

The Future of Facial Recognition:
Is it an Invasion of Privacy or do the
Benefits Outweigh the Detriments?

Savannah Price

21 April 2021

Facial recognition is a biometric technology that is somewhat new to everyday life, and its usage and popularity only continues to grow with time. Even over the past couple years, not only has the accuracy dramatically improved, but more businesses are beginning to integrate the utilization of facial recognition into everyday items and platforms. For example, in 2017, Apple introduced facial recognition with its iPhone X, allowing its consumers to ‘unlock’ their iPhones by simply looking at the screen.¹ Facial recognition was created by Woody Bledsoe, Helen Chan Wolf, and Charles Bisson between 1964 and 1965.² Since the creation, the accuracy of the biometric technologies has only improved. A commonly asked question from the public is: how does it work? Facial recognition uses millions of algorithms, and according to eff.org (Electronic Frontier Foundation), and specifically looks at the “distance between the eyes or shape of the chin” which is “then converted into a mathematical representation.”³ Although the technology has been around for nearly five decades, the United States of America has only recently implemented facial recognition into everyday life in the aftermath of the September 11, 2001 attacks in New York City. Since then, it has been used for identifying criminals, terrorists, kidnappings, rape, etc.⁴ While the biometric technology has many benefits, there is one main issue common amongst the general public: does facial recognition invade one’s privacy? The

¹ Pocket-lint, “What Is Apple Face ID and How Does It Work?,” Pocket, February 2, 2021, [https://www.pocket-lint.com/phones/news/apple/142207-what-is-apple-face-id-and-how-does-it-work#:~:text=\(Pocket%2Dlint\)%20%2D%20Apple's,found%20on%20future%20iPhones%20too](https://www.pocket-lint.com/phones/news/apple/142207-what-is-apple-face-id-and-how-does-it-work#:~:text=(Pocket%2Dlint)%20%2D%20Apple's,found%20on%20future%20iPhones%20too).

² “A Brief History of Facial Recognition - NEC New Zealand,” NEC, September 9, 2020, <https://www.nec.co.nz/market-leadership/publications-media/a-brief-history-of-facial-recognition/#:~:text=The%20earliest%20pioneers%20of%20facial,to%20recognise%20the%20human%20face.&text=These%20were%20then%20mathematically%20rotated,to%20compensate%20for%20pose%20variation>.

³ “Face Recognition,” Electronic Frontier Foundation, February 15, 2021, <https://www.eff.org/pages/face-recognition#:~:text=Face%20recognition%20systems%20use%20computer,in%20a%20face%20recognition%20database>.

⁴ Jake Parker, “Facial Recognition Success Stories Showcase Positive Use Cases of the Technology,” Security Industry Association, December 10, 2020, <https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/>.

general public has a difficult time defining the line between an invasion of privacy and public safety and security, especially those whose knowledge is limited on the subject. As any other new technology, especially one with such prevalent privacy concerns, many lawsuits regarding facial recognition have taken place over the years. One of the most recent lawsuits regarding the topic is against one of the largest social media platforms, if not the largest: Facebook. Although the concern from the public about the newer biometric technology is understandable, facial recognition has many benefits, perhaps even more benefits than detriments. As history has shown, facial recognition technologies will only continue to expand and be used more commonly from day to day, but before reaching that point, the public must come to a general consensus on whether or not the intrusion of privacy is worth the public safety benefits.

The history of facial recognition dates back as early as 1964; however, the most similar version of the biometric technology that society knows today was presented “at the 1970s World’s Fair in Osaka, Japan, the Nippon Electric Company (NEC) staged an attraction called “Computer Physiognomy.”⁵ When presented at the fair, people lined up to have their faces scanned and the technology would then present to them their most defining features. Although federal agencies and companies now use the technology for other purposes than merely entertainment, the concept of gathering facial features to identify certain parts of someone’s face originated from the “Computer Physiognomy.” Since that first pop up booth at the World Fair in 1970, scientists and mathematicians have been working on the science behind the biometric technology. Later on in the 1970s, employees of NEC named Goldstein, Harmon, and Lesk further advanced the technology. This time around, they created an algorithm that “include[d] 21 specific subjective markers including hair colour and lip thickness in order to automate the

⁵ Kelly Gates, “Facial Recognition Technology From the Lab to the Marketplace,” in *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York, New York: New York University Press, 2011), pp. 25-25.

