Colby College
Digital Commons @ Colby

Honors Theses Student Research

2019

# Algorithmic Surveillance: A Hidden Danger in Recognizing Faces

Lydia F. Venditti
*Colby College*

Jim Fleming
*Colby College*

Kara Kugelmeyer
*Colby College*

Follow this and additional works at: https://digitalcommons.colby.edu/honorstheses

Part of the History of Science, Technology, and Medicine Commons

Colby College theses are protected by copyright. They may be viewed or downloaded from this site for the purposes of research and scholarship. Reproduction or distribution for commercial purposes is prohibited without written permission of the author.

Recommended Citation

Venditti, Lydia F.; Fleming, Jim; and Kugelmeyer, Kara, "Algorithmic Surveillance: A Hidden Danger in Recognizing Faces" (2019). *Honors Theses.* Paper 932.
https://digitalcommons.colby.edu/honorstheses/932

This Honors Thesis (Open Access) is brought to you for free and open access by the Student Research at Digital Commons @ Colby. It has been accepted for inclusion in Honors Theses by an authorized administrator of Digital Commons @ Colby.

# Algorithmic Surveillance: A Hidden Danger in Recognizing Faces

Lydia Francesca Venditti
Honors Thesis
Science, Technology and Society Program
Colby College, Waterville, ME 04901
May 18, 2019

A thesis presented to the faculty of the Science, Technology, and Society Program in partial fulfillment of the graduation requirements for the Degree of Bachelor of Arts with Honors in Science, Technology, and Society

James R. Fleming, Advisor

Kara Kugelmeyer, Second Reader

# Abstract

The goal of this thesis is to present the current status and awareness of facial recognition technology and their use as part of video surveillance systems. Specifically, I intend to help readers develop a greater understanding of how facial recognition systems contain algorithms that perpetuate bias in their matching and recognition of faces. Current research demonstrates that algorithms differentially recognize faces from different races and genders. As a technology with substantive impacts for use and abuse, more scrutiny of facial recognition technology is necessary. This paper will also help readers understand the dangers of facial recognition as a biometric technology and how biometric data and privacy are large topics of discussion that affect individuals across the globe as society continues through the Information Age. This paper utilizes different critical lenses to address the issues and implications of facial recognition, including sociological and legal approaches in analyzing issues of algorithmic bias. Through the analysis of legal cases regarding the use of facial recognition, data on current algorithms used, and implications for privacy and surveillance, I present a critique of the technology is presented along with suggestions for its future uses.

# Introduction: Why is it Important to Study Facial Recognition and Bias?

Facial recognition is an important technology to understand because it has so many varied uses, from picture tagging in Facebook to security monitoring large sports stadiums as was done in Tampa, Florida for the 2001 Super Bowl and in identifying ‘terrorists’ at airports and helping the U.S. Government in creating “no fly lists” (Brey, 2004). Additionally, I am interested in this topic because so many people are not concerned about powerful technologies due to the strong culture in society that “seeing is believing” and the idea of “I have nothing to hide.” When academics conducted “man-in-the-street” interviews and asked how respondents felt that video surveillance affected them, the dominant response was, “I have nothing to hide” (Saetnan, 2007). The participants were confident that if they have not committed any crime, they would not be mistakenly seen committing a crime. Many individuals are unaware, however, that facial recognition technology carries with it the danger of false positives; so this technology is disrupting the common view of “I have nothing to hide.”

Understanding facial recognition systems is also integral because Americans place a tremendous amount of faith in technology to solve societal issues. Within American culture, there is a deep-seated belief in a mechanistic solution to problems (Bewley-Taylor, 2006). STS scholar Lewis Mumford argued this point and claimed that American culture is constructed upon mistaken beliefs that, “the universe is a fundamentally simple mechanical system subject to human control.” Arguably, facial recognition systems are and were created as a mechanical and digital solution to control and surveil society. Furthermore, as military technologies from GPS to drones have become more prominent in society, Americans have developed a desensitization to technologies that allow for an “omnivideo environment” (Bewley-Taylor, 2006). Currently, society’s rising fear of terrorism after 9/11 will be a large obstacle for critics of this technology as many proponents of facial recognition argue that facial recognition can be utilized by the military and other governmental organizations to prevent terrorist attacks.

Similar to other technologies like artificial intelligence or big data, powerful technologies like facial recognition are very influential, but there is no accountability for using these software systems. Individuals such as doctors have systems in place to control the accountability of their actions through state medical boards; however, most technologists have no such repercussions for building tools that create negative behavior such as privacy invasions, infractions upon civil liberties, or issues with bias. Similarly, surveillance technologies like facial recognition systems have not been tested for accuracy in the way we expect for medical tools and technologies (Saetnan, 2007). According to a Public Policy Initiative published by the University of Pennsylvania Wharton School, the FDA highly regulates new medical drugs and devices so stringently within the United States that they are sometimes available in other countries for extended periods of time before becoming available in the United States.  This may irritate US citizens who would like to use these products but are unable to due to the rigorous FDA approval process.  Despite this, the findings indicate that such strict regulation, such as extensive clinical trials for medications, actually lead to enhanced welfare gains and improved health outcomes. Therefore, regulation for powerful technologies–such as facial recognition systems–may be beneficial.  Unfortunately, there have been no standardized, required benchmark tests to examine the efficacy of facial recognition systems across the industry to ensure sound methods for all systems (Introna & Wood, 2004). Facial recognition is a highly obscure technology using sophisticated methods that ordinary citizens with no prior knowledge of algorithms are able to understand (Bewley-Taylor, 2006).  Algorithms refer to a set of rules or procedure that solves problems within a machine, typically a computing device (Merriam-Webster).  They are typically referred to as “black boxes” because the public does not understand how algorithms behind technologies like facial recognition operate and are able to make decisions. Therefore, this is just one reason that highlights the importance of increasing awareness of problems within these systems, especially for those who are unable to interpret these technologies otherwise.

The role of Science, Technology and Society is to question whether society is heading in the right direction with these technologies, especially because there is a high probability of misuse of facial recognition as advances in this technology are moving faster than ethics and policy to govern this technology. Examining bias in technology is integral, especially with the increasing use of algorithms. It is important to question whether the algorithms used have bias as they are made by humans and are not foolproof and can have tremendous implications within the spheres of criminality, policing and privacy. When examining issues involving facial recognition as STS lens allows us to scrutinize how society interacts with and shapes technological artifacts and whether individuals are just receivers or active, informed, and thoughtful users of the technology.  It is critical to examine how this technology can also shift the balance of power and agency within society.

When most people think of facial recognition technology, the first thought that comes to mind may be looking into their IPhone X screen to unlock it, but in reality, facial recognition systems are more complex, pervasive, and possess many hidden dangers that most people are unaware of.  From its first public use in a sports stadium during the 2001 Super Bowl in Tampa, Florida to its implementation in numerous airports and public streets, facial recognition technology has many uses (Celentino, 2016).  Along with these applications, utilizing facial recognition systems has tremendous implications within the realms of surveillance and privacy, criminality and policing, and fighting terrorism. Important questions that this technology raises include how facial recognition systems are biased, do they really keep people safe and who do they keep safe, how does facial recognition alter characteristics of a surveillance society and what happens when a society becomes highly surveilled, and what are the implications of the technology that we are already seeing? Facial recognition is a technology that enforces and promotes bias, creating larger challenges within a society where there are currently no mechanisms or policies in place to address these biases.

# Historical Development, Uses of the Technology and its Evolution

Facial recognition systems have evolved tremendously since the 1970s.  One of the first issues technologists encountered was creating a computer that could determine whether or not a face was present in a photograph even if the photograph did not contain a face that was captured head-on like a mugshot (Owen, 2018).  With the invention of graphics-processing units (GPUs) in computers, programmers were able to standardize photographs.  The technology has since evolved from systems that can scan and compare a photo to another photo to a more advanced system that can scan a real-time live video feed from a surveillance camera and compare the feed to a database of photos. Currently, most facial recognition systems use artificial neural networks that are trained by giving the networks examples of correct and incorrect information so the computer can learn how to process information. Most facial recognition systems have historically followed a series of steps as shown in Figure 1.

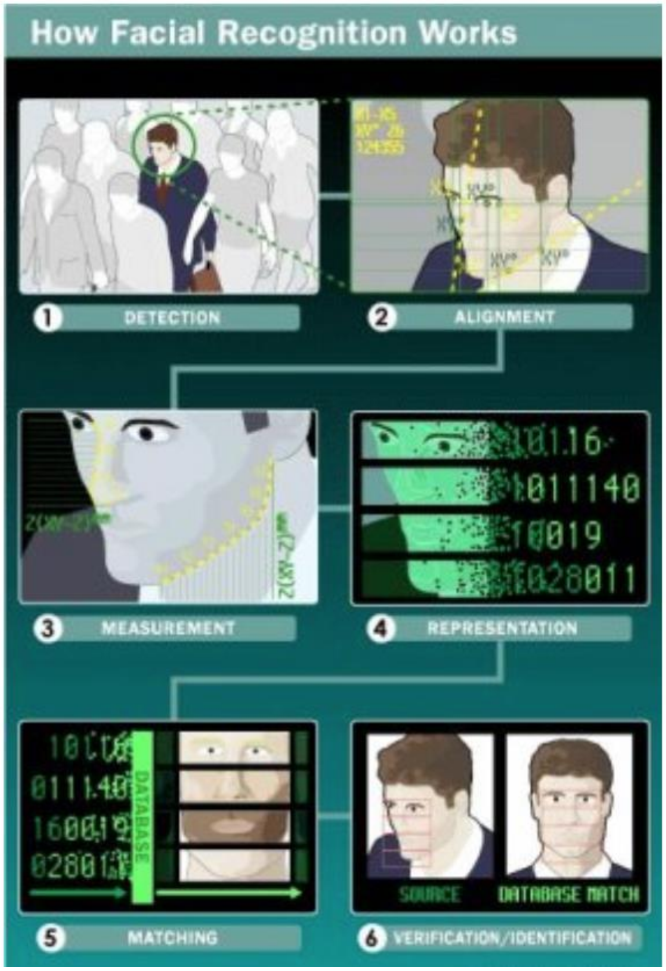


Figure 1. The series of steps that characterize facial recognition systems including detection which includes finding a familiar face within a crowd in a feed: alignment and measurement, which includes measuring the facial geometry of a face (measurements of eyes, nose, mouth, etc.); and matching and verification, which involves matching the proposed face to a face within a photo in a database (Bonsor & Johnson, 2001).

Facial recognition systems quickly gained technological sophistication with the creation of convolutional neural networks (CNN). CNNs are a class of deep neural networks that analyze visual information by assigning a value to an input image that differentiates these images from one another (Sumit, 2018). Deep neural networks refer to technologies with learning mechanisms that use mathematics to process data in a way that mimics a human brain by recognizing patterns in a set of problems (Technopedia, 2019). These networks have multiple layers including inputs and outputs of data and typically use artificial intelligence to analyze data as well. AlexNet, created by Alex Krizhevsky, is the first deep CNN that performed on the ImageNet Challenge in 2012. ImageNet contains a robust database of many different types of labelled images, proving that AlexNet is able to learn, identify, and categorize different objects shown in images (Grm, 2017). This algorithm set a standard where facial recognition technology would process images by training a machine to find unique, identifiable features in different image inputs. While AlexNet is a significant step forward in the advancement of facial recognition systems, this algorithm is still susceptible to lower matching rates due to poor image quality. Consequently, standardization of surveillance camera quality is necessary for facial recognition systems to operate successfully with more accurate matching rates.

