UNMASKING THE FACES OF FACIAL RECOGNITION TECHNOLOGY

An Honors Thesis Presented

By

SHREYA KHETTRY

Approved as to style and content by:

**** Angela Maione 05/24/23 08:16 ****
Chair

Unmasking the Faces of Facial Recognition Technology

Abstract

Facial recognition technology (FRT) has witnessed rapid advancement and widespread adoption in various societal sectors, ranging from law enforcement and government entities to corporations and social media. This paper aims to investigate and evaluate the multifaceted implications of FRT across different societal sectors. Through a comprehensive review of existing literature, this research examines the technical capabilities of FRT, including accuracy, efficiency, and potential biases. While FRT exhibits promising advancements, concerns related to algorithmic bias, false positives, and misidentification persist, highlighting the need for ongoing technical improvements and standards. The study further explores the social implications of FRT, emphasizing concerns surrounding privacy, surveillance, and the potential impact on marginalized communities. The widespread deployment of FRT raises significant ethical concerns, including consent, data security, and the potential for misuse or abuse of facial data. Furthermore, this paper critically examines the legislative landscape surrounding FRT. While some jurisdictions have implemented regulations, their effectiveness varies. The dynamic nature of FRT poses challenges in keeping pace with technological advancements, and current legislation often falls short in addressing the risks and safeguarding individual rights. The need for comprehensive and adaptable legislation becomes apparent. The analysis also includes a discussion on the challenges of regulating a rapidly evolving technology like FRT and highlights potential approaches to strike a balance between innovation and protection. Based on the analysis of technical, social, ethical, and legislative dimensions, this research concludes that the technology is still grappling with technical limitations, privacy concerns, potential biases, and

inadequate legal frameworks. Substantial work is required to address these challenges and strike a balance between innovation and protection. The findings of this study provide valuable insights for policymakers, organizations, and stakeholders, guiding their decisions regarding the responsible deployment, regulation, and ethical use of facial recognition technology across societal sectors. This paper underscores the importance of continued research and development to improve FRT accuracy, mitigate biases, and establish robust ethical guidelines. Furthermore, it emphasizes the urgency of comprehensive legislative frameworks that account for the societal implications and protect individual rights. Such efforts are crucial in harnessing the potential benefits of FRT while addressing the prevailing concerns.

Table of Contents

1. Introduction …….. Page 1
2. Literature Review ……. Page 4
3. Methodology …… Page 13
4. Portfolio
    - 4.1. Past ……..….. Page 15
    - 4.2. Present …….. Page 22
    - 4.3. Future …… Page 29
5. Conclusion …… Page 36
6. Reflection …….. Page 38
7. Bibliography …….. Page 39
8. Appendix ……..….. Page 42

Introduction

"In the far distance a helicopter skimmed down between the roofs, hovered for an instant like a bluebottle, and darted away again with a curving flight. It was the Police Patrol, snooping into people's windows. The patrols did not matter, however. Only the Thought Police mattered." [1] - George Orwell, 1984

With the advancement of technology, especially in the field of surveillance, George Orwell's dystopian vision of a totalitarian society portrayed in his novel "1984" seems to inch closer to reality. Orwell's vivid description of the omnipresent Police Patrol, constantly monitoring citizens through their windows, serves as a chilling reminder of the potential dangers associated with the abuse of surveillance technologies and its impact on individual privacy and freedom. One such technology that has gained significant attention in recent years is Facial Recognition Technology (FRT), a form of biometric identification that analyzes and matches facial features to individuals in real-time.

To better understand the significance of Facial Recognition Technology, it is crucial to recognize its position within the broader field of biometrics. Biometrics are a measure of physiological and biological characteristics of individuals that are used to uniquely identify them (Unar et al., 2014), such as fingerprints, iris patterns, voiceprints, and, in this case, facial features. Biometric technologies have witnessed rapid advancements and widespread adoption due to their ability to provide secure and reliable identification and authentication mechanisms.

