reported to be queried thousands of times a month but rarely offers the officers solid leads, since surveillance imagery is often not clear enough for facial recognition to work properly [28]. Despite not having much restriction, as of 2018 a Florida Court of Appeals was found to be one of the first courts to make a facial recognition-based evidence ruling. One Willie Allen Lynch was accused of being "Midnight", a crack-cocaine dealer, after being identified as the suspect by facial recognition [29]. Lynch requested the other potential matches put forth by the recognition system be brought in as evidence to throw doubt on the case against him, however the court denied his request, claiming the evidence was "not relevant." [29] The Court of Appeals upheld the ruling saying that Lynch could not bring them as evidence because he could not prove the photos that he did not have access to resembled him, and therefore would not have cast any doubt on the case [29]. Facial recognition matches, as previously discussed, are often not accurate. Should facial recognition matches be allowed in the courtroom as evidence, then any other potential matches the system returned should also be allowed in. These other matches would help the jury understand that facial recognition is not infallible and would not paint the system's identification of the defendant as irrefutable proof of guilt.

4.9 Hawaii

A proposed bill in Hawaii's House, HB 1126, moved to forbid Hawaii government agencies from using facial recognition technology except in the instance of a photographic lineup, comparing mugshots or driver's licenses to surveillance photos, or for contact tracing in the event of a disease outbreak [30]. These government agencies would also be prohibited from using information gained from facial recognition systems except in the established exceptions [30]. The bill was deferred as of February 5th, 2021 [30]. In the bill's introductory section, worries about facial recognition abuse were clearly outlined, citing the issues arising from Nijeer Parks' case, the increased misidentification of Blacks, Asians, and Native Americans by facial recognition software, and went so far as to liken widespread facial recognition to carrying an ID at all times along with a mandatory GPS tracking system, calling it an "unacceptable violation of privacy." [30]

4.10 Idaho

Idaho's H0492 was referred to committee February 12, 2020. The bill proposed a requirement that facial recognition software must be open to third party testing [31]. Any entity running facial recognition on a publicly accessible premises would be required to notify people that it is being employed and must get consent before "enrolling an image or a facial template of that individual in any facial recognition software [31]." The bill would also prevent facial recognition results from being used to block people from accessing financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, healthcare services, and necessities such as food and water [31]. It further prevents law enforcement from using the technology without a warrant and gives individuals the right to request their image removed from a facial recognition system [31]. If passed, the bill would apply

to any legal entity that conducts business in Idaho or that provides products or services to Idaho residents [31]. The prevention of using facial recognition for blocking access to critical institutions is a key portion of this bill that would take steps to reduce the potential negative effects of an incorrect facial recognition match, especially on a person of a marginalized community who might rely on some of those key institutions for their day to day needs.

4.11 Illinois

Illinois has enacted one of the more famous American facial recognition regulations called the Biometric Information Privacy Act. BIPA is, in essence, the same as many other states proposed bills in that it forbids any private entity from collecting a person's biometric information without first informing them, in writing, of its collection and then receiving written consent from the individual for the collection [32]. It further prohibits the sale or dissemination of this biometric data [32]. One notable deviation from several other regulatory measures proposed in other states it that it does not stop biometric data from being introduced as evidence in court, opening the door for facial recognition matches to be allowed in as evidence [32]. The act was drafted and passed due to a concern for the privacy of Illinois citizens. In the event of a data breach, biometric data cannot be changed like a password, and the full ramifications of biometric technology are not yet fully understood [32].

4.12 Indiana

Indiana currently allows the use of facial recognition and even has a specific department dedicated to assisting law enforcement with facial recognition search requests. The Indiana Intelligence Fusion Center (IIFC) handles law enforcement's use of the technology and has a clearly defined public policy on its uses. IIFC stresses that a facial recognition is to be regarded by investigators only as a lead and not as a positive identification of a suspect [33]. Furthermore, the IIFC assures the public that face recognition is not used on live or recorded video, and not used on body cameras worn by police officers [33].

The Indiana House did propose a bill, HB1238, that would require law enforcement to be open and clear with the public on their implementation of new technology for surveillance [34]. The bill would have required police departments to develop a publicly accessible policy before deploying new technologies and would have required the departments to have been open about data retention with the new systems, who has access to said data, internal audits on the systems, and what specialized training is required for their operation [34]. Unfortunately, the bill died in committee in early January 2020 [34]. The requirements that this law would impose on law enforcement in Indiana are things that should already be publicly available information. One of the simplest ways to build trust between a government agency and the people it polices is honesty and transparency. Hiding the use of surveillance tech, especially controversial tech, causes those agencies to lose credibility and face with the people it swore to protect and serve.

4.13 Iowa

Iowa's law enforcement agencies, as of 2013, had been allowed to use facial recognition for several years. The Department of Transportation began allowing state photo ID photos to be used for recognition searches beginning in 2008 [35]. Iowa is also one of the states that allows federal law enforcement access to state photo databases [35]. Iowa does stipulate that a facial recognition result is not probable cause for an arrest or a search warrant [35].

4.14 Kansas

Kansas's Senate Bill 361 from its 2018 session is a bill that would require police officers to wear and operate body cameras when responding to calls, notify a person if the camera is recording, and that would prevent the use of facial recognition on body camera footage without a warrant [36].

4.15 Kentucky

Kentucky is one more state which allows federal access to state photo databases for facial recognition searches. Kentucky not only shares this access with the FBI, but is also reported to have shared access with ICE [37]. Kentucky's proposed Senate Bill 280, which in late February 2021 went to the Senate Judiciary for review, would put limits on both government and private entities in relation to the tech [38]. The bill would require warrants for government agencies to use facial recognition or to use any information gained through the technique, while also allowing the technology to be used in the search for missing persons or children [38]. The bill would also require a warrant for federal law enforcement looking to access state photo IDs [38]. Any law enforcement that does gain a warrant to use facial recognition would find that that information would be barred from being used as evidence before any court or authority under this bill [38]. Private companies are also addressed in the bill, which would require a public policy and retention schedule for the private organization's biometric databases, as well as mandating that they inform individuals when they collect biometric data and receive consent for its collection [38]. Those companies would be banned from selling or releasing that information and fined for violations of the policy [38].

4.16 Louisiana

House Bill 662, which was referred to committee on March 9, 2021, seeks to add some checks to the use of facial recognition in the state [39]. The bill requires human review before making final decisions on facial recognition results, as well as preventing facial recognition result information from denying access to crucial institutions, similar to Idaho H0492 [39]. The bill also requires disclosure statements from facial recognition software companies about the realistic capabilities of their software and outright bans facial recognition for discrimination [39]. Finally, the bill would require notices on premises that use facial recognition and requires a warrant for its use by government agencies [39].