Facial recognition technology is recognized as the most natural identifier compared to all other biometric measurements, particularly because people recognize others not by looking at their fingerprints, but by looking at each others' faces. Most individuals are completely unaware that their face prints are just as accurate, if not more accurate and comprehensive, as their background checks. Studies have demonstrated that the average American is recorded on camera approximately 75 times per day (Martin, 2019). As facial recognition technology becomes more prevalent, the number of cameras equipped with the technology will increase and the number of faceprints stored in databases will rise dramatically.

There are uses of facial recognition technology that could prove beneficial to all members of society. Advocates for facial recognition systems argue for its ability to keep people safe from acts of crime such as burglary and assault, terrorism, and for its ability to find missing persons. This technology can be especially helpful even if the missing person has aged. In 2018, a police force in New Delhi found 3,000 missing children within four days using facial recognition (Cuthbertson, 2018). Throughout India there are approximately 200,000 missing children and the facial recognition technology was used on around 45,000 children of which 2,930 were found as missing. With these numbers, the police would struggle to analyze the photos. However, this case raises the issue of not only biometric privacy, but of the age threshold by which law enforcement and other organizations should collect and store biometric data of minors. Furthermore, while this particular use of the technology seems like a great benefit, one must weigh the benefits and all of the drawbacks of using this technology when determining if facial recognition systems should be used at all.

Retailers and shopping malls are also using facial recognition to track consumers. For instance, stores are using facial recognition systems to locate and convict shoplifters (Johnson, 2018). While these systems may allow retailers to avoid theft in their stores, there is also the possibility that the technology will falsely identify an innocent shopper as a convicted shoplifter, therefore invading their privacy. Furthermore, some stores are arguing on whether customers should be told if they are in a store where facial recognition systems are in use. Lowe’s, one of the few retailers that admits to using facial recognition, uses the technology to help locate shoplifters. The company claims that there is no federal law as of yet that requires the company to obtain consent from its consumers. With companies making decisions to use this technology throughout their stores, individuals need to be aware of the possibility that they could be filmed in public spaces. Therefore, the public is required to change their behavior according to the decisions and actions of larger corporations.

Supporters of facial recognition argue for increasing the use of the technology within stadiums for sports games, concerts, and other entertainment purposes. With stadium capacities within the tens of thousands, advocates claim that these systems could help find criminals within the crowd and keep many people safe as a result. Despite these good intentions, attempts at using these systems have not been successful. During the Champions League Match in 2017, South Wales police used the technology with embarrassing results. Many potential matches alerted the system; however, 92 percent of these matches were false positives (Meyer, 2018). Specifically, there were 2,470 possible matches but only 173 of these matches were accurate. The police interviewed but did not arrest anyone during the match and argued that no system can be completely accurate under varying conditions. However, if advocates of the technology are pushing to implement these systems into stadiums and use for surveillance and security purposes, then the algorithms must be more accurate and able to function in the environments in which they will be used. While keeping people safe in crowded stadiums is important, it is difficult to gain consent to scan individuals' faces in a crowd. Also, each stadium would need to examine state privacy laws and ensure that they are acting in accordance. Overall, while there are many uses of these systems, the algorithms require more standardization and increased accuracy in addition to stadiums and companies being attentive to privacy laws.

The closest test that measures the accuracy and efficiency of facial recognition systems are the Facial Recognition Vendor Test (FRVT) [See Figure 2 for a timeline of major events in the history of facial recognition technology]. These tests were sponsored by organizations such as Defense Advanced Research Projects Agency (DARPA), the Department of State, the Federal Bureau of Investigation, and the National Institutes of Standards and Technology (NIST), but participation in these tests are entirely voluntary (Vincent, 2018). The FRVT evaluates how facial recognition systems function in different scenarios such as confirming a proposed identity (e.g., if someone presents an ID at security), identifying within a database (e.g., when suspects are checked for previous convictions), and watch lists (e.g., screening airline passengers to protect against potential terrorists).  The watchlist function demonstrated true positive identification rates for 74% of systems with a 1% false positive rate under ideal conditions (Saetnan, 2007).  Other functions of the test include examining “demographic differentials” specifically, how algorithms perform based on gender, age, and race (Vincent, 2018). Demographic differentials is an area where many algorithms suffer in their precision, specifically with darker skinned individuals and with women.

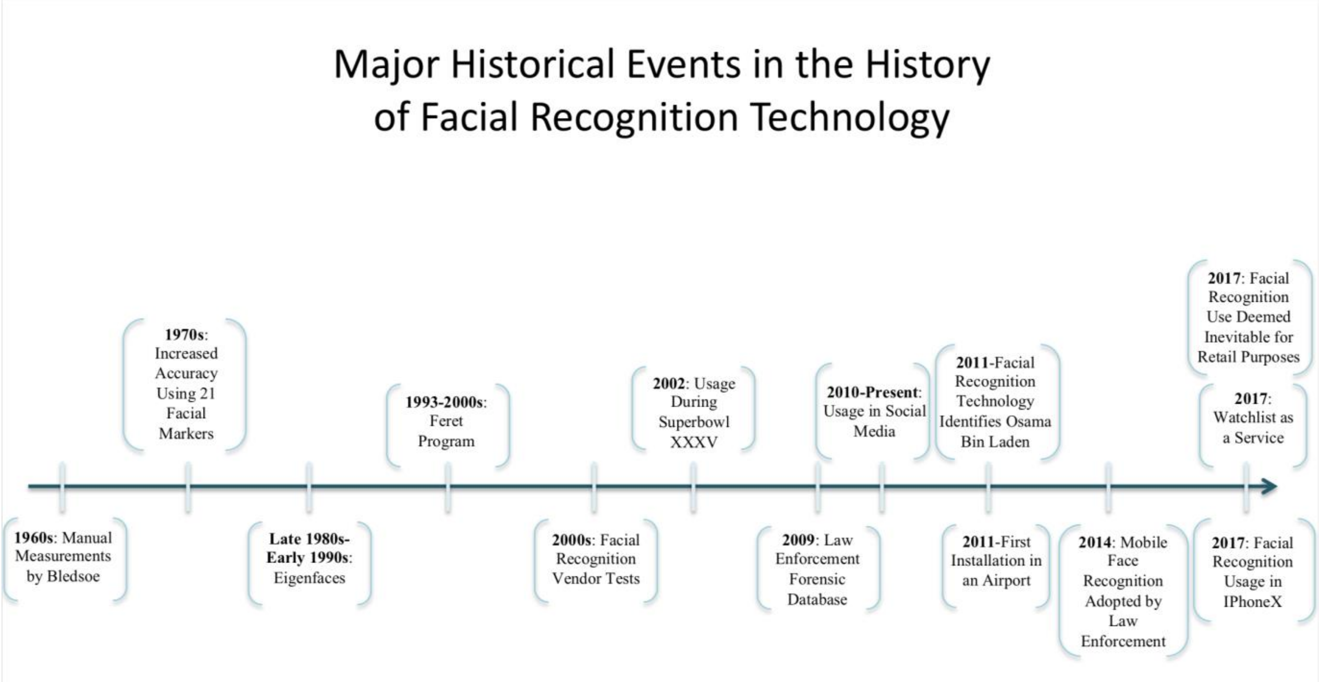

Major Historical Events in the History of Facial Recognition Technology
1960s: Manual Measurements by Bledsoe
1970s: Increased Accuracy Using 21 Facial Markers
Late 1980s-Early 1990s: Eigenfaces
1993-2000s: Feret Program
2000s: Facial Recognition Vendor Tests
2002: Usage During Superbowl XXXV
2009: Law Enforcement Forensic Database
2010-Present: Usage in Social Media
2011-Facial Recognition Technology Identifies Osama Bin Laden
2011-First Installation in an Airport
2014: Mobile Face Recognition Adopted by Law Enforcement
2017: Facial Recognition Use Deemed Inevitable for Retail Purposes
2017: Watchlist as a Service
2017: Facial Recognition Usage in IPhoneX

Figure 2.  Major landmark events in the history of facial recognition systems. Starting with the father of facial recognition, Woodrow Wilson Bledsoe who created a system to manually measure coordinates of a person’s eyes, nose, mouth and other facial features. This system’s precision increased in the 1970s when 21 markers like hair color and lip thickness were added.  Researchers created the Eigenface approach which used linear algebra to detect a face within an image using less than 100 values to code an image of a face.  The U.S Government sponsored the Face Recognition Technology (FERET) program to establish a database that could

train algorithms and to encourage the commercial production of the technology.  Adding to the FERET program, FRVT was another government program that looked to test the accuracy of commercial facial recognition products (West, 2017).

There are many issues with the FRVT tests.  The results assume the technology is working under ideal conditions such as the system operating indoors instead of outdoors or that the photographs within the database are of good quality (Saetnan, 2007).  The system also struggles based on factors such as changes in facial expression or facial hair [See Figure 3]. Additionally, the algorithms tested in the program exhibited identification biases across gender and age.  Recognition rates for males were higher than females with males being identified six to nine percent higher (Introna & Wood 2004).  Furthermore, recognition rates were higher for older individuals compared to younger people.  The average identification rate for 18 to 22 year-olds was 62 percent while the rate was 74 percent for 38 to 42 year-olds.  For every decade increase in age, the identification rate increased five percent through the age of 63 [See Figure 4 for overall performance rank based on accuracy for facial recognition companies]. Based on these results and the statistics that facial recognition systems are able to achieve 70 to 85 percent accuracy rates under ideal conditions, it is important that all individuals are aware of these recognition rates.  The public must take these results into consideration when companies and governmental organizations propose to use this software in a surveillance and security environment. This technology is used without the public’s awareness in different settings such as a crowded city street, shopping mall, or airport and may perform differently depending on how a person looks.