[1] Orwell, G. (2021). *Nineteen eighty-four*. Penguin Classics. (Original work published 1949)

Facial Recognition Technology, a subset of biometrics, is a powerful tool that uses unique facial characteristics to identify and verify individuals within a digital system. FRT analyzes facial features such as the distance between the eyes, the shape of the nose, and the contours of the face, creating a unique facial template for each person (Hamman and Smith, 2019). FRT harnesses the power of facial biometrics to enable automated identification and verification processes and FRT algorithms generate unique facial templates that can be matched against pre-existing databases or used for real-time surveillance.

The inherent connection between FRT and biometrics raises questions about the balance between identification and surveillance, as well as the delicate interplay between security and privacy. Identification is the process of verifying an individual's identity, while surveillance is the systematic monitoring of an individual's activities. Security refers to the protection of individuals or assets from harm or loss, while privacy is the right to control one's personal information and limit its access by others. FRT blurs the line between identification and surveillance, as it possesses the ability to perform both functions simultaneously. On one hand, FRT promises efficient and accurate identification, enhancing security measures and facilitating convenience in various sectors. On the other hand, the widespread deployment of FRT systems raises concerns about mass surveillance, the erosion of personal privacy, and the potential for misuse and abuse of power. Striking the right balance between these two sides is crucial for designing ethical and effective applications of FRT.

Furthermore, FRT's deployment has brought forth concerns related to bias and accountability. The algorithms used in facial recognition systems heavily rely on datasets that are prone to biases, leading to potential inaccuracies and discriminatory outcomes, particularly towards marginalized communities. These biases raise questions about fairness, justice, and the

potential perpetuation of societal inequities through FRT implementation. Additionally, the accountability of FRT systems, their operators, and the organizations deploying them raises concerns about potential misuse, data breaches, and the need for regulatory oversight.

In light of these issues, this thesis seeks to explore the technical intricacies of Facial Recognition Technology, its social implications, the ethical considerations surrounding its use, and the legislative landscape in different societal sectors. By conducting a comprehensive analysis, this thesis aims to foster a deeper understanding of the challenges associated with FRT deployment and inform future policy discussions that acknowledge the potential benefits of FRT while safeguarding individual privacy, mitigating bias, and establishing adequate regulations to ensure accountability and responsible usage.

Literature Review

Facial Recognition Technology is evolving expeditiously and its growth is driven by a combination of technological advancements and a growing demand for identification and security solutions. Although the technology has various benefits it also raises a variety of important technical, societal, ethical, and legislative concerns that need to be addressed before there is irreversible damage. As with everything controversial in academia, scholars have been conflicted and opinionated about the rise and utilization of FRT in today's society and its various implications. The scholarship currently available on FRT is related to the overall concept of biometric identification and the overarching theme of surveillance and is concentrated on specific areas of concern such as surveillance, privacy, bias, and regulations. The scholarship is examined in accordance with various concerns regarding the technology such as Surveillance, Privacy, Bias, and Regulations. A point to be noted is that all the concerns are interdependent and there are chances of redundancy and overlap in the presentation of the scholarships.

Surveillance

Facial recognition technology has been extensively employed in surveillance systems across different sectors. Law enforcement agencies utilize it for public safety, suspect identification, and crime prevention whereas commercial establishments, airports, and transportation hubs employ facial recognition for access control and monitoring purposes (Almeida et al., 2022). The widespread adoption of facial recognition technology in surveillance raises significant concerns regarding privacy and civil liberties. As surveillance systems capture and analyze facial data, individuals' identities and activities can be monitored without their

explicit consent, leading to potential infringements on privacy rights and the mass collection and storage of biometric information raise concerns about data security and unauthorized access (Almeida et al., 2022). Another key concern is the potential for discriminatory targeting and surveillance of specific racial or ethnic groups. Additionally, questions arise regarding the legality and transparency of surveillance practices, as well as the accountability of the entities deploying these technologies (Almeida et al., 2022).