recognition.”⁶ While the updated technology provided more information and had a higher accuracy rate, it still was not good enough, or ready to be used on any large scale. Additionally, the information had to be manually recorded, which branded time as the scientists’ largest enemy. Furthermore, years later, “in 1988, Sirovich and Kirby began applying linear algebra to the problem of facial recognition.”⁷ Not only did Sirovich and Kirby completely revolutionize what people once thought of as “facial recognition,” but they paved the path for future scientists. “A system that came to be known as Eigenface showed that feature analysis on a collection of facial images could form a set of basic features. They were also able to show that less than one hundred values were required in order to accurately code a normalized facial image.”⁸ Moreover, the thought of the utilization of biometric technologies as facial recognition was no longer a surreal idea. Following Sirovich and Kirby’s success, Turk and Pentland continued advancing the processes and technology of facial recognition. What may be considered as the most important research in biometric technology, they “discover[ed] how to detect faces within an image which led to the earliest instances of automatic facial recognition.” The technology no longer had to be manually inputted, and time was no longer the enemy. What many would call an outstanding “breakthrough,” this 1991 mathematical invention was the beginning of the kind of facial recognition that society knows today.

With biometric facial recognition on the rise, the United States Government knew they needed to quickly organize and develop a sector solely dedicated to this up and coming technology, which is why the Facial Recognition Technology program was created. Known as FERET, the program is a subset of The Defence Advanced Research Projects Agency (DARPA) and the National Institute of Standards and Technology (NIST). Now that the facial recognition

⁶ “A Brief History of Facial Recognition - NEC New Zealand,” NEC, September 9, 2020, <https://www.nec.co.nz>.

⁷ “A Brief History of Facial Recognition - NEC New Zealand,” NEC, September 9, 2020, <https://www.nec.co.nz>.

⁸ “A Brief History of Facial Recognition - NEC New Zealand,” NEC, September 9, 2020, <https://www.nec.co.nz>.

technologies were mainly in the hands of the United States government, the privacy concerns began to arise. In the early 2000s, The National Institute of Standards and Technology (NIST) began Face Recognition Vendor Tests (FRVT).”These evaluations were designed to provide law enforcement agencies and the U.S. government with information necessary to determine the best ways to deploy facial recognition technology.”⁹ The history of facial recognition is vast, and has taken nearly fifty years to reach the point that it has come to today. Although the history of facial recognition is interesting and important to know, the science and mathematics behind the biometrics are just as vital to its existence.

The algorithms and scientific research behind the biometric technology of facial recognition is beyond the average person’s comprehension, yet the simplicity and straightforwardness of it is beautiful at the same time. While the science of facial recognition has nearly been perfected, there is no way to know that it is one-hundred percent accurate, or if it ever will be. Although today scientists and mathematicians have come closer to one hundred percent accuracy than ever before, the algorithms behind the science still lead to imperfections and inaccuracies. As stated before, facial recognition algorithms identify and calculate certain parts of the human face, and then associate each unique trait with an individual. The issue is that some people look complexly more alike than others, and if the system doesn’t catch onto these intricate differences, the likelihood of falsified information and inaccurate recognition dramatically increases. When it comes to using facial recognition for catching criminals, according to the Electronic Frontier Foundation, “facial recognition software is particularly bad at recognizing African Americans and other ethnic minorities, women, and young people, often misidentifying or failing to identify them, disparately impacting certain groups.”¹⁰ To break

⁹ “A Brief History of Facial Recognition - NEC New Zealand,” NEC, September 9, 2020, <https://www.nec.co.nz>.

¹⁰ “Face Recognition,” Electronic Frontier Foundation, February 15, 2021, <https://www EFF.org/pages/face-recognition>.

down the six basic steps of how the biometric technology works, it looks like this: 1. Image is captured; 2. Eye locations are determined; 3. Image is converted to grayscale and cropped to only the shape of the face; 4. Image is converted to a template used by the search engine for facial comparison results; 5. Image is searched and matched using a sophisticated algorithm to compare the template to other templates on file; 6. Duplicate licenses are investigated for fraud.¹¹ Knowing that the possibility of misrecognition is substantial, some systems are designed to give multiple options of potential matches, rather than identifying a single person. More specifically, these algorithms are “designed to calculate a probability match score between the unknown person and specific face templates stored in the database.”¹² Although the science behind this biometric technology seems clear and simple, it is made up of millions of algorithms and pre-existing data in order for the modern day uses of facial recognition to be as accurate as possible.