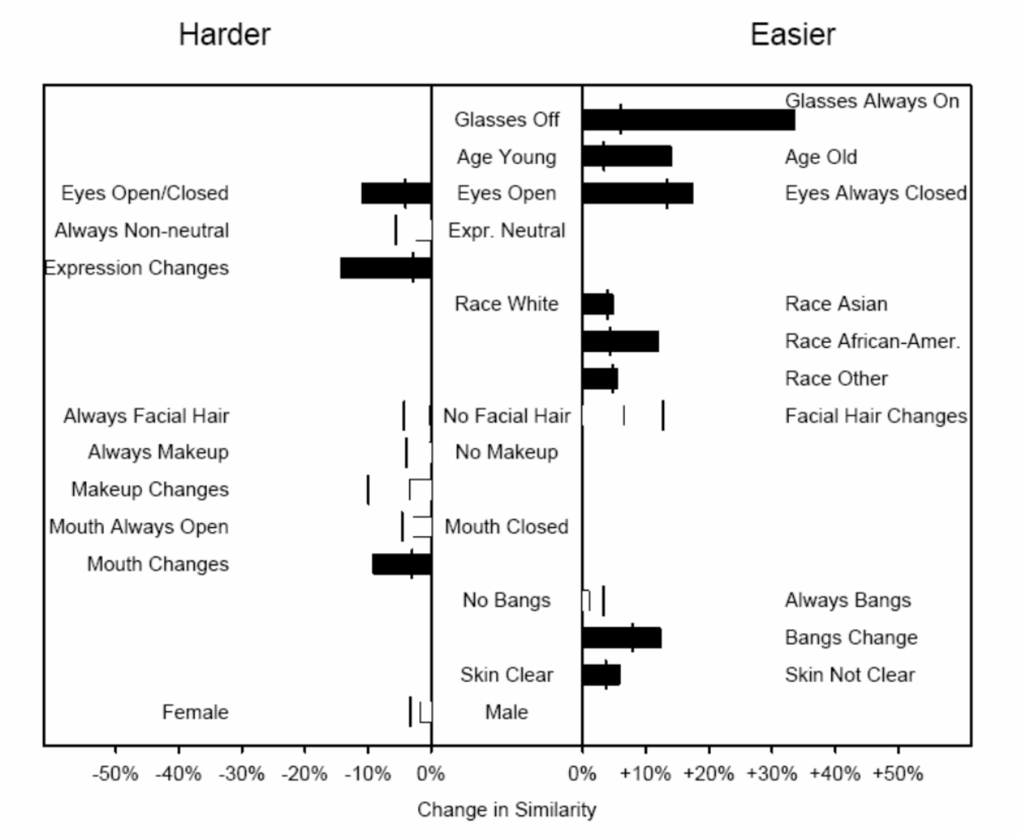


Figure 3.“Factors making it harder or easier to correctly identify a probe image presented to a system.” This diagram demonstrates that facial recognition systems differ in their accuracy in detecting a person’s face depending on physical characteristics such as facial hair, glasses, and other factors. When comparing two images of the same person to determine if the person in the images are the same, facial recognition systems are more accurate when the individual in the image is consistent (e.g., always wearing glasses, consistent facial hair, etc.)  (Givens et al., 2003).

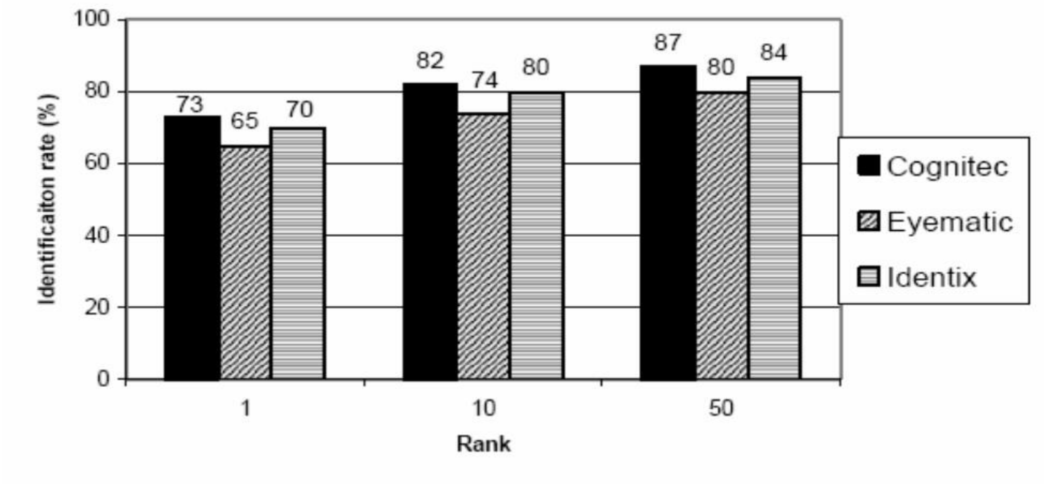


Figure 4. Performance of different facial recognition companies (Cognitec, Eyematic, and Identix) on their identification rates during FRVT tests for accuracy in facial recognition identification tasks (FRVT 2002, Overview and Summary p.9).

## Implications for Terrorism and Increased Border Security

Currently, the fear of terrorism is the most formidable opponent for critics of surveillance technologies such as facial recognition (Bewley-Taylor, 2006). Prior to September 11th, 2001, biometric technologies were dealing with opposition from privacy groups and civil rights organizations. However, since 9/11, there has been a rise in the idea of a surveillance society where the growth of algorithmic surveillance has expanded to include biometric data such as faceprints (Introna & Wood, 2004). A few weeks after the attacks, Congress passed 17 bills that would “tighten immigration, visa, and naturalization procedures, allow tax benefits to companies that use biometrics, and check employee backgrounds at border and maritime check points” (Introna & Wood, 2004). Within two weeks of 9/11, The International Biometrics Industry Association released statements advocating for the use of biometric technologies in fighting terrorism. Furthermore, on September 20th, 2001, Joseph Atick, the CEO of a facial recognition technology company called Visionics, claimed that his software would enhance security in U.S. airports (Bewley-Taylor, 2006). Atick argued that biometrics should be implemented in a surveillance plan he called Operation Noble Shield. To protect America from future acts of terrorism, he stated, “We need to create an invisible fence, an invisible shield.’’ This mindset demonstrates the idea of “technological fix” popularized by Alan Weinberg during the 1960s. Weinberg warned that society must be careful in creating technologies to try to solve problems. Technology is romanticized as a solution to every inconvenience or problem whereas in other countries, border security conduct interviews as a security measure. Visionics released a white paper, *Protecting Civilization from the Faces of Terror,* arguing that “airport security demands substantial financial resources to develop technology that can be implemented to immediately spot terrorists and prevent their actions. Boarding a plane should no longer be considered a right granted to all, but as a privilege accorded to those who can be cleared as having no terrorist or dangerous affiliations” (Pickering & Weber, 2006). Consequently, facial recognitions have taken root in many airports within the U.S. demonstrating the beginnings of using facial recognition as a counterterrorism measure.

Biometric technologies like facial recognition have reignited the discussion surrounding the constitutional ethics of surveillance within the United States. Society has felt an increasing pressure to compromise civil liberties during this period of a “surveillance surge” and the start of the war on terror (Introna & Wood, 2004). At the end of September, a survey conducted by *the New York Times* found that 80% of Americans claimed that they would sacrifice their personal freedoms to protect America from terrorist attacks (Bewley-Taylor, 2006). In fact, delays with security in airports are taken as “part of the price to pay in the war against terrorism where patience is the new patriotism” (Bewley-Taylor, 2006). However, privacy activists and opponents of the technology argue that surrendering privacy rights is notable because visual surveillance is inherently un-American since it is a powerful reminder of Big Brother (Bewley-Taylor, 2006). As a country founded on the principles of freedom and liberty, facial recognition would violate these principles because this technology infringes on the freedom and privacy of its people by creating a surveillance state that monitors its citizens 24/7. Jeffrey Rosen warns against the dangers of a visual surveillance society in his article, *A Watchful State,* published in The New York Times:

> There is, in the end, a powerfully American reason to resist the establishment of a national surveillance network: the cameras are not consistent with the values of an open society. They are technologies of classification and exclusion. If the 21st century proves to be a time when this ideal [open society] is abandoned – a time of surveillance cameras and creepy biometric face scanning in Times Square – then Osama Bin Laden will have inflicted an even more terrible blow than we now imagine (Rosen, 2001).

Rosen is stating that America and its people value freedom and terrorism and figures like Osama Bin Laden have threatened this freedom. By giving into easy, convenient technological fixes and solutions like facial recognition, America would allow threats like terrorism diminish the values of the American people. Visual surveillance within airports is a slippery slope as it will likely serve as a template for increased surveillance within malls, sports arenas, and other public areas (Pickering & Weber, 2006). While the debate over whether to use this software as an anti-terrorist tool is highly contentious, facial recognition systems will continue to play an integral role in visual surveillance.

Since 9/11, The Department of Homeland Security, along with the United States Customs and Border Patrol are working quickly to install this technology in airports. For over 10 years, Congress has advocated for biometric programming that would monitor who enters and exits the United States (Aratani, 2018). In 2016, Congress allocated $1 billion from visa fees to start establishing biometric screening in airports. Similarly, President Donald Trump's executive order in March of 2017 pushed the installation of biometrics to track all travelers crossing the US borders. This order requires all international passengers to undergo face scans in the 20 busiest US airports by 2021. CBP is rushing to install facial recognition technology to meet this goal. Currently, the technology is in use in seventeen airports including New York City, Boston, Atlanta, Chicago, San Jose, and two airports in Houston. Airlines that are advocating for these changes include American Airlines, JetBlue, Delta, British Airways, and Lufthansa (Alba, 2019). In June of 2016, US Customs and Border Patrol (CBP) performed its very first pilot test for facial recognition scanning in an airport (CPB Report, 2016). CBP scanned individuals once daily at Hartsfield-Jackson Atlanta International Airport taking a flight to Tokyo, Japan. Passengers between 14 and 79 years were encouraged to participate in the process. Prior to boarding the plane, passengers scanned their boarding passes and had their photo taken, which was then compared to a database of photos to search for a potential match to a wanted criminal.

CBP and the Department of Homeland Security (DHS) argue that airport security needs facial recognition technology in order to keep up with the increasing amount of travelers, to decrease time spent in the airport, and to combat threats to national security. However, many privacy organizations are questioning whether the facial recognition systems are accurate. CBP only confirmed the biometrics for 85% of the passengers processed in the system and the matches were inconsistent according to the age and nationality of the passenger (Alba, 2019). Specifically, Mexican and Canadian passengers were more difficult for the system to correctly match. Any technology that differentially processes photos based on race cannot be implemented on a large-scale.  Even though the threshold of the system could be lowered to increase the verification rate, this may lead the system to increase the number of false positives which would alert the system and cause a passenger to be wrongly accused of a crime they did not commit. Critics of facial recognition also recognize that CBP claims to only keep the passenger photos for 14 days for US citizens, but they hold photos of non-US citizens for up to 75 years (Aratani, 2018).  Therefore, CBP are biased in the way they treat citizens versus non-citizens.  There are also no rules or regulations as to whether CBP could use the data to further train their algorithms, or restrictions on how other companies or airlines could use the biometric data.  Consequently, airlines or CBP could sell the biometric data to technology companies without any permission from passengers or repercussions.  CBP is also looking to use cloud technology to store the face scans, in which they would partner with a large technology commercial retailer like Amazon or Microsoft to provide cloud capabilities (Alba, 2019).  CBP's actions are worrisome because of the complete lack of vetting and regulation of these facial recognition systems within airports.  This organization needs to obtain public feedback prior to subjecting civilians to the technology and gaining access to their biometric identities.  CBP has previously taken photos from the State Department and used these images to track individuals entering and exiting US borders (Aratani, 2018).  Therefore, more safeguards need to be established to protect the privacy of travelers from the intrusive actions of the CBP.  In May of 2018, Democratic Senator Ed Markey and Republican Senator Mike Lee wrote letters to DHS asking for the agency to establish more official rules prior to further developing biometric technologies within airports (Alba, 2019).  Despite the current polarized political climate, these two senators agreed that this technology is too powerful to be released to the public without formal rules.