4.17 Maine

On March 18th, 2020, Maine enacted "An Act To Amend Certain Motor Vehicle Laws", which allowed the Secretary of State to use facial recognition to give information to law enforcement only in the event of an extreme emergency involving an immediate threat to life and generally prohibited the use at all other times [40].

4.18 Maryland

In late January 2021, Maryland legislature proposed two laws, House Bill 23 and Senate Bill 234, which had the same goal in mind: to forbid facial recognition on state photo ID databases at both the state and federal level for matters relating to immigration [41, 42]. The laws also require the managers of those databases to record and report annually to the state government both the number and nature of federal access requests to state photo databases [41, 42]. This implies Maryland is another state that allows federal access to state databases for facial recognition searches. The bill would also limit access to those databases only to their owners and to law enforcement [41,42].

4.19 Massachusetts

Somerville, MA took it upon themselves to enact legislation to regulate facial recognition within their city. The Somerville City Council, amidst worries of racial inequalities and massive tracking and surveillance by government, moved to ban facial recognition in police investigations and municipal surveillance programs [43]. The vote carried 11-0 in June of 2019. The Massachusetts ACLU publicly supported the move [43].

The rest of the state has not enacted similar laws as of yet. In fact, in December of 2021, Massachusetts passed a police reform bill that allowed facial recognition in cases where people "face a substantial risk to harm." [44] More recently, Massachusetts Senate Bill 1383 attempted to extend the Somerville moratorium to other state government agencies, with the exception of cases of "statutory authorization." [45] The proposed bill did not define "statutory authorization", and stated that until it is defined, facial recognition is not admissible in court [45]. The bill was proposed out of concern for civil rights issues and threats to personal liberties posed by facial recognition, however the committee has taken no further action as of January 5th, 2021 [45].

4.20 Michigan

Michigan allows law enforcement to use facial recognition and has since 2001 [46]. Michigan even has SNAP, the State Network of Agency Photos, which is a central location of digital images for searches [46]. Michigan does limit its use slightly in that it does not allow use on real time video and is not supposed to be considered a positive identification, but rather only an investigative lead [46]. Despite not allowing the technology to be used on real time video, Detroit has allegedly had the capability to monitor real time video since 2019 [47]. Project Green Light, which is a network of cameras across the city at nearly 700 locations as of April 2020, provides real time video feeds that could be used for facial

recognition if the policy were to change [48]. As of 2019, the camera feeds were no longer allowed to be used for facial recognition or issues relating to immigration [48].

4.21 Minnesota

HF 240 is a bill introduced to the Minnesota House January 21st, 2021 that outlines facial recognition use during the application process for a Minnesota State driver's license [49]. The bill would require facial recognition to be run on any individual applying for a driver's license to ensure that the individual is not applying under a false name or applying for multiple licenses [49]. The bill outlines that, should a match be returned, it will undergo human review. If confirmed, the individual will not be dispensed a driver's license until the match is invalidated [49]. The match is sent to law enforcement. If human review by the "appropriate law enforcement agency" also confirms the match, the matter may be referred for criminal prosecution [49]. The bill does not yet offer an alternative means of proving that an identification is false if a false match should occur. Additionally, the bill allows the individual to be checked against photographs in databases of ID photos and criminal law enforcement databases such as mugshots [49].

4.22 Mississippi

In August of 2020, the Jackson Police Department was reported to have been banned from using facial recognition by the city council, who voted 4-2 in favor of the ban [50]. The ban was proposed amidst concerns of privacy and in the interest of placing limits on government tracking of civilians [50].

4.23 Nebraska

Nebraska Bill 1091 would have banned facial recognition or information gathered as a result of facial recognition from being admissible evidence in court [51]. The bill received support from the Nebraska ACLU, however the committee took no immediate action on the bill, which still has not been passed [51].

4.24 New Hampshire

Introduced on January 11, 2021, House Bill 499 sought to limit facial recognition use by law enforcement to only in cases where they had obtained a warrant, as well as forbidding facial recognition evidence from being admissible in court if the information was unlawfully gained or if the warrant is shown to have been issued for insufficient reasons [52]. If the facial recognition evidence was obtained legally and in good faith, the evidence would stand in court [52]. As of March 5, 2021, committee reports say that the bill ought to pass with an amendment [52].

4.25 New Jersey

In early 2020, Clearview AI, a commercial facial recognition company that offers its services to numerous law enforcement agencies, published a video advertisement that featured an image of New Jersey State Attorney General Gurbir S Grewal [53]. Clearview AI claimed that its services had been used to assist in a police sting operation [53]. Attorney General Grewal barred the use of Clearview AI's technology by New Jersey police amidst worries of the integrity of their investigations and pledged to investigate which departments had, up until that point, been using facial recognition applications [53]. The New Jersey state legislature then took measures further than simply investigating the use of the technology but proposed several bills to help regulate it.

New Jersey Bill A5974 was introduced and referred to committee June 1, 2020 [54]. The bill would prohibit law enforcement use of facial recognition without approval from the Attorney General's office [54]. The Attorney General would, in turn, have to notify the general public about its use [54]. The bill would also force any department currently using the technology to hold a public hearing about its use [54]. Senate Bill 1916, introduced and referred to committee February 25th, 2020, held most of the same stipulations, including that public hearings must be held on the matter before implementing new facial recognition systems by departments [55].

Other bills introduced during this time period include Senate Bill 1917 (sent to committee February 25th, 2020), which prohibited the use of facial recognition on police body camera footage [56]. Additionally, bill A4211, introduced in June of 2020 and combined with A3625 in January of 2021, would prevent law enforcement from using biometric surveillance systems as well as establishing a biometric surveillance regulation commission to examine and propose legislature [57]. Bill A989 would mandate the testing and auditing of the five most commonly available facial recognition systems for biases and report those findings back to the legislature [58]. Finally, the most drastic bill from the influx of proposed legislation was Senate Bill 116, which cited facial recognition as a threat to civil rights and liberties and proposed a ban on its use by government agencies [59]. None of these legislative measures have passed as of the writing of this paper.

4.26 New Mexico

New Mexico also shares driver's license photographs with the FBI for their facial recognition program [60]. Albuquerque, however, requires probable cause for arrest be shown before allowing the use of facial recognition in a case [60]. Police departments in both Las Cruces and Albuquerque, New Mexico employed Rekognition, Amazon's facial recognition service [61]. However, in response to the Black Lives Matter movement in 2020, Amazon suspended its service for a year [61].