Public opinion and acceptance play a crucial role in the deployment of facial recognition technology for surveillance. Studies have indicated varying levels of public trust and concerns regarding its use (Kostka et al, 2023; Smith and Miller, 2022). Factors such as transparency, accuracy, and accountability of the technology, as well as clear communication about its purpose and safeguards, influence public perception. Scholars discovered that faith in the government, concerns about terrorism, and a "high level of technological affinity among citizens" have a positive relationship with the acceptance of the usage of FRT (Kostka et al, 2023). Contrastingly knowing about a country's history and usage of surveillance methods and doubts in regards to privacy resulted "in a more cautious attitude towards the use of FRT in public settings" (Kostka et al, 2023). The scholars also believe that other than regulating the usage of the technology and establishing various policies, raising awareness of the technology and its applications for the general knowledge of the citizens is equally important as they should be aware of the benefits and risks surrounding the use of the technology. Surveillance is an operation in which monitoring an environment transforms it. Beyond simply incorporating FRTs into our present society, it is needed to consider the kind of society that FRTs and constant supervision would generate, and how the balance of privacy and surveillance would emerge (Kostka et al, 2023; Smith and Miller, 2022).

Privacy

One of the primary ethical challenges of FRT is its potential for misuse and abuse as it allows for the mass collection of biometric data without individuals' consent or knowledge resulting in the depletion of autonomy and privacy (Miller 2023). Some scholars mention this to be “an inevitable result of modernization, technological change, globalization, and a shrinking world” (Milligan 1999; Leong 2019; Miller 2023). Scholars agree that privacy issues extend to both the public and private sectors. If the government’s technology misidentifies individuals, it can result in innocent people being placed on watch lists consequently disproportionately affecting minority groups and other vulnerable populations (Leong 2019; Miller 2023). Similarly, commercial or corporational institutions might employ facial recognition technology to unfairly or unlawfully discriminate against people. Another factor to be considered is individuals' readiness to have their lives monitored by cameras and surveillance systems, and their ability to give up personal control while potentially risking the misuse of their information by authorities in exchange for the perception of security and organization offered by video surveillance(Milligan 1999).

Scholars explore the differences between ethics to security and privacy (Almeida et al., 2022; Smith and Miller, 2022; Miller 2023). They argue that although it is considered morally justifiable to gather facial biometric data for specific and limited safety-related reasons, such as using it for border control passports or driver's licenses, it is not ethical to gather such data to create extensive surveillance systems and use it to discriminate against individuals based on their ethnicity (Smith and Miller 2022). They also discuss the “power imbalances" that arise between the different societal levels such as government and law enforcement, the private sector and the general public due to the creation of extensive and interconnected databases and systems for

biometric facial recognition and utilizing this information to identify and monitor citizens. Using the data from surveillance systems to monitor citizens can jeopardize fundamental principles that are integral to the liberal democratic state (Smith and Miller 2022). Scholars deduce that it is essential that individuals are adequately educated about biometric facial recognition systems and have given their consent for its usage and that deployment of such systems should be discussed publicly and supported by legislation, with their functioning subjected to judicial scrutiny (Almeida 2022; Smith and Miller, 2022; Miller 2023).

Bias

FRT uses algorithms to analyze and identify various facial features, patterns, and expressions. Several factors contribute to bias in facial recognition technology. One key factor is the lack of diversity and representativeness in the training datasets used to develop these algorithms. Research has indicated that the datasets used are often skewed towards lighter skin tones and predominantly male faces (Buolamwini 2017, Selbst et al., 2019). Several scholars have highlighted the presence of bias in these algorithms, resulting in discriminatory outcomes across different demographic groups; for example, facial recognition systems exhibit higher error rates when identifying individuals with darker skin tones, women, and elderly individuals (Buolamwini 2017; Grother et al., 2019; Wang and Kosinski 2018). Consequently, the algorithms may not accurately generalize across different demographic groups, resulting in biased outcomes. Furthermore, other sources of bias can stem from variations in lighting conditions, camera angles, and image quality, which can disproportionately affect the accuracy of certain groups (Wang and Kosinski 2018).