## Facial Recognition Technology in Corporations

Due to increasing global competition, technology companies are pushing the limit with facial recognition technology. In 2014, Chaochao Lu and Xiaoou Tang created the GaussianFace algorithm at Hong Kong University (James, 2014). This algorithm is supposedly better at identifying faces compared to humans, with a facial identification score of 98.52% compared to the typical human identification rate of 97.53%. The algorithm was trained on 20,000 matched photos and 20,000 unmatched photos with a wide variety of datasets allowing the system to learn a range of different facial features. One dataset includes the Labelled Faces in the Wild (LFW)–a dataset created by University of Massachusetts Amherst. This dataset includes photos with different light conditions and image quality, which can cause issues for facial recognition systems (James, 2014) [See Figure 3 again to reference how facial recognition systems vary based on environmental and personal conditions in a photo, highlighting the importance of training algorithms on high quality images with people of differing appearance].

Within the United States, multiple tech giants have released facial recognition technology and are racing to create the fastest and most accurate algorithm. The DeepFace program, created by Facebook in 2014, has an accuracy score of 97.25% when calculating if two images contain the same face (Gemalto, 2018). One year later in 2015, Google released their algorithm FaceNet which obtained a 95% accuracy rate on the YouTube Faces database and a 100% accuracy rate when tested on the LFW dataset. The FaceNet algorithm instantly tags and sorts photos in the Google Photos app. In 2018, Amazon designed their cloud-based algorithm, Rekognition. These tech giants are competing in a race with each other, pushing the limits on facial recognition technology in order to take hold of their share of the biometric market.

While many technology companies, both smaller startups and large tech giants, are creating facial recognition software, is this rapid advancement being achieved due to the unauthorized use of consumer data? In early January 2019, the #10YearChallenge went viral as a Facebook competition urging users to post a photo of themselves from ten years ago and another present day photo answering the question, “how has aging affected you?” (Silverstein, 2019). In only three days, over 5.2 million people including many celebrities and public figures posted photos of themselves on different social media platforms such as Facebook, Twitter, and Instagram. The #10YearChallenge seemed like a harmless, viral social media meme until Kate O’Neill, the author of the book, *Tech Humanist: How You Can Make Technology Better for Business and Better for Humans,* posted on Twitter: “Me 10 years ago: probably would have played along with the profile picture aging meme going around on Facebook and Instagram. Me now: ponders how all this data could be mined to train facial recognition algorithms on age progression and age recognition.” O’Neill’s tweet raised the question of whether Facebook created The 10 Year Challenge as a ploy to improve their algorithms for age progression and biometric identification (Fortin, 2019). If a company is looking to train a facial recognition algorithm to understand how people look as they age, then an expansive data set with millions of pictures all 10 years apart would create ideal conditions for the algorithm. Facebook denied any involvement with the start of #The10YearChallenge, claiming they do not benefit from the challenge, the challenge was created by users through a meme that went viral on its own, and users can turn off facial recognition at any time.

O’Neill published an article that further develops the ideas from her twitter post, arguing that Facebook absolutely benefits from The #10YearChallenge going viral. Many are claiming that Facebook already owns access to the uploaded photos; however, O’Neill states that individuals do not consistently upload pictures in chronological order and that users do not always upload profile pictures of themselves, but actually have profile pictures of pets, family members, political statements, and other non-portrait photos. O’Neill writes that the #10YearChallenge is “a perfect storm for machine learning” as it gives Facebook a “clean” dataset of photos with information from the post. With 2.2 billion people uploading photos, Facebook is gaining control of an even more robust database than they currently possess (Fortin, 2019). Facebook is most likely using their facial recognition technology for “targeted advertising” and “personalized experiences” as they make most of their revenue from this. The worry for most users is how their data may be utilized outside of the Facebook platform if the company decides to sell user data to third parties—a strong possibility because Facebook already underwent scandals in 2018 when Cambridge Analytica, a political consulting company tied to President Trump, inappropriately gained access to data from 87 million Facebook users (Martin, 2019). Furthermore, there are currently little to no regulations and laws in place to prevent Facebook from making users’ facial recognition data available outside of the Facebook platform.

The one benefit from #10YearChallenge may be that it has sensitized people to the dangers of carelessly sharing biometric data. O’Neill claims that people, “should be way of any company being in possession of such as large trove of biometric data” (O’Neill, 2019). Through ancestry sites like 23andMe and AncestryDNA, many people have already voluntarily given up their DNA— important biometric information that is stored in large databases and could potentially be used in the future by law enforcement (military, government, etc.). People may not think certain actions are dangerous, like sending a sample of their spit to a lab to determine their ancestral make-up; however, in a few years many individuals will have to deal with the consequences of their choices in releasing their unique biometric information. One consequence lies within the realm of health care where insurance companies may ask for more money or may deny certain individuals coverage if they are found to be aging too fast (O’Neill, 2019). It is necessary for the public to understand that while it may be convenient to give up data to companies like Facebook, these companies are profiting off of the data from their users: “Our data is the fuel that makes business smarter and more profitable” (O’Neill, 2019).

Corporations are also creating products with their facial recognition algorithms such as doorbells like Amazon’s “Nest Hello” and Google’s “Ring.” Google’s wifi-enabled smart doorbell captures “high definition HDR video with night vision after dusk” (Gibbs, 2018). The doorbell can send pictures and alerts to the homeowner’s smartphone, who can also talk to the visitor through the doorbell when the homeowner has Internet connection. The homeowner can also elect to send messages through the doorbell such as “I will be right there.” Nest also contains machine-learning technology that analyzes footage of people passing on the street, loiterers, and potential burglars allowing the doorbell to then alert the homeowner. The doorbell has a “Nest Aware” option because Google enabled the doorbell with cloud video recording and face recognition to allow the doorbell to alert the homeowner if their family or a strange are at the door (Gibbs, 2018). While these features may seem useful and safe at first glance, the Nest’s wide-range camera may capture footage of people on the street which can violate data protection laws and invade people's’ privacy.

Amazon’s “Nest Hello” doorbell also allows homeowners to tag familiar and unfamiliar faces in order to allow the homeowner to be alerted when strangers are at the door. One unique feature of the Ring doorbell is that it allows other houses equipped with Ring doorbells in the neighborhood to communicate with one another with its Ring Neighborhood feature. This trait allows neighboring properties to communicate with each other of any suspicious activity (e.g., strangers loitering, infidelity) occurring within the neighborhood (Cardinal, 2018). The footage from the Ring doorbells can be forwarded directly to law enforcement, which may be helpful in catching suspect characters. However, the public should be wary of consistently handing over facial recognition images and other footage to local law enforcement. Ring's features of "aggregating multiple camera angles" to create comprehensive recordings and pictures of people could be dangerous in police hands because police forces would then be able to add this footage to their extensive databases, creating a more complete profile of "suspicious individuals" (Ruben, 2018). The ACLU places Amazon's Ring, "at the center of a massive decentralized surveillance network running real-time facial recognition on members of the public" (Gibbs, 2018). Law enforcement agencies would then be able to surveil anyone deemed a threat to the public, potentially targeting people such as political activists.

## Privacy and Policing

Biometric data collection includes a person's "unique physical, physiological, and behavioral characteristics" making this data potentially dangerous if it falls into the wrong hands and is misused or violated (Dune, 2016). Many supporters of the technology believe that biometrics, specifically facial recognition, is the newest and best innovation in identification technology. Before long, consumers may sign into their bank accounts with a face scan, placing facial recognition systems and therefore biometric data at the center of technologies that society interacts with for everyday tasks. While a person can easily change the password to his/her online banking account, one cannot simply change a fingerprint or retinal scan. Furthermore, while facial recognition may have started with only analyzing facial characteristics, newer systems contain real-time video surveillance that analyzes both facial data and behavioral characteristics. This may include data from Amazon’s Ring doorbell on how people walk along with other personal characteristics which can be aggregated to create a complete data profile of an individual (i.e., data on multiple characteristics of a person can be combined to generate specific and unique information on a person). Therefore, understanding and making oneself aware of the laws and rights to privacy for biometrics is integral in order to keep a person’s data and identity safe.

Currently, The European Union has the most stringent data and privacy law, including the General Data Protection Regulation (GDPR). This law is the only one that seeks conserve the security of personal data for members of the European Union. Even if a non-EU organization, such as Facebook, processes the private data of a citizen of the EU, a non-EU organization must still abide by the rules of the GDPR (Gemalto, 2018). The European Union privacy laws also forbid the handling of data to third parties without explicit agreement from the EU citizens unless the data is required for employment, social security, legal claims, or if the person is incapable of giving consent (Gemalto, 2018). What really sets the GDPR apart as protective over its citizens’ data is “The Right to be Forgotten” which claims, “the data subject shall have the right to withdraw his or her consent at any time.” Furthermore, according to “The Data Minimization Principle” personal information can only be collected for legitimate purposes and the data that is collected cannot be further analyzed and processed outside of the original specified purposes. Consequently, these restrictions on a person’s private data places the GDPR as the data privacy law for other countries to follow.

While the GDPR in the European Union may be highly protective of data and privacy rights, The United States is struggling to create a comprehensive and overarching data protection law. Illinois was the first to create a biometric privacy law in 2008, called the Biometric

Information Privacy Act (BIPA), which was created to safeguard the individual's right to privacy with the increasing use of biometrics. (Dune, 2016). BIPA is the only law in the United States that restricts how companies and organizations collect and process personal data like finger and voice prints, retinal scans, and other biometric information. The law classifies biometric information as any identifier such as a "retina, iris scan, a scan of hand or face geometry, or a fingerprint" (Ratanaphanyarat, 2018). BIPA is the most rigid privacy law in the United States, forcing companies to let individuals know through writing that their private biometric information is being collected along with the length of the information storage and the purpose of the storage. Along with written consent, companies must also let individuals know when their biometric information will be destroyed. (Marine, 2018). BIPA emphasizes the importance of understanding the value of biometric information, stating that,