4.27 New York

New York has had several bills introduced during its 2021 session relating to facial recognition regulation. Assembly Bill A03759, sent to committee on January 28th, 2021, and Senate Bill S03234 are dual bills referred to as the "Facial Recognition Technology Study Act", which is proposed to allow for the study of privacy concerns and development of regulatory approaches to the development and use of facial recognition technology [62, 63]. Assembly Bill 05492, sent to committee February 19th, 2021, and

Senate Bill 00079, sent to committee January 6th, 2021, both propose to ban biometric surveillance by law enforcement [64, 65]. The bills further establish a biometric surveillance regulation task force [64,65]. Bills A01601 and S01076, sent to committee early 2021, prohibit facial recognition on officer body camera footage at both the state and local level [66, 67]. Assembly Bill A00768 was referred to governmental operations January 2021 and would prohibit biometric identification such as facial recognition from being probable cause for arrest [68]. A04916 tackles a broader issue, proposing a ban on state agencies or state government contractors from retaining facial recognition images without court approval [69].

Outside of law enforcement regulations, Assembly Bill A04352 and Senate Bill 00073, both in committee as of the writing of this paper, would ban facial recognition use by landlords on residential premises [70, 71]. Additionally A00954 and S00893 would prohibit biometric identifying technology in schools until mid-2022 at the earliest [72, 73].

4.28 North Dakota

North Dakota is another state that allows the Federal Bureau of Investigations to access state photograph databases for facial recognition searches [74].

4.29 Ohio

Ohio is a state that allows the FBI access to their driver's licenses databases [75]. In August of 2019, Ohio cut off access to the facial recognition program using driver's license photos until further training is provided to those accessing it [75]. A review of their facial recognition program showed that the Hamilton County Sheriff's Office made the most requests to the system, with Ohio Homeland Security coming in second [75]. Ohio Attorney General David Yost sponsored a review of the system and reported no misuse of the law enforcement facial recognition system [76]. The review showed that federal requests made up 3.8% of searches between January 1 2017 and July 31 2019, and that of the Ohio law enforcement, only 17% have access to make facial recognition requests [76].

4.30 Oregon

Oregon's state senate has seen two separate facial recognition legislative proposals during the 2021 session. The first, Senate Bill 309, proposed banning facial recognition use by state agencies altogether, including information gathered using facial recognition systems, save in a few specific circumstances [77]. This could include allowing facial recognition for accessing state issued electronic devices (think FaceID for IPhones) or automatic face detection for purposes of social media applications or facial redaction from images for privacy purposes [77]. The second bill, Senate Bill 310, was introduced January 2021 and proposes similar regulations on private entities, banning facial recognition use except in device access procedures such as FaceID [78]. The bill leaves the door open, upon review and revision, for the Bureau of Labor to have input on what limits should exist for private entities [78].

4.31 Rhode Island

Rhode Island has two current bills proposed in both the House and the Senate, both proposing a ban on law enforcement at the state or federal level using facial recognition in Rhode Island jurisdiction for matters of immigration [79, 80]. Senate Bill 0253 was referred to the Senate Judiciary February 10th, 2021 and House Bill 5652 was scheduled to be heard March 17th, 2021, on which date the Committee recommended the bill be held pending further study [79, 80].

4.32 South Carolina

South Carolina's House Bill 3918 was referred to the Committee on Judiciary February 18, 2021 [81]. If passed, the bill would prohibit the use of facial recognition technology on footage from a police officer's body camera and would make any surveillance information gathered in violation of the bill inadmissible in court [81]. This bill would be a terrific step in the right direction helping to improve the quality of facial recognition. If it is used at all, the software should only be used on high quality, distinct images. Body camera footage is often grainy and unclear and should not be used as a source for reliable facial recognition results.

4.33 Texas

Texas' famous CUBI bill, found in the Commerce Code Title 11 Subtitle A Chapter 503, forbids the capturing of biometric data without informing the individual first and receiving that individual's consent [82]. CUBI also requires that stored biometric data be shared with law enforcement if they present a warrant, stresses that the biometric database managers are responsible for protecting the sensitive information, and mandates that employers get rid of biometric data about their employees upon said employees termination with the company [82].

4.34 Utah

Utah has two bills in the 2021 session that deal with facial recognition. House Bill 0250, known as the Uniform Driver's License Act, considers a facial recognition match "satisfactory evidence of identity," potentially setting a precedent for faith in the technology later down the road [83]. Senate Bill 0034, however, would seek to limit facial recognition's use to felonies, violent crimes, assisting in situations with a threat to human life, or identifying someone who is already dead [84]. Facial recognition search requests would also be required in writing and must be performed by a trained government employee, and, should the case go to trial, any information gained from facial recognition searches must be disclosed as such to the prosecutor [84]. Like other states, the Utah bill would prevent the technology from being used for civil immigration violations [84]. SB 0034's draft was prepared March 9th, 2021 and has not yet been passed [84].

4.35 Vermont

Vermont's House Bill 75 tackles commercial facial recognition. If passed, it would not allow facial recognition use on an individual unless that individual opts in [85]. Furthermore, facial recognition would only be allowed for product development, not for marketing purposes [85]. Any biometric data kept on file must be deleted after 21 days, and companies must disclose when they are using facial recognition in public spaces [85]. The bill was read and referred to committee on January 14th, 2021 [85].

In the law enforcement vein, House Bill 195, which was referred to committee March 12th, 2021, would propose that, starting July 2021, facial recognition be allowed on images of victims, potential victims, or suspects in cases of sexual exploitation, sexual assault, homicide, or kidnapping of minors [86].

4.36 Virginia

Virginia's recently proposed House Bill 2031 would forbid the use of facial recognition on public college campuses starting July 1, 2021, with select exceptions [87]. The bill was put to the house January 20th, 2021.

4.37 Washington

Washington state currently has enacted a law, RCW 19.375.020, that requires notice or consent to collect a biological identifier to place in a database for a commercial purpose, or a mechanism to remove any biological identifier from said database [88]. The Washington state also introduced a bill, Senate Bill 5104, on January 11th, 2021 that proposes a moratorium on facial recognition by government agencies [89]. The moratorium would end July 2026 and wouldn't penalize accidental use of information gained from facial recognition [88]. The bill also states that the information would be admissible in court and does not apply to facial recognition done by the licensing department [89]. The bill also would set up a joint legislative task force that would review and research facial recognition technology, document potential abuses of the technology, and provide recommendations for legislation to the senate by the end of September 2021 and would be disbanded by January 2022 [89]. The task force would consist of members from the house and senate, representatives from advocacy organizations to represent minorities that may be affected by the technology, members of law enforcement, facial recognition company representatives, and facial recognition researchers [89].