The presence of bias in facial recognition technology has significant implications for society, justice, and civil liberties. In law enforcement and surveillance applications, biased algorithms can lead to wrongful arrests, false identifications, and potential violations of individuals' rights (Garvie et. al, 2019). Moreover, bias can perpetuate existing societal inequalities and reinforce discrimination against marginalized groups (Buolamwini 2017, Selbst et al., 2019). The consequences of biased facial recognition technology highlight the urgent need to address these issues and develop fair and accountable systems.

From an ethical standpoint, biases in facial recognition systems violate principles of fairness, justice, and equal treatment (Buolamwini 2017; Selbst et al., 2019; Miller 2023). Discriminatory outcomes undermine trust in these technologies and exacerbate social divisions. Legally, the use of biased facial recognition systems can potentially infringe upon civil liberties, such as privacy and freedom from unjust surveillance. Existing legal frameworks often lag behind technological advancements, calling for comprehensive regulations and policies that explicitly address bias in facial recognition technology (Selbst et al., 2019).

Scholars emphasize the importance of recognizing the challenges and future directions concerning bias in facial recognition technology, despite advancements in understanding and mitigating it. Primarily, the inclusion of comprehensive and diverse datasets that accurately represent the entire range of human diversity is crucial for effectively training facial recognition algorithms (Buolamwini 2017, Selbst et al., 2019). Achieving this goal necessitates collaborative endeavors among researchers, industry professionals, and policymakers to gather and curate datasets that encompass inclusivity. Moreover, there is a need for continued research to establish standardized evaluation metrics and benchmarks that can be used to assess bias and ensure fairness in facial recognition systems (Buolamwini 2017, Selbst et al., 2019).

Regulations

Scholars believe that the current legislation is not prepared to deal with the issues that arise from the inception and implementation of FRT (Milligan 1999; Chilson and Barkley 2021) There are several “constitutional issues” related to facial recognition technology and video surveillance; one of them is if they constitute a search under the Fourth Amendment, and another one is whether they could negatively affect the First Amendment’s freedoms of speech and association.

The Two Faces of Facial Recognition Technology by N.A. Chilson and T.D. Barkley is a scholarship that discusses various approaches on how FRT can be governed and regulated to minimize its dilemmas. Chilson and Barkley examine the potential benefits of FRT such as higher level of individual security, smartphone security which in turn helps in the protection of private information, as well as various uses by major applications, services and products like Google’s Nest cameras, Facebook, Amazon Photos, Microsoft’s Seeing AI etc. They also discuss various privacy and algorithmic bias concerns related to the technology. Analyzing and Critiquing the benefits and concerns related to FRT, the authors quite smartly create a base to build on and discuss their regulation and governance approaches in terms of what has been done, what is currently being done, and what should be done. The authors establish two primary approaches for the regulation of FRT: “Hard Law Approach" and “Soft Law Approach” (Chilson and Barkley 2021) .

The authors describe the hard law approach as “legislation or common law decisions established and enforced by the government” (Chilson and Barkley 2021). Their definition of the soft law approach is based on the description by Arizona State University Law Professor Gary Marchant and his colleagues and is described as “frameworks that set forth substantive

expectations but are not directly enforceable by government and include approaches such as professional guidelines, private standards, codes of conduct, and best practices" (Chilson and Barkley 2021) . In short, it can be said that the hard law approach is about being bound by the written law and its enforcement whereas the soft law approach is more about voluntarily abiding by a set of community standards and code of conduct for the betterment of the environment and society.

The authors discuss the regulation of FRT through hard-law approaches such as the Biometric Information Privacy Act (BIPA) passed in Illinois, Washington, and Texas, and the potential unintended consequences of such laws. They mention that the BIPAs have led to some companies withdrawing products or services from these states and triggering numerous class action lawsuits that target technical violations of the law, but there is little evidence that the law is materially protecting the privacy of Illinois residents. The authors mention that even though BIPA has led to a lot of expensive litigation without clear evidence of benefiting consumers does not necessarily mean that all hard law approaches for the regulation of FRT will have the same consequences but the former does serve as a warning and suggests the need to explore other approaches, such as soft law (Chilson and Barkley 2021) .