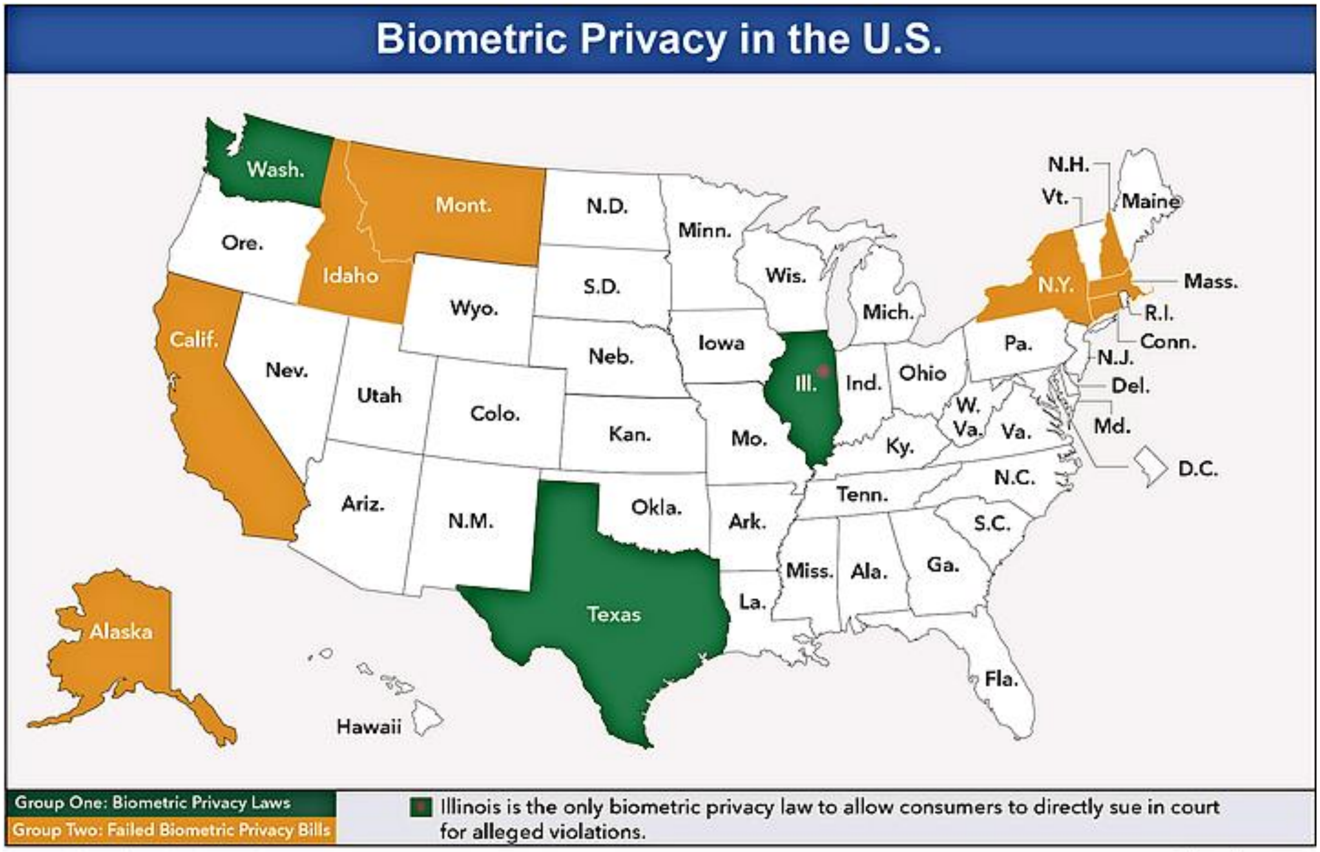
> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

Therefore, compromised biometric information will remain compromised forever, leaving an individual barred from using biometric technology.

Following the creation of BIPA, Texas released its own law, The Texas Biometric Privacy Act of 2009. This law is less strict than BIPA because it does not require companies to gain written consent from users in order to obtain private biometric information (Marine, 2018). Washington State also issued a law in 2017; however, this law is even less specific than the biometric laws passed in Illinois and Texas. Washington's law neglects to mention specific terminology related to biometric identifiers like “voice recordings” or “hand and face geometry” (Ratanaphanyarat, 2018). However, Oregon and New Hampshire have specific laws relating to regulating the use of facial recognition in law enforcement settings (Thakkar, 2018). There are currently six states that limit the use of police use of databases containing driver’s license photos in facial recognition technology.

Unexpectedly, California has no privacy laws despite Silicon Valley being a center for technology start-ups and innovation [See Figure 5 for a visual demonstrating biometric privacy laws throughout the United States]. There have been many bills in California legislature considering the protection of biometric data. In 1998, the legislature considered a bill to require permission prior to collecting and sharing biometric data (Welinder, 2012). There was also a bill in 2001 asking for clear notice when using facial recognition technology and gaining consent for collecting and sharing data. Finally, in 2011-2012, legislature proposed a bill for companies to allow users to opt out of the collection and storage of biometric information. None of these bills were passed into law, most likely due to the strong resistance from tech companies within Silicon Valley. Companies like Google, Facebook and Yahoo! claimed that such laws would restrict innovation and advancements of technology which would further harm consumers.

Despite legislative setbacks in California, Illinois and other states that are establishing biometric privacy laws are paving the way for others to do the same, and potentially allowing for the possibility of the United States creating a federal law for biometric privacy rights. This would be especially necessary as biometric information continues to become more commonplace and heavily used in daily life.



Source: Bloomberg BNA Research

Bloomberg BNA

Figure 5. A map depicting the status of biometric privacy laws in the United States

Use of this facial recognition systems are desirable because unlike other biometric technologies like fingerprint or iris scans, facial recognition requires no explicit consent from the target making this surveillance technology completely unintrusive. Therefore, facial recognition systems are considered a “silent technology” because they operate passively in the background, unnoticed by subjects (Introna & Wood, 2004). For this reason, this software is highly desirable for surveillance purposes. According to recent studies, “half of American adults, some 117 million people, are in unregulated facial recognition networks used by state and local law enforcement agencies and at least 26 states allow law enforcement to run searches against database driver’s license photos” (McCullon, 2017). Furthermore, over 50 percent of American adults can be found in biometric databases that are used in criminal investigations. In 2011, Maryland police and other police forces started to use the Maryland Image Repository System (MIRS) (Jouvenal, 2018). Using a photo's facial features, this system matches the selected photo against millions of driver's license photos, a state offender database, and a mugshot database used by the FBI containing over 25 million mugshots. This is worrisome because these government agencies are using Americans' data without consent and most Americans are completely unaware, bringing ethics into the debate of how facial recognition systems should be used.

Many privacy organizations raise issues with MIRS and systems similar to it. The ACLU revealed that MIRS was used to identify individuals protesting the death of Freddie Gray, an African American man who was taken into custody in 2015 by Baltimore police and fell into a coma and eventually died due to spinal cord injury during his arrest. This is problematic because if law enforcement is tracking individuals attending political protests who are not breaking the law, then the police are violating their rights to privacy and free speech. Similarly, there is no information on whether the MIRS database is cleaned of people who were labelled as innocent or who had their charges dropped or dismissed (Jouvenal, 2018). Consequently, this technology is being increasingly used in law enforcement duties and requires further scrutiny in order to protect the privacy and principle rights of American citizens.

Aside from Federal and State regulation, big corporations must have their own law regarding the use of biometric data. For example, when companies such as Facebook combine these systems with data from their social media platforms, they are given too much power over people's private data. Facebook created a new feature on their site in December 2012 called "photo tag suggest" which allows facial recognition technology to label individuals in photos (Welinder, 2012). By October 2012, Facebook possessed a photo database of approximately 220 billion photos, which increases by 300 million photos daily and are tagged at a rate of 100 million tags per day. Facebook is also able to collect metadata from photos including the date, time and place a photo is taken by its users. The company encourages its users to fill out a well-rounded profile complete with “friending” other users, information on the users’ sexual orientation, hometown, work life, relationships, religious beliefs, and more. Facebook can also obtain data in other ways off of the actual Facebook website by asking users to sign into other sites using a Facebook login and through websites the company owns such as Instagram.

Connecting a face scan with other personal data falls under the category of data aggregation–a threat to privacy that many are unaware of but is very damaging to a person. Data aggregation includes combining data from different sources to create a more complete profile of a person. This occurs through Facebook’s facial recognition technology such as “photo tag suggest” with other distinctive information contained on their social media site. Furthermore, Facebook takes a photo that a user shares and turns this photo into a piece of biometric data by tagging the photo with Facebook’s facial recognition technology (Welinder, 2012). “Photo tag suggest” may also breach Children’s Online Privacy Protection Act (COPPA) by processing photos of 7.5 million users that are under 13 years old.

Because Facebook holds so much power by scanning the faces of its users and by collecting personal information from their profiles and other sites, Facebook must be required to operate under more regulation and users must be aware of the power this company holds over their privacy. Currently, Facebook asks all of their users to accept a “Privacy Agreement” and their “Terms and Conditions” which is written in very technical legal language that most people cannot understand, and many users do not bother reading. Even when companies gain consent, do consumers actually know what they are consenting to (e.g., such as the data they are giving up and what could happen to their data)? Facebook needs to ask for consent and provide their users with explicit information on how their data is used. Specifically, Facebook should provide easy-to-understand information of how a user's data is collected, processed, stored, shared, and deleted and when the data is used for a different purpose (Welinder, 2012). Furthermore, instead of fragmented state laws regarding biometric data privacy, more complete federal laws are needed. BIPA is a strong first step; however, this law is not enforced by any agency, but rather is a private act so the public needs technical expertise to understand their data and privacy rights in order to enforce this law. Facebook and other social media platforms are global companies, so their users are situated across the globe and are sharing photos, videos, and other data across country borders. Therefore, instead of privacy laws that only apply to certain states or countries, Facebook and companies like them must create regulations for biometric information privacy world-wide. Technology users must also be cognizant of how easily they share data and how this data can aggregate. Public education should be provided to children as technology becomes more widely used by all ages (Welinder, 2012). According to Professor Charles Fried's Control Theory, "Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves." Therefore, the public needs more understanding, awareness, and control over their own personal and private information. By becoming more cognizant of how social media companies like Facebook use their personal data, people can take the first step in controlling information about themselves and their own privacy.

## Issues with the Technology Within Corporations

As an emerging technology lacking regulation, many major companies have run into issues surrounding facial recognition within the realms of biometric privacy rights, security, and policing. Amazon came under scrutiny when the ACLU tested its facial recognition algorithm, Rekognition, against pictures of 535 members of Congress within a database of 25,000 public mugshots. The test revealed that 28 Congress members who were not a part of the mugshot database were falsely matched to mugshots of criminals within this database (Brandom, 2018). The ACLU used this test to raise issue with Amazon selling their facial recognition algorithms to local law enforcement agencies and police departments in Orlando and Washington County, Oregon (Martin, 2019). In Orlando, Florida, Amazon and the local police established a pilot program where seven officers volunteered to participate in scanning live footage from surveillance cameras to determine if individuals walking past the cameras match photos in a database containing images of missing people or wanted criminals. Furthermore, Amazon and the Washington County Sheriff's Department in Oregon compared surveillance feeds against a database containing approximately 300,000 mugshots. Amazon's partnership with police forces and the use of facial recognition technology by law enforcement raises alarms for citizens because police are able to use these systems not only to track individuals who are wanted as suspects for crimes but also to track people who can be categorized as nuisances by law enforcement. This may include groups such as political activists and protesters (O'Neill, 2019). The ACLU states that Rekognition is "unproven" and is "being deployed without any rules" claiming that this is problematic for citizens if the technology falsely accuses an individual for a crime. Therefore, opponents of this technology reject its use by law enforcement because the algorithms are not precise and because there are no rules or guidelines that control how the police use the technology.