4.38 Wyoming

Passed and signed into law on February 9th, 2021, Washington's recent facial recognition law considers facial recognition as a means of "identity proofing", in which a third party can provide a notarial officer with verification of a person's identity [90].

Chapter 5

CURRENT LAWSUITS

5.1 ACLU vs. Louisiana State Police

The Louisiana American Civil Liberties Union (ACLU) is suing the Louisiana State Police department for a release of their documentation on police use of facial recognition technology during police investigations [91]. The Louisiana ACLU filed an earlier request that was denied, saying the requested documents such as staff training documents for use of facial recognition technologies, analysis of results and facial recognition programs, and communications regarding the use of the technology either were not maintained as records or were not subject to the public record [91]. A second request to the Louisiana State Police yielded the release of approximately 50 pages of email communications detailing requests for use of facial recognition technology as a potential lead in an ongoing investigation [92]. The released emails also outline a policy for the use of facial recognition technology by the police department and even shows an example of an image being rejected because key facial features were obscured and therefore not suitable for use in recognition [92].

The Louisiana ACLU claims the technology should not be utilized by the police department because of its racially biased nature [91] and hopes this effort to uncover the official documentation for public consumption will spark a movement against the use of facial recognition. However, a further issue with the Louisiana State Police's use of the tech is the fact that its use has been hidden from the public. The New Orleans Chief Technology Officer claimed that in 2020, the city does not employ any sort of facial recognition technology [93], while the ACLU had discovered and were working to make public the state police's use of facial recognition back in 2019 [92]. When the fact of its use came to light, it was claimed the program was only used in "violent cases." [93] Despite this claim, no clear numbers were provided on exactly how many of those "violent cases" actually employed facial recognition to help identify a suspect [93]. The lack of transparency with the public regarding police use of a technology that infringed on the privacy of US citizens should be a cause for concern.

5.2 Tech Giants Violate Illinois Privacy Law

Two Illinois residents, Steven Vance and Tim Janecyk, filed a class action lawsuit in response to finding their images in a database of images produced by IBM called Diversity of Faces [94]. The pair claim that the database containing their faces directly violates Illinois' BIPA act, protecting Illinois residents from having their biometric data collected and stored without their consent. Large tech companies such as Microsoft and Amazon use the database to train and develop their facial recognition programs [94]. The case is not without precedence, as Facebook was also forced to pay out $550 million dollars to settle an earlier BIPA case [94].

BIPA act is a law that clearly outlines the rights to privacy that citizens have in relation to biometric data. Widespread facial recognition is a major violation of privacy that can only work if the facial

recognition data of a large pool of people is collected and used. This can be easy to collect without consent, especially if it is argued that facial recognition data is not biometric and not protected under laws such as BIPA. However, as a result of the prior Facebook case, a US Circuit Court of Appeals ruled to confirm facial recognition data as biometric data and thus subject to the privacy protections of BIPA [94]. The BIPA suits are a key indicator to the public that big tech will exploit data if given the chance, and unless held accountable to government regulation, will not respect the privacy and bodily autonomy of US citizens.

5.3 Nijeer Parks

Another recently filed lawsuit is that of Nijeer Parks, one of the three wrongfully arrested men discussed earlier. Parks, in his filed complaint against the Woodbridge, NJ police department, detailed his own account of the events that led up to and then proceeded his wrongful arrest. Parks claimed to have received a phone call about the warrant out for his arrest, after which he willingly went to the Woodbridge police department to clear up what he presumed to be a simple misunderstanding [95]. Upon arrival, Parks was detained for questioning regarding a crime he did not commit. Parks asserted to police that prior to coming to the station, he had never been to Woodbridge and didn't even know where it was [95]. Furthermore, Parks pointed out that he did not and never previously had a driver's license, and in fact was brought to the station by his cousin [95]. The perpetrator was seen renting a car at the hotel in question and drove away after the incident. Parks was even able to provide a solid alibi at the time of the interview [95]. Nevertheless, based solely on a faulty facial recognition result, the Woodbridge police had Parks arrested, where he spent the first week in "functional solitary confinement [95]." At the time of his first day in court, Parks' complaint alleges that the Woodbridge police knew by that point neither his DNA nor his fingerprints matched those found at the scene [95] . Therefore, the only evidence that the police had to go on was the facial recognition match. Parks' complaint alleges that the police action taken against him was unjustified and he is seeking damages from the police department for his pain and suffering.

In this case, facial recognition was used as a tool to violate a person's basic freedoms with no other evidence. This case outlines how dangerous a blind faith in this technology can be. As previously addressed, the technology is flawed and biased, specifically against people of color, and thus cannot be used as the sole reason for arrest. This is especially true in a case such as Nijeer Parks', where all the other evidence including a solid alibi for the time of the crime pointed to Parks' being the wrong suspect.

Chapter 6

CLEARVIEW AI

Clearview AI is a growing tech company run by CEO and co-founder Hoan Ton-That [96]. The company offers an application, accessible by phone or web, to run facial recognition to determine the identity of the subject of an uploaded photo. The company claims to have over 600 law enforcement agencies across the United States as clients [96]. The company also boasts one of the largest existing facial recognition databases, claiming to have over 3 billion photos amassed [96]. Ton-That collected these photos by scraping them from major websites across the internet, including Facebook, Twitter, and Youtube [98]. Clearview also retains the photos submitted to it by clients for recognition requests, so its database is ever growing [98].

The app differs from the existing facial recognition programs available to law enforcement not only due to the size of its database, but also due to the fact that officers can upload non-standard photots (full, unimpeded photographs of the individual's face, typically front facing) and still receive matches [98]. Indiana State Police claimed the app help solve one of their cases in minutes when they uploaded a photo of the suspect, who had no driver's license or mugshot on record and would otherwise have been inaccessible to normal databases [98]. The company allegedly has also toyed with developing their app to run in real time on augmented reality glasses, like a technology from a dystopian science fiction film.

The app works by uploading a photo of an individual to the app. The neural network behind the scenes takes the photo and checks it against Clearview's database searching for a match. When the match is returned, the results are labeled with how sure the neural network is that the results are accurate [99]. Clearview AI boasts an unverified 98.6% accuracy rate, meaning that if the algorithm returns a match, the odds of it being a false positive are very low [99]. The company claims that the results are merely indicative and not a definitive identification, and that Clearview AI is not designed or intended to be used as evidence in a court proceeding [99].