The first time the United States government fully, publicly recognized the importance and value of utilizing facial recognition biometric technologies was after the September 11, 2001 attacks on the twin towers in New York City. Amongst the chaos and uncertainty felt by an entire nation, the US government needed to act on their feet, and as quickly as possible. One particular glimpse of hope to catch the terrorists who orchestrated the attack was a piece of film footage of suspected terrorist, Mohamed Atta, passing through security in the Portland, Oregon airport.¹³ The US government and others began to think that if facial recognition had been installed prior to the attacks, there could have been a chance of catching the known threat (Atta) before he had the chance to hijack the aircraft. “The idea that computerized face recognition may have helped

¹¹ “Securing Your Identity - Transportation Matters for Iowa: Iowa DOT,” Transportation Matters for Iowa | Iowa DOT, accessed April 20, 2021, <https://www.transportationmatters.iowadot.gov/2014/05/securing-your-identity-.html>.

¹² “Face Recognition,” Electronic Frontier Foundation, February 15, 2021, <https://www.eff.org/pages/face-recognition>.

¹³ Kelly A. Gates; Biometrics and Post-9/11 Technostalgia. *Social Text* 1 June 2005; 23 (2 (83)): 35–53.

avert the al-Qaeda terrorist attacks was perhaps the most ambitious claim circulating about biometric identification technologies in the aftermath of September 11.”¹⁴ At this moment in time, it became clear to not only the US government, but the public that facial recognition may have more safety benefits than initially assumed.

Whether people are aware of it or not, facial recognition is used in everyday life now and has gotten to the point where it is unavoidable. In 2017, Apple Inc. incorporated facial recognition into the iPhone X, which was a monumental step for smartphones and biometric technology as a whole. The integration of facial recognition into everyday life had officially been introduced to society, and people had mixed feelings. Some believed it made accessing their iPhone more convenient, while others worried about what kind of personal data Apple was receiving, and where it was going. Although the technology is being used for convenience and everyday purposes now, it is still being used for what it was originally intended for: catching criminals. For example, in 1977, a murderer named James Robert Jones escaped a military prison at Fort Leavenworth in Kansas. He escaped a 23-year prison sentence for killing a fellow soldier, and lived under the alias Bruce Walter Keith for 40 years in Florida.¹⁵ Little did he know, 40 years after his escape, Jones was arrested after a facial recognition system identified him from a database that housed Florida state drivers’ license photographs. Furthermore, although Jones’ instance is solely one example of tens of—if not hundreds of—thousands, it proves that there are genuinely useful factors of facial recognition, aside from the fun uses like Apple’s iPhone X.

More recently, the Transportation Security Administration (TSA) has implemented facial recognition into its customs and border control into its Global Entry security checkpoints across

¹⁴ Kelly A. Gates; Biometrics and Post-9/11 Technostalgia.

¹⁵ Davis, Wendy N. "Face Time: Facial Recognition Technology Helps Nab Criminals—and Raises Privacy Concerns." ABA Journal 103, no. 10 (2017): 16-18. Accessed April 20, 2021. <https://www-jstor-org.access.library.miami.edu/stable/26516097>.

America. Global Entry is a United States Customs and Border Protection (CBP) program that expedites ‘trusted travelers’ customs process after returning to the US from international travel.¹⁶ Upon deplaning, travelers are ushered to the Customs and Border Protection checkpoint where the members of Global Entry file into their own line. When a machine becomes available, the ‘trusted traveler’ proceeds and takes a picture of their face using the camera on the machine. Then, a slip of paper with the picture of the traveler is dispensed from the machine. The paper contains information such as: name, date of birth, flight number, etc.. While people may be shocked that the machine knows nearly every single fact that identifies a human being, Global Entry, CBP, and TSA argue that it is for the safety of all travelers. By using facial recognition in and throughout airports around the world, it prevents dangerous individuals, such as known terrorists, to sneak through the system.¹⁷ Facial recognition in places that have a specifically high demand for safety protocols is highly beneficial and, at this point, arguably essential. It all comes down to determining whether the intrusion of privacy, as some may see it, is worth the extra safety measures; however, not all government officials view it as a positive addition to society.