Amazon is not the only tech giant that is facing criticism for their handling of facial recognition technology. After 2008 when BIPA was passed into law, many corporations' use of facial recognition was placed under intense scrutiny. In 2016, Facebook found themselves in trouble over their “photo tag suggest” tool. The company lost a court case involving three users from Illinois who sued the company under BIPA. As a class action complaint, BIPA allows every Facebook user in Illinois receive $1,000-$5,000 as penalty from Facebook for violating BIPA. Despite Facebook requesting to resolve the case under California law, which has no biometric data restrictions, the judge refused this plea and ruled that Illinois BIPA law should apply. The judge claimed that if the case is tried under California law, then BIPA’s authority of “protecting its citizens’ privacy interests in their biometric data, especially in the context of dealing with major national corporations like Facebook, would be written out of existence” (Roberts, 2016). Facebook appealed this ruling under the argument that they should be treated in the same way as Google was treated in their court battle. Google faced a similar case in federal court for the Google Photos tool that scans faces to create photo galleries in the Google Photos app. While the courts claimed that Google scanned users’ faces without consent, the court acknowledged that the users did not “demonstrate some sort of harm” and therefore were unable to collect compensation (Roberts, 2019). The distinguishing characteristic between the Facebook and Google court cases includes the reasons behind scanning the users’ faces: Facebook scans faces in photos in order to “tag” the face and sell user information to third parties whereas Google scans faces to organize a person’s photos into different galleries.

Tech giants are not the only organizations that are coming under scrutiny for biometric privacy violations. Six Flags Amusement Park also faced a lawsuit by Stacy Rosenbach whose 14-year old son was fingerprinted by Six Flags to authenticate his season pass (Perela, 2018). Rosenbach argues that Six Flags’s behavior is a direct violation of BIPA because the company did not obtain her permission to scan her son’s fingerprint and collect his biometric data. On the other hand, Six Flags’ claim is precisely the same as Facebook and Google’s argument: that in order to violate BIPA, the victim must demonstrate harm. This argument, however, would "limit the scope" of BIPA (Perela, 2018). Whether the court case involves a corporation like Facebook or Six Flags, the expansive use of facial recognition and other biometric technologies have run into a barrier in BIPA despite the tech industry's attempt to change the law in 2016 (Dune, 2016).

Shutterfly is yet another company that is facing litigation for collecting and storing facial recognition data, specifically pictures, on their website without explicit consent from their users. On September 15th, 2017 a judge denied Shutterfly's motion to dismiss their alleged BIPA violations (Hunton, Andrews & Kurth, 2017). In *Monroy v. Shutterfly, Inc.*, Shutterfly argued that BIPA biometric protection should not apply to photographs and that the user did not suffer any damage or harm from Shutterfly's actions. The judge dismissed these arguments, claiming that photographs are indeed considered a biometric identifier and that the user faced damages under his/her rights to privacy. With cases involving large technology companies moving forward in the courts, many other companies and retailers should be cautious when manipulating the biometric information of users–especially when damages could cost a company dearly. Furthermore, hopefully these cases regarding biometric data privacy raise public awareness to the issues of large corporations wrongfully manipulating such data.

While many large corporations have lobbied for less biometric privacy laws, Microsoft is one exception that is pushing for more regulation. In a company blog post published in 2018, Microsoft demanded more corporate responsibility for facial recognition systems as well as increased governmental regulations. Despite their own efforts in creating a facial recognition algorithm, they acknowledge that the technology is powerful but dangerous. Therefore, Microsoft develops their own technology under 6 key principles: fairness, transparency, accountability, non-discrimination, notice and consent, and lawful surveillance. The company understands that the uses of facial recognition systems are almost limitless in that the government could track citizens wherever they go whether it is to a political protest gathering allowed for under America's values of free speech, or to a shopping mall. This type of facial recognition tracking would neglect to obtain consent from its subjects and the data would be stored in a database for extended periods of time. Microsoft asks its fellow colleagues and the general public, "What role do we want this technology to play in everyday society?" This is an important question to consider, especially as the technology is being increasingly used for everyday tasks such as opening an IPhone or paying for a sandwich. Microsoft is seeking more proactive government regulation and has supported the establishment of the GDPR within the EU.

Other companies are taking steps to self-regulate. In April 2018, Axon released their intentions to establish an ethics board that would oversee their use of artificial intelligence in their products. This board meets twice a year to discuss the implications of Axon's products, especially if they apply to policing. This decision is monumental because Axon is currently the biggest provider of police body cameras within the United States, and the company recently filed for a patent regarding the use of real-time facial recognition systems (Vincent & Brandom, 2018). Many civil rights organizations wrote letters to the newly devised ethics board surrounding their worries of using real-time facial recognition–especially if there is a possibility that police officers could be equipped with these real-time facial recognition cameras within their jacket lapels to capture everything a police officer sees. Other police forces around the world are already utilizing real-time facial recognition, specifically in CCTV cameras in soccer stadiums within the UK and in train stations throughout China (Vincent & Brandom, 2018). Axon also has a cloud platform that contains over 20 million gigabytes worth of photos and videos from police body cameras. This cloud platform has categorized Axon as, “the largest custodian of public safety data in the United States and possibly the world” (Vincent & Brandom, 2018). The amount of data in Axon’s cloud is worrisome, along with governments’ ability to purchase facial recognition technologies made possible by the competitive nature of companies within the United States and other countries. Consequently, despite actions by Axon to follow ethical technological business procedures, real-time facial recognition may be an unavoidable reality in the near future.

Sometimes new regulation may seem restrictive but increased governmental regulation can benefit the public in the long run. During the 20th century, the government experienced resistance in their efforts to control the automobile industry. In retrospect, both consumers and automobile companies are grateful for the government initiatives that requires all automobiles to contain seat belts and airbags and for drivers to obtain licenses to drive safely. These automotive regulations decreased the number of deaths tremendously since the first car hit the road (Vardi, 2019). Similar to automobiles, information technology should also be regulated because this technology companies lack ethics. Many companies such as Google and Facebook are free for users to create an account; however, these companies profit through collecting user data and targeting advertisements to their consumers [See Figure 6]. This concept of “surveillance capitalism” popularized by Shoshana Zuboff illustrates the lack of ethics in information technology because companies are unwilling to alter their business models if they are making billions even if this is at the cost of the consumer’s privacy. Unfortunately, until these technology companies are forced to follow stronger laws surrounding facial recognition data these corporations will continue to operate on a lack of ethics in business practice with the sole focus on profitability.

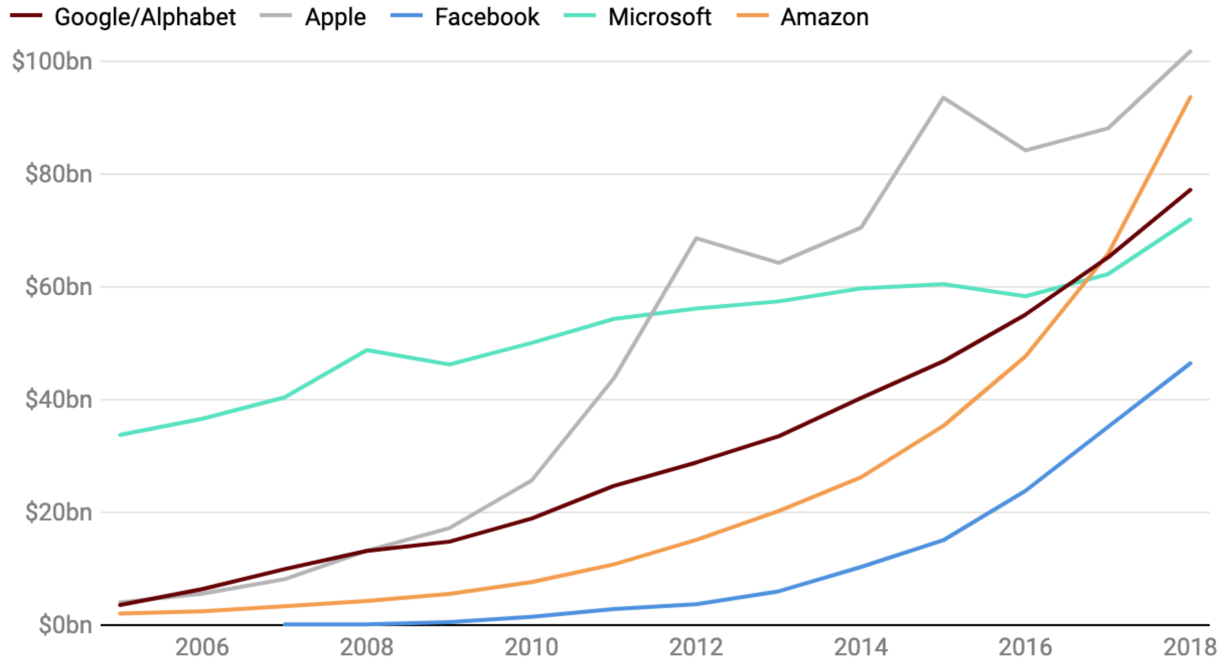


Figure 6. Profits by technology companies from personalized advertising, illustrating the rise of “surveillance capitalism” (Vardi, 2019).

## Cases of Facial Recognition in Court

As a technology that is arguably underdeveloped in its algorithm but is being implemented in surveillance cameras across the world, one may question the validity of using facial recognition as evidence within courts to convict or prove the innocence of individuals accused of a crime.  Facial recognition evidence was used for the first time in court in 2011: a California judge sentenced a man to 25 years of prison for an armed robbery and murder of another person (“A First: Biometrics Used to Sentence a Criminal”).  This decision was and continues to be controversial because the algorithms of these systems are not always accurate.

Therefore, if there is any chance that there was a false positive or negative, a person could be incorrectly sentenced or set free due to an error with the technology.

Advocates for using facial recognition systems in court claim that the technology is increasing in sophistication and will be invaluable for implicating criminals.  According to a Michigan Law Review, these systems will only increase in precision. The United States government has historically contributed to the technological advancement of facial recognition technology and will use these systems within the spheres of policing especially as the software is further developed.  The Department of Defense Counterdrug Technology Development Program funded the Face Recognition Technology Program (FERET) in 1993, the main goal of which was to further develop the technology.  Celentino (2016) argues that the number of databases containing face scans is growing tremendously, especially those used by the government, which is only helping train algorithms that will increase the precision of the technology and its value as evidence in court. The FBI created the Next Generation Identification database in September of 2014 containing over 100 million images that are available to at least 18,000 police forces. Collecting data, especially data of a person's face, is easier than ever before with the increase in video and photo technology through phones, cameras, and video systems.  With the affordability and prevalence of these cameras, catching a crime on video is becoming more common. According to law enforcement agencies, at least a quarter of crimes that are caught on tape contain the face of the perpetrator.  Consequently, government databases containing data for facial recognition systems are growing rapidly along with their use of these systems.

Even though advocates of the technology claim that these databases can train facial recognition algorithms to be more accurate and helpful in courts, the public must keep ethics in mind.  Computers have the capability of searching through millions of records in seconds;

however, until the algorithms are completely accurate, these systems should not be allowed to be used as evidence in court. The government has been compiling these databases for years and many people are completely ignorant because they are unaware that their information is being used to train facial recognition algorithms.  Proponents of the technology claim that facial recognition systems can help fight crime; however, nothing is stopping the government from using this technology to track people outside of the realm of crime. For instance, the government could track people’s whereabouts and monitor people’s activities.