Clearview AI itself has continuously declined to provide a list of its clients to the public [98]. Despite this, leaked documents picked up by BuzzFeedNews provided a list of numerous clients in both law enforcement at the state and federal level, as well as private companies. Federal agencies named as users by the leak include ICE, DoJ, FBI, CBP, DHS, Secret Service, DEA, Bureau of Alcohol, Tobacco, Firearms, and Explosives and the criminal investigative division of the US Marshalls [100]. Many state and local police departments were also named as users of the app [100]. In addition to law enforcement, many non-law enforcement entities were reported as app users including Best Buy, Macy's, Kohl's, Wells Fargo, Bank of America, Madison Square Garden, Eventbrite, Las Vegas Sands, Penchaga Resort Casino, and Equinox [100]. Despite claims from the company that their services are only provided in the United States and Canada, the leaked documents indicate that a sovereign wealth fund in the United Arab Emirates was also a client [100].

On top of those lists, the app users have also been affiliated with educational institutions such as the University of Alabama, Colombia University, Southern Methodist University, and the University of Minnesota [100]. The app has even reportedly been used by people associated with two high schools, Central Montco Technical High School and Somerset Berkley Regional High School [100]. Many of the entities on the list only signed up for free trials of the product, and many more initially responded to

reporter's questions with denial of the use [100]. When reporters followed up, most of the entities that initially denied the use confirmed that individual employees had signed up for the service without the knowledge of the entity [100].

Clearview's operations have been called illegal by many, however despite these claims, there is little being done about the company's practices. Most places in the United States do not have firm laws in place that protect citizens biometric data, so the company operates in an "absence of…rigorously enforced consumer privacy laws." [96]. New Jersey's Attorney General banned the use of the app after concerns that it was being used by police without any state government oversight [53]. However, there is now legally established precedence that ruled data scraping is not a violation of the law, even if it technically violates the terms of use of a site or service [96]. Twitter is just one of many companies that issued a cease and desist to the company, but nothing concrete can be done without a legal ruling in Twitter's favor [96].

The Clearview AI database was created with photos scraped from the internet without receiving consent form the photograph's owners or subjects. If you live most places in the world, there is nothing you can do about this. The company claims that by scraping from public pages, it is free information and available under the First Amendment [101]. However, for residents of Illinois, after David Mutnick sued for violation of the Biometric Identification Protection Act, Clearview AI must allow an opt out method [102]. This also extends to Californians, who can find an opt-out form on Clearview's website which allows users to request their data be removed from the database [97]. EU citizens enjoy similar options under the GDPR [103]. The Canadian government also banned the app and demanded that Canadian photos be deleted from the database [103]. The company countered, claiming that Canadian law does not apply to them, seeing as they have no substantial ties to the country [104]. Stanford Law School privacy professor Al Gidari said, "Absent a very strong federal privacy law, we're all screwed [98]."

The privacy implications of an app like this are enormous. Having your photo in Clearview's database without your consent is likened to being in a constant police lineup with no real say in the matter [104]. Up until now, major tech giants have had the capabilities to construct a database as Clearview AI did, but chose not to due to privacy concerns and worries about abuse of such a system [98]. Like a game of Hearts, Clearview AI has broken the unspoken barrier of amassing public photos for private use, allowing other companies to now follow suit and lead the charge, companies that may have blatantly nefarious intentions or lack the security mindset to keep such a database of personal information safe. The CEO of the company does not seem to understand the ramifications of his actions, or just doesn't care. Ton-That refused to outright say he would not share his product with countries that have long standing histories of human rights abuses [101]. He was also "taken aback" in an interview when asked his thoughts on his apps potential to end public anonymity, saying he would "have to think about that." [98] His blatant disregard for consent from subjects of images also does not take into consideration the images that exist online without the subject's consent in the first place, due to things like doxing or revenge porn [103]. The company's practices and care-free attitude towards personal privacy coupled with the lack of legal regulations could spell a new age of facial recognition privacy violations for United States Citizens.

CHAPTER 7

CONCLUSIONS

The laws currently enabling US citizen's right to protect their biometric data is sparse and lacking. At the federal level, nothing yet exists. At the state level, only Texas, Washington, and Illinois have clearly defined privacy laws protecting an individual's biometric data. Most states, however, have some sort of bill proposed in the state legislature, many of them tackling the same concerns. Nearly all of these proposed laws were introduced in the last year to year and a half, illustrating how recent these technological advancements are.

Most of the proposed bills concern law enforcement and its use of the technology. Several of the bills proposed would ban law enforcement from using facial recognition in conjunction with immigration matters. While the issue of immigration is a complex one, immigrants who are in the country without papers already live daily life in fear of being discovered and deported. Adding facial recognition to the list of worries is excessive and unnecessary. Additionally, using facial recognition to vet incoming foreign nationals could return incorrect results that would bar an innocent, deserving person a chance at the American dream. Facial recognition laws in committees across the US also propose requiring a warrant before law enforcement uses it, which would be an excellent step to monitoring and regulating its use as an investigative tool. Further laws in the works also propose to ban facial recognition matches from being considered positive identifications and keep them from being admissible in court, highlighting that facial recognition is not an infallible technology and should not be considered probable cause for arrest or the end all, damning evidence in a trial, as evidenced by the multiple cases of false accusations discussed earlier.

There are also common themes with commercial limitations on facial recognition. Illinois' Biometric Information Privacy Act has appeared in several lawsuits since it was passed, showing how crucial this sort of legislation has been in protecting the personal information of the citizens of Illinois. At the federal level, the Commercial Facial Recognition Privacy Act of 2019 would offer the same protections as Illinois' BIPA to all US citizens.

Clearview AI is a perfect example of why these regulations are absolutely critical for the privacy and safety of the public. Should an app such as Clearview AI or Clearview AI itself become publicly available, public anonymity will be a thing of the past. Anyone walking by you on the street could discreetly snap a photograph of you and instantly have your identity and the ability to find out heaps of personal information about you through simple web searches. In the hands of a stalker, this could be catastrophic for a victim who would no longer be able to show their face in public without risk of being found and threatened again. The same situation apples to individuals in Witness Protection. Furthermore, in the modern age of cancel culture and mass public shaming on the internet, coupled with intense political division, the recognition software could be used by the public to identify and attack protestors exercising their democratic rights. The same could be done by police officers.

The mass presence of cameras, either surveillance or on our phones, has nearly eliminated the idea of privacy by invisibility. Facial recognition takes the elimination of privacy one step further, eliminating

our anonymity in public spaces. Without strong federal laws guaranteeing our right to privacy and protecting us from both government and private abuse of the technology, privacy as we know it is a relic of the past.