On May 14, 2019, one of the most influential cities in the United States shocked the rest of the country, the nationwide news read in papers and on screen: “San Francisco Bans Facial Recognition Technology.”¹⁸ The most shocking part of the announcement is that just miles away from San Francisco, in the outskirts, lies the technology capital of the United States: Silicon Valley. Ironically, a substantial amount of the biometric technology that is used in America is

¹⁶ “Global Entry,” U.S. Customs and Border Protection, accessed April 20, 2021, <https://www.cbp.gov/travel/trusted-traveler-programs/global-entry>.

¹⁷ Lewis, James A., and William Crumpler. Report. Center for Strategic and International Studies (CSIS), 2021. Accessed April 20, 2021. <http://www.jstor.org/stable/resrep28766>.

¹⁸ Conger, Kate, Richard Fausset, and Serge F. Kovaleski. "San Francisco bans facial recognition technology." *The New York Times* 14 (2019).

developed in Silicon Valley.¹⁹ San Francisco was the first city to ban facial recognition technology in America, which prevents police forces from using it to capture criminals on large and small scales. Although the ban of facial recognition in a smaller town or city would not have as large of an impact, since San Francisco is one of the largest metropolitans in the United States, the ban has a wider effect than the public is able to comprehend. According to an article from the *New York Times* by Quentin Fottrell, the reason San Francisco got to the point of banning facial recognition was that “civil liberty groups [had] expressed unease about the technology’s potential abuse by government amid fears that it may shove the United States in the direction of an overly oppressive surveillance state.” Unfortunately, the voting to ban the technology has begun to turn the once-solely safety and privacy issue into a political issue as well, distracting society from the facts and benefits. Following San Francisco’s lead, twelve other cities in the United States have also banned facial recognition technologies. These cities include: Boston, Massachusetts; Portland, Oregon; Springfield, Massachusetts; among nine others.²⁰ Furthermore, in light of the current social movements such as Black Lives Matter and Asian and Pacific Islander Forward Movement, society should expect for more larger metropolitan areas to ban facial recognition technologies.

Facial recognition technology has recently received severe backlash for misidentifying minority groups and people of color, specifically African Americans. According to an article from the American Society for Engineering Education (ASEE), facial recognition has a higher chance of falsely recognizing people of color, but more specifically black women.²¹ According to

¹⁹ Quentin Fottrell, “Silicon Valley's Final Frontier for Payments: 'The Neoliberal Takeover of the Human Body',” *MarketWatch* (MarketWatch, October 23, 2019), <https://www.marketwatch.com/story/the-technology-that-should-finally-make-your-wallet-obsolete-2019-09-06>.

²⁰ Shannon Flynn, “13 Cities Where Police Are Banned From Using Facial Recognition Tech,” *Innovation & Tech Today*, November 16, 2020, <https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/>.

²¹ T.G. "FACIAL RECOGNITION: TRANSCENDING BIAS." *ASEE Prism* 29, no. 4 (2019): 10. Accessed April 20, 2021. <https://www-jstor-org.access.library.miami.edu/stable/26844536>.

statistics from Harvard University, the accuracy rate for caucasian adults sits at over 90 percent, while the accuracy rate for darker skinned adults at times falls below 60 percent.²² The discrepancy in accuracy for different colored skin is astounding, showing a standard deviation rate of over 30 percent in certain statistics. According to Alex Najibi, a PhD student at Harvard University and the author of the article, "Racial Discrimination in Facial Recognition Technology," facial recognition is the least effective of all biometric technologies. Other biometric technologies include: fingerprint, iris, palm, and voice; however, the reason that facial recognition is used the most frequently is because it's the most accessible and has the largest database.²³ Per the current social movements regarding race, people have been, and are only going to continue to, push for facial recognition technologies to be banned in other large cities in the United States. Another set of data to look at is the current databases that contribute to the facial recognition process. According to Najibi, African Americans are significantly more likely to be profiled and arrested by law enforcement, which strongly affects the databases. "Consequently, Black people are overrepresented in mugshot data, which face recognition uses to make predictions. The Black presence in such systems creates a feed-forward loop whereby racist policing strategies lead to disproportionate arrests of Black people, who are then subject to future surveillance."²⁴ Though the current social movements affect the way in which society views the downfalls of facial recognition, this is just one of few issues the public has expressed.

On February 21, 2021, Facebook settled a \$650 million privacy lawsuit over its failure to disclose to its users that the platform "created and stored scans of their faces without

²² Anna says: et al., "Racial Discrimination in Face Recognition Technology," Science in the News, October 26, 2020, <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/>.