The scholars argue that the soft law approach will over time provide a better solution for FRT. They state that the technology is evolving rapidly and it will not be the same 10 years from now and that they anticipate the hard law approach will eventually fail to try to keep up with the evolution; in this scenario, the soft law approach will flourish as it evolves alongside the technology (Chilson and Barkley 2021). They argue that the hard law "often focuses on preventing worse-case scenarios" whereas soft law is better able to foresee harm without hampering potential benefits and can react and adapt faster as well (Chilson and Barkley 2021).

They further go on to discuss various soft law approaches such as: “social norms, self-censorship, education, labeling, education, voluntary standards, private certifications, and public pressure” that address privacy and algorithmic bias.

The scholars further discuss various examples of Hard Law approaches present currently and that are in the developmental or processing stage such as the Facial Recognition Technology Warrant Act. They also argue that it is imperative to establish regulations and “hard law restrictions” for government entities that utilize FRT so that they are unable to evade the legislation and/or misuse the technology consequently making it possible for the soft law approach to be used commercially. The scholars conclude by stating that FRT should be evolved under a “soft law framework” and civil liberties should be protected by using the hard law approach to limit the government’s FRT utilization (Chilson and Barkley 2021) . This scholarship provides us with various aspects that lawmakers and stakeholders should consider during the creation of legislation for the use of Facial Recognition Technology in society and the “soft-law approach” they mention adds another dimension to be considered by private and public sector corporations.

In conclusion, this literature review has provided a comprehensive exploration of the multifaceted aspects of facial recognition technology. The review examined the implications of FRT in the context of surveillance, highlighting concerns regarding its potential for invasive monitoring and discrimination. Privacy considerations shed light on the challenges of protecting individuals' personal information and ensuring ethical use. The discussion on bias revealed the presence of inherent biases within facial recognition algorithms, raising important questions about fairness and equity. Lastly, the examination of regulations demonstrated the ongoing

efforts to develop frameworks that balance innovation, public safety, and individual rights. By considering the complex interplay of surveillance, privacy, bias, and regulations, stakeholders and policymakers can work towards responsible and equitable deployment of facial recognition technology in our increasingly digital and interconnected world.

Methodology

In this thesis the technical, social, ethical and legislative implications of the utilization of FRT at different societal levels is explored. The research question is "What are the technical, ethical, social, and legislative implications of Facial Recognition Technology?".

A mixed-method approach is used to thoroughly review the literature on facial recognition technology to gather insights on the current state of the technology, its applications, and social-ethical implications along with its various regulations. The analysis is done in accordance with the Digital Technology in Time Portfolio Exploration in which a 'multigenerational view' of the technology is explored by reflections on the past, present and future of this technology in society. The answer to the research question would be that the deployment of Facial Recognition Technology presents multifaceted implications across the realms of technology, ethics, society, and legislation, demanding a balanced approach to address potential risks and safeguard individual rights.

The research data was collected from a variety of secondary sources such as academic journals, books, articles, opinion pieces etc. and the search was carried out using Google Scholar, ACM Digital Library, and the UMass Library's website. A few of the key words for the searches were "facial recognition technology", "regulation of facial recognition", "accuracy of facial recognition", "ethical facial recognition" etc. Following this a thorough systematic literature review on the topic was conducted.

The Portfolio section of the project consists of three sections: the past, the present, and the future. Each section has been approached with a different lens and have been thematically linked so that they can overall help in exploring, analyzing, and answering the research question.

The ‘Past Section’ of the portfolio aimed to explore the historical origin of the use of biometric identification. By understanding the history of biometrics, valuable insights into the evolution of identification systems and their impact on society in today’s world were explored. In this section, discussions were held regarding how ancient civilizations used various forms of biometrics as identification and how this identification system developed into the technology it is today. A detailed insight was provided into the creation of the concept of this technology, its development and evolution, and finally, its implementation into reality and our society as it existed at that time.

The 'Present Section' of the portfolio delved into the topics of bias, discrimination, misidentification, privacy, and surveillance associated with Facial Recognition Technology (FRT), drawing insights from the documentary "Coded Bias" and intertwining it with real-life cases to support the arguments and analysis conducted. Furthermore, it examined the societal implications of FRT by analyzing its impact on marginalized communities and the potential infringements on civil liberties.