REFERENCES

[1] "*Face Recognition."* Electronic Frontier Foundation, 2017, www.eff.org/pages/face-recognition.

[2] S. Symanovich. *"How Does Facial Recognition Work?"* NortonLifeLock, 8 Feb. 2019, us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html.

[3] P. Grother, M. Ngan, K. Hannaoka, "*Face Recognition Vendeor Test (FRVT) Part 3: Demographic Effects*", National Institute Of Standards and Technology, 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[4] J. A. Buolamwini, "*Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers*", Massachusetts Institute of Technology, 2018, https://dam-prod.media.mit.edu/x/2018/02/05/buolamwini-ms-17_WtMjoGY.pdf

[5] I. D. Raji, J. Buolamwini, "*Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*", Massachusetts Institute of Technology, 2019, https://dam-prod.media.mit.edu/x/2019/01/24/AIES-19_paper_223.pdf

[6] "*User Agreement*.", LinkedIn, www.linkedin.com/legal/user-agreement

[7] "*Statement of Rights and Responsibilities",* Facebook, https://www.facebook.com/legal/terms/previous

[8] K. Hill, "*Wrongfully Accused by an Algorithm."* The New York Times, 24 June 2020, www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[9] "*About Us – DataWorks", Plus*, DataWorks Plus, www.dataworksplus.com/about.html.

[10] E. Stokes. "*Wrongful Arrest Exposes Racial Bias in Facial Recognition Technology*.", CBS News, 19 Nov. 2020, www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/

[11] K. Hill, "*Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match."*, The New York Times, 29 Dec. 2020, www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[12] "*Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties*." House Committee on Oversight and Reform, 2019, oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and.

[13] "*Federal Law Enforcement Use of Facial Recognition Technology*", Congressional Research Service, 27 Oct. 2020, https://crsreports.congress.gov/product/pdf/R/R46586

[14] "*FTC Recommends Best Practices For Companies That Use Facial Recognition Technologies",* Federal Trade Commission, 22 Oct. 2012, https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition

[15] "*California Company Settles FTC Allegations It Deceived Consumers about Use of Facial Recognition in Photo Storage App."* Federal Trade Commission, 27 Jan. 2021, www.ftc.gov/news-events/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers.

[16] "*S.4084 - 116th Congress (2019–2020): Facial Recognition and Biometric Technology Moratorium Act of 2020*." Congress.Gov | Library of Congress, 2020, www.congress.gov/bill/116th-congress/senate-bill/4084.

[17] "*Text - S.2878 - 116th Congress (2019–2020): Facial Recognition Technology Warrant Act of 2019*." Congress.Gov | Library of Congress, 2019, www.congress.gov/bill/116th-congress/senate-bill/2878/text.

[18] "*S.847 - 116th Congress (2019–2020): Commercial Facial Recognition Privacy Act of 2019*." Congress.Gov | Library of Congress, 2019, www.congress.gov/bill/116th-congress/senate-bill/847.

[19] B. Moseley, "*Orr Pre-Files Bill to Limit Use of Facial Recognition Technology by Law Enforcement*." Alabama Political Reporter, 1 Feb. 2021, www.alreporter.com/2021/02/01/orr-pre-files-bill-to-limit-use-of-facial-recognition-technology-by-law-enforcement.

[20] "*SB 98: 'An Act Relating to Biometric Information.* '" Alaska State Legislature, www.akleg.gov/basis/Bill/Text/27?Hsid=SB0098A

[21] "*Arizona HB2478 | 2019 | Fifty-Fourth Legislature 1st Regular*." LegiScan, 2019, legiscan.com/AZ/text/HB2478/id/1857901.

[22] "*EPIC - State Facial Recognition Policy.*" Electronic Privacy Information Center, epic.org/state-policy/facialrecognition.

[23] *"Colorado SB132 | 2021 | Regular Session."* LegiScan, 2021, legiscan.com/CO/text/SB132/id/2314784.

[24] "*Connecticut HB05326 | 2016 | General Assembly."* LegiScan, 2016, legiscan.com/CT/bill/HB05326/2016.

[25] "*Connecticut HB05333 | 2019 | General Assembly*." LegiScan, 2019, legiscan.com/CT/bill/HB05333/2019.

[26] N. Ciolino, "*Delaware DMV Assists FBI Investigations Using Facial Recognition Tech, License Info*." Delaware Public Media, 17 Sept. 2019, www.delawarepublic.org/post/delaware-dmv-assists-fbi-investigations-using-facial-recognition-tech-license-info.

[27] "*U.S. Senator Christopher Coons of Delaware*." Sen. Coons, 14 Nov 2019, www.coons.senate.gov/news/press-releases/facial-recognition-tech-sens-coons-lee-bill-requires-court-orders-for-law-enforcement-use-of-facial-recognition-technology.

[28] J. Valentino-DeVries, "*How the Police Use Facial Recognition, and Where It Falls Short."* The New York Times, 12 Jan. 2020, www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

[29] *"Willie Allen Lynch vs State of Florida."* Justia Law, law.justia.com/cases/florida/first-district-court-of-appeal/2018/16-3290.html.

[30] "*Measure Status."* Hawaii State *Legislature*, www.capitol.hawaii.gov/measure_indiv.aspx?billtype=HB&billnumber=1226&year=2021.

[31] "*House Bill 0492*." Idaho State Legislature, 2020, legislature.idaho.gov/wp-content/uploads/sessioninfo/2020/legislation/H0492.pdf.

[32] "*740 ILCS 14/ Biometric Information Privacy Act.*" Illinois General Assembly, www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

[33] "*Indiana Intelligence Fusion Center - Facial Recognition Policy."* Indiana State Police, 1 June 2019, www.in.gov/iifc/files/Indiana_Intelligence_Fusion_Center_Face_Recognition_Policy.pdf.

[34] "*Indiana HB1238 | 2020 | Regular Session."* LegiScan, 2020, legiscan.com/IN/bill/HB1238/2020.

[35] "*Iowa DOT Using Facial Recognition Technology*." The Gazette, 3 July 2013, www.thegazette.com/2013/07/03/iowa-dot-using-facial-recognition-technology.

[36] "*Senate Bill No.361."* Kentucky State Legislature, 2018, kslegislature.org/li_2018/b2017_18/measures/documents/sb361_00_0000.pdf.