²³ Anna says: et al., "Racial Discrimination in Face Recognition Technology," Science in the News, October 26, 2020.

²⁴ Anna says: et al., "Racial Discrimination in Face Recognition Technology," Science in the News, October 26, 2020.

permission.”²⁵ The lawsuit was filed in Illinois in 2015, and once the case was settled in February of 2021, it is logged as one of the biggest privacy lawsuits in history.²⁶ On the social media platform, there is a feature that allows users to ‘tag’ their friends’ faces in order to personalize the photo more. When a user goes to ‘tag’ someone in a photo, Facebook already has the notable faces in the picture outlined in a white box. According to NBC News Channel 5 in Chicago, “Facebook broke Illinois’ strict biometric privacy law that allows people to sue companies that fail to get consent before harvesting consumers’ data, including through facial and fingerprint scanning.”²⁷ That being said, only residents of Illinois are able to ask for a portion of the settlement, ranging between \$250 and \$400. Moreover, although facial recognition has received severe criticism and backlash from millions of citizens around the country, there are just as many, if not more, benefits to the biometric technology that is so feared.

Facial recognition is used today in more ways than ever before, and will continue to parallel all other technological advances. For instance, “the Direct Marketing Association has said that businesses are finding that facial recognition technology can be used as a way to communicate with consumers and provide new tools, products, and services.”²⁸ According to a United States Government Accountability Office journal on Facial Recognition Technology, there are four major functions for facial recognition technology in businesses: photograph identification and organization; safety and security; secure access; and marketing and customer

²⁵ “Facebook Biometric Information Privacy Litigation,” Facebook Biometric Information Privacy Litigation, accessed April 20, 2021, <http://www.facebookbipaclassaction.com/>.

²⁶ Edward Moyer, “Facebook Privacy Lawsuit Over Facial Recognition Leads to \$650M Settlement,” CNET (CNET, February 27, 2021), <https://www.cnet.com/news/facebook-privacy-lawsuit-over-facial-recognition-leads-to-650m-settlement/>.

²⁷ NBC Chicago, “Illinois Facebook Users Can Now File Claims for Payouts in \$650 Million Lawsuit Settlement,” NBC Chicago (NBC Chicago, September 23, 2020), <https://www.nbcchicago.com/news/local/illinois-facebook-users-can-now-file-claims-for-payouts-in-650-million-lawsuit-settlement/2342967/>.

²⁸ Jason Bromberg et al., “Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law,” *United States Government Accountability Office* GAO-15-621 (July 2015): pp. 7-7.

service.²⁹ More specifically, in regards to photograph identification, as mentioned before, social media platforms—among other things—can use facial recognition to identify faces in a picture in a more positive connotation. Pertaining to safety and security, small and large businesses can use facial recognition to combat shoplifting and other crimes. Additionally, businesses like casinos can use the biometric technology to keep an eye on players who may be cheating or stealing money. When it comes to secure access, facial recognition can be useful in a multitude of ways. For example, as previously mentioned with Apple’s iPhone X, facial recognition can be used to unlock something personal, whether that be an apartment building, game console, or computer. Along the lines of marketing and customer service, retailers and other companies are “using facial recognition technology to target marketing and advertising more effectively and to improve customer service.”³⁰ In relation, after Apple released the iPhone X in 2017, more and more applications are utilizing the facial recognition technology to allow customers and users to log into accounts. For example, the Wells Fargo banking application has an option to use facial recognition to log into one’s personal banking accounts. Similarly, the stock brokerage, Fidelity, also allows their customers to opt into the same feature. Not only does the facial recognition feature add a sense of security and safety to users’ experience, but it saves people time and stress of remembering a password. The alternative to using facial recognition in applications like Wells Fargo and Fidelity without memorizing a password is to ‘save’ the password in your phone or with Google; however, this option also comes with many complications. According to Security.org, compromised passwords made up 80% of all data breaches in 2019, leading to tremendous financial loss for both businesses and consumers.³¹ Aside from marketing and digital

²⁹ Jason Bromberg et al., “Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law.”

³⁰ Jason Bromberg et al., “Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law,” *United States Government Accountability Office GAO-15-621* (July 2015): pp. 8-9.

³¹ “How Secure Is My Password?: Password Strength Checker,” Security.org, January 5, 2021, <https://www.security.org/how-secure-is-my-password/>.

uses, facial recognition is used to make peoples' lives easier everyday, whether they are aware of it or not.