Advocates of the technology also argue that facial recognition could help augment eyewitness testimonies, claiming that historically eyewitnesses have proven unreliable. However, to qualify as evidence in federal court, the evidence must “be evaluated for relevance and reliability” (Celentino, 2016).  Companies that produce facial recognition software believe that their technology will eventually be reliable and precise enough to meet court standards, especially with the growing amount of data within databases to train algorithms.  But this technology is definitely not reliable enough to act as evidence in court.  Furthermore, how will the public ever know if facial recognition technology is reliable enough when there are currently no regulation tests that check the accuracy of all algorithms? Different companies and producers of the technology from all over the world have different algorithms that are implemented in different systems worldwide, and none of these systems are standardized or regulated.  Different algorithms could be used in court and all of these algorithms have different accuracy rates. Therefore, how can these algorithms all be created equal in the face of the court?

## Potential for Bias Within the Algorithm

Introna & Wood (2004) describe how bias exists in the way facial recognition systems function.  The authors present two different methods utilized by facial recognition systems: template-based algorithms and feature based algorithms.  The template-based method calculates correlations between faces to estimate face identities against a standard template created from a gallery of face images.  The individual face identity is the difference and deviation from the general “standard” face.  The system inspects the database of faces and compares the newly presented face to the database.  Feature based algorithms analyze geometric relationships among local facial features using key facial elements such as eyes, noses, and mouths by measuring the distances and angles of these features to create unique faceprints.  The template-based method is biased because this method depends on the gallery used to develop the standard template; therefore, because minorities deviate the most from the standard, they may be easier to recognize.  Feature based algorithms are also biased because as the gallery increases, more faceprints are generated making the discrimination required for the recognition task more difficult.  Consequently, this system operates best with a small gallery and high-quality images.

Presenting the facial recognition systems as neutral and unproblematic disregards the fact that the technology is not entirely accurate. According to research conducted by the MIT Media Lab, facial recognition algorithms created by Microsoft, Face++ and IBM had false identifications 35 percent more for the detection of darker-skinned women compared to lighter-skinned males.  Therefore, this technology is perpetuating societal prejudices against women and minorities (Vincent, 2018).  The issue of bias arises partly because these algorithms are not trained on diverse data.  Because there is more footage of white people available as models, algorithms are typically trained on this footage so the databases themselves are often biased.

These algorithms can only be as effective and diverse as the data set they are trained on. Therefore, these algorithms are only as accurate and effective as the data they are trained on, especially because algorithms lack human common sense so if the training data is biased, then the results will also be biased.

Another issue of bias arises in the engineers who create the software. Psychological studies demonstrate the phenomenon of “the other race effect” or “the cross race effect” where people are better recognizing faces from their own race rather than faces from other races or faces they are more familiar with (Tanaka & Simonyi, 2016). A study conducted by the NIST in 2011 found that algorithms designed in Western Europe and the United States performed better on Caucasians while algorithms created in East Asia performed better on Asians. In this way, algorithmic bias imitates human cognitive bias and creates a “programmer’s bias” within this technology (McCullom, 2017).

Use of facial recognition in policing is problematic because there are no laws or regulations for law enforcement agencies to follow when using these systems. Georgetown Law released the most comprehensive report thus far on police use of facial recognition in their publication, “The Perpetual Line-Up: Unregulated Police Face Recognition in America” (Garvie, Bedoya & Frankle, 2016). According to this report, only 17 percent of agencies specified that they monitor employee use of facial recognition systems for misuse. Previously, law enforcement databases typically contained criminal samples such as fingerprints and DNA. For instance, the Federal Bureau of Investigation’s National DNA Index System, a national DNA database, contains only DNA information of criminals (Triplett, 2017). FACE Services, the Federal Bureau of Investigation’s facial recognition unit, disrupts this pattern by using driver’s license photos from 16 states as well as photos from American passport and visa applications.

Between August 2011 through December 2015, the FBI ran approximately 214,920 face searches of which 118,490 searches were in its own database and 36,420 were searches within the driver's license and mug shot database. Similarly, of all American local and state police agencies, one of four can run their own facial recognition technology or have access to other facial recognition systems.

Algorithmic bias in facial recognition technology becomes a larger issue due to the implications and consequences this software has for different races in law enforcement and policing. Researchers at the Center on Privacy and Technology at Georgetown Law filed a freedom of information lawsuit against the New York Police Department because the department denied access to information about its use of facial recognition technology (McCullom, 2017). Use of facial recognition software in policing has created the idea of a "digital lineup" or "virtual lineup" where algorithms are replacing eyewitnesses. Facial recognition systems were designed to merge human perceptual abilities with the memory and processing power of a computer (Welinder, 2012). Humans identify each other according to appearance and face, but the human brain also combines facial features with other senses. A surveillance system is unable to combine a face scan with other characteristics of unique human perception such as contextual knowledge like a sense of smell or what clothes a person typically wears. To make matters worse, the algorithmic bias is particularly problematic because the identification rates are consistently lower for African Americans with rates of at least five to 10 percent lower compared to white faces (McCullom, 2017). In this way, the technology will create larger issues because it will be used on a population that is already highly scrutinized by law enforcement. According to the researchers at Georgetown Law, facial recognition technology "is likely to be overused on the segment of the population on which it underperforms" (Garvie, Bedoya & Frankle, 2016).

There will be higher false-positives for African Americans, leading to more stops and arrests. Individuals should be incredibly concerned if the public accepts a technology that is inaccurate and constantly perform false positives, the nature of which requires people to defend themselves against acts they did not commit. Therefore, this technology will frequently misidentify an African American suspect, causing them to be under increased police inspection due to technological fault.

Joy Buolamwini, a fierce advocate for increasing scrutiny of facial recognition systems, is a researcher at the MIT Media Lab and founder of the Algorithmic Justice League, an advocate group for fighting bias in machine learning systems. She describes facial recognition algorithms as “the coded gaze” which directly relates to the sociological concept “the white gaze” implying that the technology takes on the perspective of a white person and assumes the audience is always white (McCullom, 2017). Buolamwini acknowledges the inevitability of the use of facial recognition systems and argues, “we have to look at how we give machines sight.” Buolamwini published a paper investigating algorithmic performance on classifying gender and skin tone of prominent facial recognition software from IBM, Megvii, and Microsoft. IBM and Megvii had error rates for darker-skinned females of approximately 35 percent while Microsoft had error rates of 21 percent (Lohr, 2018). Due to the minority underrepresentation in STEM fields, if African Americans are not part of the engineers writing the code that helps to identify faces, then those systems will have data gaps and failures in identifying black faces. Allowing for more equity in computer engineering for facial recognition software, such as African Americans being able to help code algorithms, may help this bias issue. Increasing awareness and the inclusivity of coding and engineering of facial recognition algorithms may be one part of the solution to solving this bias issue.

A biometric visual surveillance technology like facial recognition is characterized as flexible and very useful by advocates for the technology.  However, the software cannot be isolated from the bias within the software algorithms and the fact that these systems are being deployed within specific political, social and global contexts.  According to the President of Ford Foundation, “There is a battle going on for fairness, inclusion, and justice in the digital world” (Lohr, 2018).  The lack of diversity within the machine learning community and the lack of standards and guidelines for improving accuracy for this technology has created issues with algorithmic bias in facial recognition software.  The National Institute of Standards of Technology (NIST) has examined facial recognition studies every few years since the mid 1990s but has investigated bias within this technology only one time.  Individual companies are developing and testing their software systems; however, there needs to be more regulation and benchmark tests to ensure that all facial recognition technologies are efficient and accurate. When powerful tools such as facial recognition are used by the government, the stakes are higher because government agencies have more power and access to tremendous amounts of data (Lohr, 2018).  As Buolamwini claims “the technical considerations cannot be divorced from the social implications.” Therefore, individuals must consider technological artifacts like facial recognition within the social landscape in which it is embedded.  As the FRVT is currently the only test that investigates accuracy within these systems, expanding it and making it mandatory is one possible avenue (Vincent, 2018).   Similarly, the unregulated use of facial recognition systems by the government whether it is within a shopping mall, airport, sports stadium, or by law enforcement, is giving the government a granular and intrusive level of control over the public.  If one thing is certain with this technology, it is that facial recognition systems will remain very influential in the future and therefore the public to increase their awareness, scrutiny, and push back against unethical corporate and governmental uses of this technology.

## Concluding Thoughts

Facial recognition is a pervasive technology that lacks regulation as well as accuracy in the algorithms it uses, leading to racial biases and tremendous social consequences. As a biometric identifier, facial recognition is the most efficient and least intrusive; however, face scans are segments of data that require official laws to control the way companies and organizations can use such valuable, private information. Even though the European Union has enacted stringent laws regarding biometric data, only three out of 50 states have any semblance of a biometric privacy law that restricts how companies can collect and manipulate a person's personal biometric information. Furthermore, if corporations like Facebook and Amazon are creating facial recognition software, then these companies are able to combine data from their software with personal data they collect on their website and platform. While companies like Facebook advertise their service as "free," users are paying for this platform with their data. The *Economist* stated in 2017 that, "the world's most valuable resource is no longer oil, but data." This is very dangerous because these corporations are aggregating data that could create a complete profile on users containing both biometric and personal data potentially used for intrusive or malicious purposes, such as targeted advertising, invasion of privacy, or, in politics for opposition research. Consequently, it is absolutely necessary that companies face more rigorous regulation and that consumers become more informed about these threats to their privacy so they can fight for their rights when their privacy is violated.

As front runners in facial recognition technology, U.S. companies have responsibility to understand the implications of the technology they are creating. Like Axon's recently developed ethics board, every company should take steps to ensure that the technologies they are producing are taking into account societal welfare by considering all implications of their products. The public also needs more transparency, responsibility, and awareness of the way facial recognition operates and the consequences of its use. Most consumers are ignorant in how corporations use facial recognition systems and are therefore incapable of policing these networks and demanding recompense for when their rights are violated. With society becoming increasingly reliant on technology and with the growing value of using technology as an easy, efficient way of completing tasks, facial recognition systems are not disappearing any time soon.

It is also important to recognize that these systems are advancing rapidly and combining two highly contested technologies: video surveillance and the scanning of face prints. Even though information on how facial recognition systems work will eventually become outdated, the social implications of the technology will stay relevant. In the near future, facial recognition systems may be combined with other disruptive technologies such as drones in which facial recognition systems would know no boundaries and be completely invisible to the victim. Currently, China is establishing a surveillance state with networks of video surveillance operating 24/7. China contained 176 million surveillance cameras in 2017 and this number is predicted to increase to 626 million cameras by 2020 (Gemalto, 2018). Therefore, spreading awareness to the public of how these contentious systems are currently functioning and the issues with the systems is important as this product grows in popularity and use and also as a warning of what the technology could potentially lead to. It is important to understand that, as the saying goes, “with great power comes great responsibility”—the process of using a powerful technology demands proper action and accountability. In this way, facial recognition is a disruptive technology because of the hidden dangers when these systems recognize faces.

# Works Cited

“A First: Biometrics Used to Sentence a Criminal.” 1 February 2011. Homeland Security Newswire. News Wire Publications. www.homelandsecuritynewswire.com/first-biometrics-used-sentence-criminal.

Alba, Davey. 12 Mar. 2019 “The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show.” *BuzzFeed News*, BuzzFeed News. www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for.