[37] B. Maples, "*Kentucky one of 21 states sharing driver's license photos with FBI and ICE*", Forward Kentucky, 9 July 2019, https://forwardky.com/kentucky-one-of-21-states-sharing-drivers-license-photos-with-fbi-and-ice/

[38] "*Kentucky SB280 | 2021 | Regular Session."* LegiScan, 2021, legiscan.com/KY/bill/SB280/2021?utm_campaign=rss&guid=5a2sYpxQJtQubatv41Lbbk

[39] "*HB662*." Louisiana State Legislature, 2018, www.legis.la.gov/legis/BillInfo.aspx?i=238406

[40] "*COMMITTEE AMENDMENT to S.P. 651, L.D. 1899, Bill, 'An Act To Amend Certain Motor Vehicle Laws."*" Maine Legislature, legislature.maine.gov/legis/bills/getPDF.asp?paper=SP0651&item=2&snum=129.

[41] "*Maryland HB23 | 2021 | Regular Session."* LegiScan, 2021, legiscan.com/MD/bill/HB23/2021

[42] *"Maryland SB234 | 2021 | Regular Session."* LegiScan, 2021, legiscan.com/MD/bill/SB234/2021

[43] S. Wu, "*Somerville City Council Passes Facial Recognition Ban."* BostonGlobe.Com, 28 June 2019, www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html.

[44] S. Solis, "*Massachusetts Passes Bill With Facial Recognition Rules*." GovTech, MassLive.com, 22 Dec. 2020, www.govtech.com/policy/Massachusetts-Passes-Bill-With-Facial-Recognition-Rules.html.

[45] "*Bill S.1385 - An Act Establishing a Moratorium on Face Recognition and Other Remote Biometric Surveillance Systems."* The 192nd General Court of the Commonwealth of Massachusetts, malegislature.gov/Bills/191/SD671.

[46] *"MSP - Statewide Network of Agency Photos (SNAP)."* Michigan State Police, www.michigan.gov/msp/0,4643,7-123-72297_64747_64749-357133--,00.html.

[47] T. Perkins, *"'It's Techno-Racism': Detroit Is Quietly Using Facial Recognition to Make Arrests."* The Guardian, 19 Aug. 2019, www.theguardian.com/us-news/2019/aug/16/its-techno-racism-detroit-is-quietly-using-facial-recognition-to-make-arrests.

[48] V. Carducci, "*Detroit's Project Green Light and the 'New Jim Code.*'" Public Seminar, 8 Oct. 2020, publicseminar.org/essays/detroits-project-green-light.

[49] "*Minnesota HF240 | 2021–2022 | 92nd Legislature."* LegiScan, 2021, legiscan.com/MN/bill/HF240/2021.

[50] K. Crown, "*Jackson Bans Facial Recognition Tech; New Airport Academy, Sewer Repairs.*" Jackson Free Press | Jackson, MS, 20 Aug. 2020, www.jacksonfreepress.com/news/2020/aug/20/jackson-bans-facial-recognition-tech-new-airport-a.

[52] "*Ban on Facial Recognition Evidence Considered."* Unicameral Update, update.legislature.ne.gov/?p=27728.

[52] "*New Hampshire HB499 | 2021 | Regular Session*." LegiScan, 2021, legiscan.com/NH/bill/HB499/2021

[53] K. Hill, "*New Jersey Bars Police From Using Clearview Facial Recognition App*." The New York Times, 25 Jan. 2020, www.nytimes.com/2020/01/24/technology/clearview-ai-new-jersey.html.

[54] "*New Jersey Legislature – Bills A1210."* New Jersey Legislature, www.njleg.state.nj.us/bills/BillView.asp?BillNumber=A1210.

[55] "*New Jersey S1916 | 2020–2021 | Regular Session*." LegiScan, 2020, legiscan.com/NJ/bill/S1916/2020.

[56] "*New Jersey S1917 | 2020–2021 | Regular Session."* LegiScan, 2020, legiscan.com/NJ/bill/S1917/2020.

[57] "*New Jersey A4211 | 2020–2021 | Regular Session."* LegiScan, 2020, legiscan.com/NJ/bill/A4211/2020.

[58] "*New Jersey Legislature - Bill A989*." New Jersey Legislature, www.njleg.state.nj.us/bills/BillView.asp?BillNumber=A989.

[59] "*New Jersey S116 | 2020–2021 | Regular Session*." LegiScan, 2020, legiscan.com/NJ/bill/S116/2020.

[60] M. Shephard, "*Albuquerque Police Use Facial Recognition Tech Responsibly, Report Says*." GovTech, Albuquerque Journal, 27 Dec. 2016, www.govtech.com/em/safety/Albuquerque-Facial-Recognition.html.

[61] J. Nguyen, "*New Mexico Law Enforcement Suspended from Using Amazon's Facial Recognition Technology."* KRQE News 13, 13 June 2020, www.krqe.com/news/new-mexico/new-mexico-law-enforcement-suspended-from-using-amazons-facial-recognition-technology.

[62] "*NY - A03759*." BillTrack50, www.billtrack50.com/billdetail/1292405.

[63] "*NY - S03234."* BillTrack50, www.billtrack50.com/billdetail/1292826.

[64] "*NY - A05492."* BillTrack50, www.billtrack50.com/billdetail/1321824.

[65] "*NY - S00079."* BillTrack50, www.billtrack50.com/billdetail/1254327.

[66] "*NY - A01601*." BillTrack50, www.billtrack50.com/billdetail/1263870.

[67] *"NY - S01076."* BillTrack50, www.billtrack50.com/billdetail/1259873.

[68] *"New York A00768 | 2021–2022 | General Assembly."* LegiScan, 2021, legiscan.com/NY/bill/A00768/2021.

[69] *"NY - A04916."* BillTrack50, www.billtrack50.com/billdetail/1305616.

[70] *"NY - A04352."* BillTrack50, www.billtrack50.com/billdetail/1296903.

[71] *"NY - S00073."* BillTrack50, www.billtrack50.com/billdetail/1255245.

[72] "*NY - S00893*." BillTrack50, www.billtrack50.com/billdetail/1258389.

[73] "*NY - A00954."* BillTrack50, www.billtrack50.com/billdetail/1258272.

[74] "*MEMORANDUM OF UNDERSTANDING BETWEEN THE FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES DIVISION AND THE NORTH DAKOTA ATTORNEY GENERAL BUREAU OF CRIMINAL INVESTIGATION CONCERNING THE SEARCH OF PROBE PHOTOS AGAINST THE NORTH DAKOTA ATTORNEY GENERAL BUREAU OF CRIMINAL INVESTIGATION PHOTO REPOSITORY*." United States House Committee of Oversight and Reform, 2017, republicans-oversight.house.gov/wp-content/uploads/2017/03/North-Dakota-MOU.pdf.