The 'Future Section' of the portfolio examined the then-current legislation regarding the ethical implications associated with Facial Recognition Technology (FRT) in various sectors, including government, law enforcement agencies, and corporations. It further delved into discussions about the potential implementation of solutions to ensure responsible use of this technology in the future, envisioning the possible advancements and adaptations that could shape its development and impact.

Portfolio: Past Section

Biometrics has a long fascinating history that dates back thousands of years. From ancient Babylonian clay tablets (Scherer 2005; Maguire 2009; Mulholland 2020) to modern facial recognition technology, biometrics has played a critical role in various fields, including law enforcement, border control, and even mobile phone security (Scherer 2005; Mulholland 2020). The application of biometrics has undergone a transformative journey, adapting to technological progress, legal frameworks, and societal attitudes. Examining the historical development of biometrics unveils the evolution of identification systems and sheds light on its prevalent use as a surveillance tool, often intertwined with the context of imperialism and power dynamics. The attached infographic at the end of this section provides a visual representation of the chronological timeline for the History of Biometric Authentication. It is utilized to arrange and structure the points in this section chronologically. While not strictly followed, additional information points are incorporated. The infographic serves as a valuable reference to ensure the inclusion of all essential information and prevent any omissions.

The origins of biometrics can be found in ancient civilizations, where individuals were identified based on their unique physical or behavioral characteristics. For instance, as early as 500 BC (Scherer 2005; Mulholland 2020) Babylonians utilized fingerprints in their business transactions, while Assyrians employed fingerprints on payment receipts (Maguire 2009). In 14th-century China, children's palms and footprints, as well as inky footprints on divorce records, served as distinguishing markers. Similarly, physical attributes were used to differentiate traders in ancient Egypt. These practices demonstrate the early recognition of the distinctiveness of certain traits for identification purposes (Maguire 2009; Mulholland 2020). In the 19th

century, advancements in biometric systems of identification emerged through the collaborative efforts of administrators, anthropologists, and detectives in colonial India, London, and Paris (Maguire 2009). The historical development of biometrics surpasses mere cycles of innovation, experimentation, and varying degrees of legal and public acceptance. Fingerprinting and facial recognition, which lie at the heart of the current biometric revolution, offered pioneers of the 19th century more than just the means to identify criminals. Early biometric methods carried the potential for an idealistic vision of bio-governmentality, where the verification of individual identities played a central role in population control (Maguire 2009).

In 1880 Henry Faulds, a Scottish medical missionary based in Tokyo, published a brief letter in the journal, Nature, in which he discussed his observations on fingerprints, including those of primates and impressions found on ancient pottery and suggested that these "nature-copies" could be visually compared, potentially leading to the scientific identification of criminals (Maguire 2009). Following Faulds's letter in Nature, William Herschel, a colonial administrator, published an additional article, drawing attention to his extensive work with fingerprints spanning over two decades (Maguire 2009). Herschel's involvement in fingerprinting stemmed from a broader objective of verifying the identities of colonial subjects. He credited the genesis of modern fingerprinting to a significant incident where he demanded a local individual in India's Hooghly River region to sign a contract while including their palm print, intending to instill fear. The practice of using palm prints and fingertips, known as '*tip sahi*,' in written agreements was not uncommon in the local context (Maguire 2009). However, Herschel was fascinated by the replicability and genuineness of these natural imprints. Colonial literature often discussed the challenge of uncertain individual identities from the colonial perspective, leading Herschel to perceive biometrics as a practical solution to this predicament (Maguire 2009).

Despite William Herschel's aspirations, fingerprinting continued to be an informal security measure without substantial scientific validation by the time of his retirement. He then passed along his findings to Charles Darwin's cousin, Francis Galton, a multifaceted Victorian scholar, anthropologist, and advocate of eugenics (Maguire 2009).