Aratani, Lori. 15 Sept. 2018. “Facial-Recognition Scanners at Airports Raise Privacy Concerns.” *The Washington Post*, WP Company. www.washingtonpost.com/local/trafficandcommuting,/facial-recognition-scanners-at-airports-raise-privacy-concerns/2018/09/15/a312f6d0-abce-11e8-a8d7-0f63ab8b1370_story.html?noredirect=on&utm_term=.3186fdeb2d67.

Bewley-Taylor, D. R. (2006). Watch this space: Civil liberties, concept wars and the future of the urban fortress. *Journal of American Studies, 40*(2), 233-255. doi:10.1017/S0021875806001368

“Biometric Data and the General Data Protection Regulation.” 2018. *Gemalto*. www.gemalto.com/govt/biometrics/biometric-data.

Bonsor, K & Johnson, R. (2001) "How Facial Recognition Systems Work" HowStuffWorks.com. <https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial recognition.htm> 23 April 2019.

Brandom, Russell. 26 July 2018 "Amazon's Facial Recognition Matched 28 Members of Congress to Criminal Mugshots." The Verge. https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition.

Brey, P. (2004). Ethical aspects of facial recognition systems in public places. *Journal of Information, Communication and Ethics in Society, 2*(2), 97-109. doi:10.1108/14779960480000246

Cardinal, David. 14 Dec. 2018. "Worried Amazon Will Add Facial Recognition to Doorbells? Too Late." *ExtremeTech*. www.extremetech.com/electronics/282227-worried-amazon-will-add-facial-recognition-o-doorbells-too-late.

CBP Report. 13 June, 2016. "CBP Deploys Test of Departure Information Systems Technology at Hartsfield–Jackson Atlanta International Airport." *U.S. Customs and Border Protection*, www.cbp.gov/newsroom/local-media-release/cbp-deploys-test-departure-information-systems-technology-hartsfield.

Celentino, Joseph Clarke. Face-To-Face with Facial Recognition Evidence: Admissibility Under The Post-Crawford Confrontation Clause. *Michigan Law Review*. Vol. 114, Issue 7. (2016). http://repository.law.umich.edu/mlr/vol114/iss7/3

Cuthbertson, Anthony. "Police Trace 3,000 Missing Children in Just Four Days Using Facial Recognition Technology." *The Independent*, Independent Digital News and Media, 24 Apr. 2018. www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-acial-recognition-tech-trace-find-reunite-a8320406.html.

"Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility." 17 July 2018. *Microsoft Green Blog*. blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/.

Fortin, Jacey. 19 January 2019. “Are '10-Year Challenge' Photos a Boon to Facebook's Facial Recognition Technology?” *The New York Times*, The New York Times. www.nytimes.com/2019/01/19/technology/facebook-ten-year-challenge.html.

Garvie, Clare., Bedoya, Alvaro M., & Frankle, Jonathan. The Perpetual Line-Up: Unregulated Police Face Recognition in America. Georgetown Law Center for Privacy and Technology. October 18, 2016.

Gibbs, Samuel. 30 May 2018. “Google Launches Video Doorbell with Facial Recognition in UK.” *The Guardian*, Guardian News and Media, www.theguardian.com/technology/2018/may/31/nest-hello-google-launches-facial-recognition-data-doorbell-uk-privacy-concerns-amazon-ring.

Grennan, Matthew & Town, Robert. “The FDA and the Regulation of Medical Device Innovation.” *Wharton Public Policy Initiative*, publicpolicy.wharton.upenn.edu/issue-brief/v4n2.php.

Grm, Klemen., Sˇtruc, Vitomir., Artiges, Anais., Caron, Matthieu., Ekenel, Hazim Kemal. 4 October 2017. Strengths and Weaknesses of Deep Learning Models for Face Recognition Against Image Degradations. *IET Biometrics.*

Hunton, Andrews & Kurth. 14 October 2017. “Facing Privacy Suits About Facial Recognition: BIPA Cases Move Forward as More States Consider Passing Biometric Data Laws.” *Privacy & Information Security Law Blog*, www.huntonprivacyblog.com/2017/10/04/facing-privacy-suits-about-facial-recognition-ipa-cases-move-forward-as-more-states-consider-passing-biometric-data-laws/.

Introna, L. D., & Wood, D. (2004). Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance and Society*, *2*(2-3), 177-198. Retrieved From www.scopus.com

James, Mike. 25 April 2014. "GaussianFace Recognizes Faces Better Than Humans." *Programmer* www.i-programmer.info/news/105-artificial-intelligence/7223-gaussianface-recognizes-faces-better-than-humans.html.

Johnson, Tim. 21 May 2018. "Shoplifters Meet Their Match as Retailers Deploy Facial Recognition Cameras." McClatchy Washington Bureau. www.mcclatchydc.com/news/nation-world/national/article211455924.html#storylink=cy.

Jouvenal, Justin. 29 June 2018. "Police Used Facial-Recognition Software to Identify Suspect in Newspaper Shooting." *The Washington Post*, WP Company. www.washingtonpost.com/local/public-safety/police-used-facial-recognition-software-to-identify-suspect-in-newspaper-shooting/2018/06/29/6dc9d212-7bba-11e8-aeee-4d04c8ac6158_story.html?noredirect=on&utm_term=.b3430fcbbd6f.

Lawrence, Dune. 7 July 2016. "Do You Own Your Own Fingerprints?" *Bloomberg.com*, Bloomberg. www.bloomberg.com/news/articles/2016-07-07/do-you-own-your-own-fingerprints.

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

Marine, Erin. 20 March 2018. "Biometric Privacy Laws: Illinois and the Fight Against Intrusive Tech." *Fordham Journal of Corporate and Financial Law*.

news.law.fordham.edu/jcfl/2018/03/20/biometric-privacy-laws-illinois-and-the-fight-against-intrusive-tech/.

Martin, Nicole. 17 January 2019. “Was The Facebook '10 Year Challenge' A Way To Mine Data For Facial Recognition AI?” *Forbes*, Forbes Magazine. www.forbes.com/sites/nicolemartin1/2019/01/17/was-the-facebook-10-year-challenge-a-way-to mine-data-for-facial-recognition-ai/#706fa9c85859.

McCullom, Rod, David Collier-Brown, & Rick Guasco. 17 May 2017. "Facial Recognition Technology Is Both Biased and Understudied." Undark https://undark.org/article/facialrecognition-technology-biased-understudied/.

Merriam-Webster, “Algorithm.” Merriam-Webster. www.merriam-webster.com/dictionary/algorithm.

Meyer, David. May 7 2018 “Police Tested Facial Recognition at a Major Sporting Event. The Results Were Disastrous.” *Fortune*, fortune.com/2018/05/07/wales-police-champions-league-facial-recognition/.

O'Neill, Kate. 16 January 2019. “Facebook's '10 Year Challenge' Is Just a Harmless Meme-Right?” *Wired*, Conde Nast. www.wired.com/story/facebook-10-year-meme-challenge/.

Owen, David. “Here’s Looking at You” 17 December 2018. The New Yorker

Perela, Alex. 28 November 2018. “Pivotal Biometrics Lawsuit Gets Underway Before Illinois Supreme Court.” *FindBiometrics*, findbiometrics.com/pivotal-biometrics-lawsuit-illinois supreme-court-511282/.

Pickering, S., & Weber, L. (2006). Borders, mobility and technologies of control. *Borders, mobility and technologies of control* (pp. 1-222) doi:10.1007/1-4020-4899-8 Retrieved fromwww.scopus.com

Ratanaphanyarat, Carissa. 2018. “Biometric Privacy Laws: Do They Exist and Why Should You Care?” *Smart Speakers and Voice Recognition: Is Your Privacy at Risk? – NextAdvisor Blog*, www.nextadvisor.com/blog/biometric-privacy-laws/.

Roberts, Jeff. 6 May 2016. “Facebook Just Lost a Major Case Over Face Scanning.” *Fortune*, Fortune, fortune.com/2016/05/06/facebook-biometrics/.

Roberts, Jeff. 4 January 2019. “Google, Facebook, and the Legal Mess Over Face Scanning.” *Fortune*, Fortune, fortune.com/2019/01/04/google-face-scanning-illinois/.

Rosen, Jeffrey. "A Watchful State." The New York Times. October 07, 2001. https://www.nytimes.com/2001/10/07/magazine/a-watchful-state.html.

Rubin, Ben Fox. 14 December 2018. “Amazon's Ring Takes Heat for Considering Facial Recognition for Its Video Doorbells.” *CNET*, CNET. www.cnet.com/news/amazons-ring-takes-heat-for-considering-facial-recognition-for-itsvideo-doorbells/.

Saetnan, A. R. (2007). Nothing to hide, nothing to fear?: Assessing technologies for diagnosis of security risks. *International Criminal Justice Review, 17*(3), 193-206. doi:10.1177/1057567707306651

Saha, Sumit. 15 Dec. 2018 “A Comprehensive Guide to Convolutional Neural Networks-the ELI5 Way.” *Towards Data Science.* towardsdatascience.com/a-comprehensive-guide-to-convolutional-neural-networks-the-eli5-way-3bd2b1164a53.

Silverstein, Jason. 17 January 2019. “Is the ‘10 Year Challenge’ on Facebook a Privacy Scheme Disguised as a Meme?” *CBS News*, CBS Interactive. www.cbsnews.com/news/facebook-10-year-challenge-meme-could-it-mine-your-data-facial-recognition/.

Tanaka, J.W. & Simonyi, D. The “parts and wholes” of face recognition: a review of the literature. March 4th, 2016. The Quarterly Journal of Experimental Psychology, Vol. 69, No. 10, 1876–1889, http://dx.doi.org/10.1080/17470218.2016.1146780

Technopedia. (2019). “What Is a Deep Neural Network? *Techopedia.com*, www.techopedia.com/definition/32902/deep-neural-network.

Thakkar, Danny. 23 Aug. 2018. “U.S. States Enact Biometric Information Privacy Act.” *Bayometric*, Bayometric, www.bayometric.com/u-s-states-enact-bipa/.

Vardi, Moshe Y. 22 Mar. 2019. “Cars Are Regulated for Safety – Why Not Information Technology?” *The Conversation*. theconversation.com/cars-are-regulated-for-safety-why-not-information-technology-111415.

Vincent, James. 26 July 2018. "The Tech Industry Doesn't Have a Plan for Dealing with Bias in Facial Recognition." The Verge. https://www.theverge.com/2018/7/26/17616290/facial-recognition-ai-bias-benchmark-test.

Vincent, James, and Russell Brandom. 26 Apr. 2018. “Axon Launches AI Ethics Board to Study the Dangers of Facial Recognition.” *The Verge*, The Verge. www.theverge.com/2018/4/26/17285034/axon-ai-ethics-board-facial-recognition-racial-bias.

Weinberg, A. M. (1966). Can technology replace social engineering?. *Bulletin of the Atomic Scientists*, *22*(10), 4-8.

Welinder, Yana. (2012). A Face Tells More Than a Thousand Posts: Developing Face Recognition Privacy in Social Networks. *Harvard Journal of Law & Technology*. Volume 26, Number 1, 166-239.

West, Jesse. 1 August 2017. “History of Face Recognition - Facial Recognition Software.” *FaceFirst Face Recognition Software*, www.facefirst.com/blog/brief-history-of-face-recognition-software/.