[75] J. Balmert, "*Ohio Cuts off Access to Facial-Recognition Database – for Now.*" Cincinnati Enquirer, 14 Aug. 2019, eu.cincinnati.com/story/news/politics/2019/08/14/ohio-cuts-off-access-facial-recognition-database-temporarily/2006517001.

[76] "*Review of Facial-Recognition Database Finds No Evidence of Misuse - Ohio Attorney General Dave Yost*." Ohio Attorney General, 2019, www.ohioattorneygeneral.gov/Media/News-Releases/August-2019/Review-of-Facial-Recognition-Database-Finds-No-Evi.

[77] "*SB309 2021 Regular Session - Oregon Legislative Information System.*" Oregon Legislative Information System, 2021, olis.oregonlegislature.gov/liz/2021R1/Measures/Overview/SB309

[78] "*Oregon SB310 | 2021 | Regular Session."* LegiScan, 2021, legiscan.com/OR/bill/SB310/2021

[79] "*Rhode Island H5652 | 2021 | Regular Session."* LegiScan, 2021, legiscan.com/RI/bill/H5652/2021

[80] *"Rhode Island S0253 | 2021 | Regular Session."* LegiScan, 2021, legiscan.com/RI/bill/S0253/2021. Accessed 31 Mar. 2021.

[81] "*South Carolina H3918 | 2021–2022 | 124th General Assembly."* LegiScan, 2021, legiscan.com/SC/bill/H3918/2021.

[82] "*BUSINESS AND COMMERCE CODE CHAPTER 503. BIOMETRIC IDENTIFIERS."* Texas Constitution and Statutes, statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm.

[83] "*H.B. 250 Driver License Revisions."* Utah State Legislature, 2021, le.utah.gov/~2021/bills/static/HB0250.html.

[84] "*S.B. 34 Governmental Use of Facial Recognition Technology*." Utah State Legislature, 2021, le.utah.gov/~2021/bills/static/SB0034.html.

[85] "*VT H0075 | 2021-2022 | Regular Session."* LegiScan, 2021, https://legiscan.com/VT/bill/H0075/2021

[86] "*Vermont H0195 | 2021–2022 | Regular Session.*" LegiScan, 2021, legiscan.com/VT/bill/H0195/2021. Accessed 31 Mar. 2021.

[87] "*HB 2031 Facial Recognition Technology; Authorization of Use by Local Law-Enforcement Agencies, Etc.*" Virginia's Legislative Information System, lis.virginia.gov/cgi-bin/legp604.exe?211+sum+HB2031.

[88] "*RCW 19.375.020: Enrollment, Disclosure, and Retention of Biometric Identifiers."* Washington State Legislature, app.leg.wa.gov/RCW/default.aspx?cite=19.375.020.

[89] *"Washington SB5104 | 2021–2022 | Regular Session."* LegiScan, 2021, legiscan.com/WA/bill/SB5104/2021.

[90] "*Wyoming SF0029 | 2021 | Regular Session."* LegiScan, 2021, legiscan.com/WY/bill/SF0029/2021.

[91] "*ACLU of Louisiana Sues Louisiana State Police for Facial Recognition Documents*." American Civil Liberties Union, 2021, www.aclu.org/press-releases/aclu-louisiana-sues-louisiana-state-police-facial-recognition-documents.

[92] "*50 pages of email requests*", ACLU of Louisiana, 2020, https://www.laaclu.org/sites/default/files/field_documents/facial_recognition_public_records.pdf

[93] M. I. Stein, "*New Orleans Police Department Using Facial Recognition despite Years of Denial*" The Lens - New Orleans, 13 Nov. 2020, thelensnola.org/2020/11/12/new-orleans-police-department-using-facial-recognition-despite-years-of-denial/.

[94] T. Hatmaker, "*Lawsuits Allege Microsoft, Amazon and Google Violated Illinois Facial Recognition Privacy Law."* TechCrunch, 15 July 2020, techcrunch.com/2020/07/15/facial-recognition-lawsuit-vance-janecyk-bipa/.

[95] D. W. Sexton, Esq, *"Nijeer Parks vs. JOHN E. McCORMACK, MAYOR OF WOODBRIDGE, In his personal and official capacity ROBERT HUBNER DIRECTOR OF THE WOODBRIDGE POLICE, in his personal and official capacity, CITY OF WOODBRIDGE POLICE OFFICERS JOHN AND JANE DOE, 1–20, being as yet unknown actors, MIDDLESEX DEPARTMENT OF CORRECTIONS, JOHN and JANE being unknow actors, MIDDLESEX COUNTY PROSECUTOR, ACTING PROSETOR, CHRISTOPHER KUBERIET: Complaint and Demand For Trial by Jury",* Superior Court of New Jersey Law Division Passiac County, 2020, https://int.nyt.com/data/documenttools/new-jersey-facial-recognition-lawsuit-nijeer-parks-v/38ff3e74088a95a9/full.pdf

[96] K. Hill, "*Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*." The New York Times, 23 Jan. 2020, www.nytimes.com/2020/01/22/technology/clearview-ai-twitter-letter.html.

[97] "*Clearview AI – Clearview.Ai*." Clearview AI, clearview.ai.

[98] K. Hill, "*The Secretive Company That Might End Privacy as We Know It.*" The New York Times, 18 Mar. 2021, www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[99] "*Clearvie FAQ*", Clearview AI, https://int.nyt.com/data/documenthelper/6690-clearview-faq/c8b081a0bcca12e7903a/optimized/full.pdf#page=1

[100] R. Mac, "*Clearview AI's Facial Recognition Tech Is Being Used By The Justice Department, ICE, And The FBI*." BuzzFeed News, 28 Feb. 2020, www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[101] R. Heilweil,. "*How Clearview AI Is Using Facial Recognition*." Vox, 8 May 2020, www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement.

[102] N. Statt, "*Clearview AI to Stop Selling Controversial Facial Recognition App to Private Companies.*" The Verge, 8 May 2020, www.theverge.com/2020/5/7/21251387/clearview-ai-law-enforcement-police-facial-recognition-illinois-privacy-law.

[103] A. Möhle, "*Clearview AI's Photo Database Declared Illegal in the EU and Canada.*", Tutanota, 10 Feb. 2021, tutanota.com/blog/posts/clearview-scandal-opt-out.

[104] K. Lyons, "*Clearview's Facial Recognition Tech Is Illegal Mass Surveillance, Canada Privacy Commissioners Say."* The Verge, 4 Feb. 2021, www.theverge.com/2021/2/4/22266055/clearview-facial-recognition-illegal-mass-surveillance-canada-privacy.