In the late 19th century, Galton conducted groundbreaking research on fingerprints, recognizing their unique and unchanging nature. He published his findings in his influential book, "Fingerprints," in 1892, which sparked a wave of interest and research in the field. Galton's work provided the scientific basis for fingerprint identification as a means of establishing personal identity (Maguire 2009). His research demonstrated that fingerprints exhibit distinct patterns, such as loops, whorls, and arches, which remain consistent throughout a person's life. This breakthrough opened up new possibilities for law enforcement agencies and forensic science. Despite Galton's original intention of using biometric identification for racial discrimination to advance his eugenics research, his work inadvertently led to the development of a system where fingerprints became utilized as distinct individual identifiers (Maguire 2009).

During the 1880s, Francis Galton, while conducting experiments on fingerprinting In Paris, Alphonse Bertillon, a French criminologist, was rapidly gaining recognition as a detective who placed a greater emphasis on the individual rather than the concept of "race" (Maguire 2009). Bertillon recognized the need for a standardized method of criminal identification, which led him to create a system known as anthropometry. This system relied on a series of precise physical measurements, including facial dimensions, to create individual profiles for identification purposes (Maguire 2009). Bertillon's anthropometric system gained widespread recognition and adoption, particularly in Europe and the United States (Maguire 2009; Mulholland 2020). It marked a significant shift from subjective and less reliable methods of

identification to a more scientific and standardized approach. The measurements collected by Bertillon, including facial measurements such as the distance between certain points on the face, were recorded on identification cards known as Bertillon cards. These cards formed the basis for the identification and classification of criminals in many countries (Maguire 2009). The limitations of anthropometry became apparent over time. The system relied on precise measurements that were difficult to obtain consistently and accurately. Moreover, the system did not account for changes in an individual's appearance, such as aging or alterations to facial features. These limitations led to the exploration of alternative biometric methods that could offer more reliable and practical identification techniques.

Another significant milestone in biometric history was the discovery of iris patterns as a unique identifier. In the 1930s, ophthalmologist Frank Burch proposed the idea that the intricate patterns in the iris could serve as a reliable method of identification. It wasn't until the 1980s, with the advent of computer-based image processing, that iris recognition technology began to be developed and refined (Mulholland 2020).

Woody Bledsoe, Helen Chan Wolf, and Charles Bisson were among the first pioneers of facial recognition technology (NEC New Zealand, “A brief history…”). They began their work in 1964 and 1965, using computers to recognize human faces. Their work was funded by an unnamed intelligence agency, and much of it was never published. Their early work involved manually creating various points on the face as unique identifiers, however, the computers used would rotate these points resulting in various errors (NEC New Zealand, “A brief history…”). Despite being severely limited by the technology of their time, their work is considered an important first step of facial recognition as a biometric technology (NEC New Zealand, “A brief history…”). In the 1970s, 1980s, and 1990s, there were various novel methods developed, such

as the "Eigenface approach" and "Fisherfaces," which enhanced the facial recognition technology's capacity to detect faces and recognize features (Klosowski 2020). These developments were crucial in laying the groundwork for contemporary automated systems.

The first time facial recognition became a widespread terminology was during the Super Bowl XXXV in 2001 held in Tampa, Florida, where security cameras were utilized to capture images of all 100,000 attendees, which were then electronically cross-checked with Tampa police mug shots using face recognition technology (Mulholland 2020; Klosowski 2020). Law enforcement wanted to identify criminals and potential terrorists. This sparked a major debate nationally as many individuals criticized this as they believed that it violated Fourth Amendment rights that protect against unjustified search and seizure. Moving forward to 2008, Illinois passed the Biometric Information Privacy Act (BIPA), which was the first law in the US to address the “unauthorized collection and storage of biometric data”, including facial images (Klosowski 2020).

Facial recognition entered a new era in the 2010s where there is a divergence of the technology being used as more than a surveillance tool. Big Tech companies such as Meta, Google, Amazon, Microsoft etc. implemented this technology in one or more of their products. From Meta introducing DeepFace into Facebook as a photo-tagging software in 2014 to FRTs trickling into our personal devices with the introduction of Apple’s iPhone X and its FaceID feature, this technology has now become part of our day-to-day lives and is now a common security feature. Border controls, airport security and authorities, stadiums, concerts etc. are now all using biometric technology, especially facial recognition technology, as a means of identification and maintenance of security standards. FRT has seamlessly integrated into various aspects of our everyday lives.