Facial recognition technology is used in public spaces everyday beyond law enforcement, and most people do not even realize it. For example, many educational institutions use it to keep track of students and monitor possible intruders.³² Additionally, some public transportation companies use facial recognition for multiple reasons. Particularly, the New York City Subway uses facial recognition to “deter fare evasion.”³³ A newer use of facial recognition is now being seen in apartment buildings and complexes as a way of entry, therefore making access to buildings handsfree and keyless.³⁴ By eliminating keys to the main entry ways of buildings, it adds a sense of security as well as efficiency. Lastly, as mentioned previously, the United States Customs and Border Protection use facial recognition to identify possible international threats and to aid in deportations.³⁵ Depending on political views, some people may find that using this biometric technology as a means for detecting illegal immigrants for deportation is inhumane, but looking at it from an objective standpoint, it is for the public's safety and best interest. While just a few of the many benefits of facial recognition have been exhibited, through more research and fact finding, it becomes more clear that the use of the biometric technology has more positive outcomes than negative.

The underlying issue most commonly expressed regarding facial recognition is: privacy. Does the unknown, and even known, use of this incredibly intricate technology breach someone's privacy in everyday life? Although many may believe that the utilization of facial recognition is a threat to one's privacy, people must weigh the positives and negatives. Knowing

³² Richardson, Rashida. Report. German Marshall Fund of the United States, 2021. Accessed April 20, 2021. <http://www.jstor.org.access.library.miami.edu/stable/resrep28529>.

³³ Richardson, Rashida. Report. German Marshall Fund of the United States, 2021.

³⁴ Richardson, Rashida. Report. German Marshall Fund of the United States, 2021.

³⁵ Richardson, Rashida. Report. German Marshall Fund of the United States, 2021.

that millions of faces and the ornate details of those faces are stored in databases with a plethora of other information may sound discomfoting; however, society must also recognize that this so-called “breach” of privacy is directly correlated with public and personal safety as well.

Without thinking about it, millions of individuals upload hundreds of personal pictures onto the internet, choosing to display these images to the public. By posting pictures for the entire public to see on the internet, one must consider how that is any different than an individual’s face being held in a database for public safety reasons.³⁶ Social media platforms such as Facebook and Instagram are, in other words, massive public databases, providing personal information on strangers from all around the world. Simply by clicking on someone’s profile, if they choose to have a public account, one can see this specific person’s interests, friends, location, and more.³⁷ With social media today, barely anything is private anymore, so the use of facial recognition for safety purposes is comparable to a large social media network with hundreds of millions of faces, with the addition of a safety motive. According to the Security Industry Association (SIA), nearly 70 percent of Americans believe that facial recognition offers more benefits in regards to safety and security.³⁸ Therefore, the majority opinion on the facial recognition biometric technology is positive, with benefits outweighing the detriments.

In conclusion, as manifested by history and current events, facial recognition is, and will probably always be, a point of contention. Depending on one’s political, personal, and ideological views, opinions on this matter vary immensely. With the ever-changing advancements of technology, the algorithms and science behind this particular biometric

³⁶ Jason Bromberg et al., “Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law,” *United States Government Accountability Office* GAO-15-621 (July 2015): pp. 12-15.

³⁷ TG, “FACIAL RECOGNITION: Forget Anonymity,” *ASEE Prism* 21, no. 5 (2012): 13. Accessed April 21, 2021. <http://www.jstor.org.access.library.miami.edu/stable/24164005>.

³⁸ Geoff Kohl, “U.S. Public Opinion Research on the Support of Facial Recognition,” Security Industry Association, November 10, 2020, <https://www.securityindustry.org/report/u-s-public-opinion-research-on-the-support-of-facial-recognition/#:~:text=O%20all%20races%20and%20ethnicities>.

technology are bound to change overtime, as history has shown. As it is clear that facial recognition yields more advantageous than harmful outcomes, it is a technology that is most necessary for a safe and secure civilization. In order to please those who believe their privacy is being infringed upon, more laws and guidelines surrounding the issue should be put in place.³⁹ Once a larger majority of society sees the true advantages of facial recognition, it will be less challenging to reap the benefits. If more laws are passed providing people with the sense of security and privacy they desire, facial recognition can and will be used to its fullest extent for the good of humanity.

³⁹ Richardson, Rashida. Report. German Marshall Fund of the United States, 2021.