The historical evolution of biometrics, intertwined with colonialism, sheds light on the development and use of FRT as a surveillance tool. What began as crude and rudimentary identification methods have now transformed into sophisticated systems capable of capturing and analyzing vast amounts of personal data. From the anthropometric measurements of colonial times to the sophisticated facial recognition systems of today, the underlying motivations of control and power remain unchanged. While FRT offers some benefits, it is essential to critically examine its implications and potential consequences.

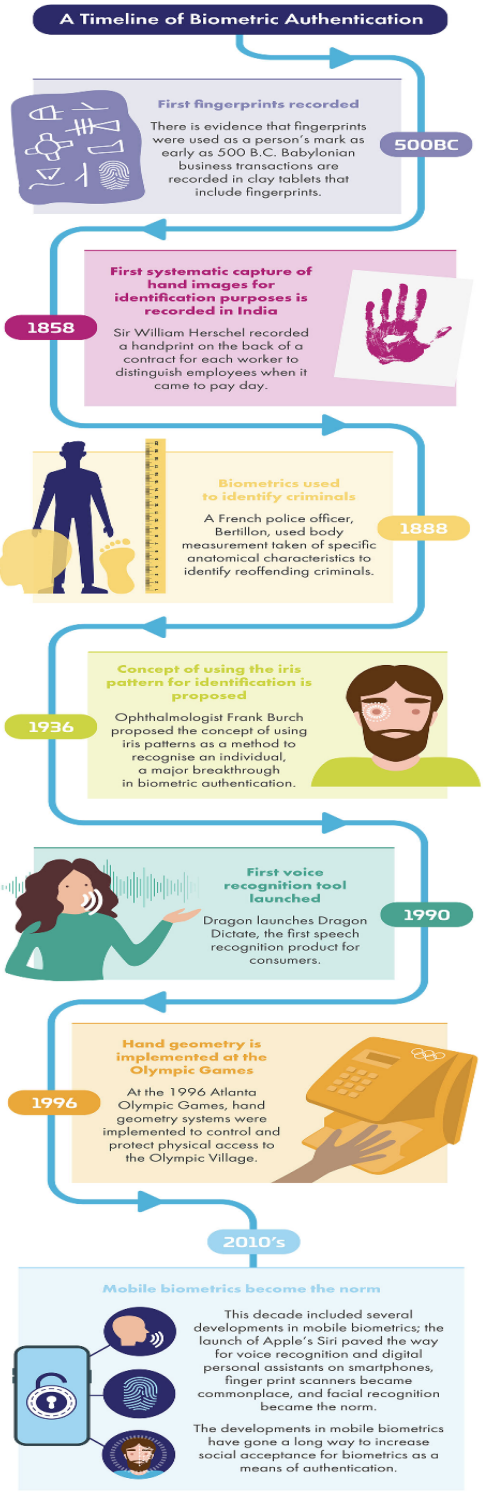

Figure 1: Excerpt of the Infographic Used [2]

[2] Thales Group. (n.d.). History of Biometric Authentication. Retrieved from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-biometric-authentication

Portfolio: Present Section

Throughout this essay, I have highlighted the significant concerns surrounding Facial Recognition Technology that must be effectively addressed before its widespread adoption by government agencies, law enforcement bodies, and public and private corporations. This section will delve into the topics of bias, discrimination, misidentification, privacy, and surveillance related to Facial Recognition Technology (FRT), drawing insights from the documentary "Coded Bias". Concrete examples from real-life cases will be utilized to illustrate and support the arguments being made.

Bias, Discrimination, and Misidentification

The documentary "Coded Bias", directed by Shalini Kantayya, highlights the deeply rooted biases present in surveillance technology and algorithms. Coded Bias revolves around the central narrative of Joy Buolamwini, whose research serves as the foundation of the documentary's exploration. During her pursuit of a doctoral degree at the MIT Media Lab, Joy Buolamwini encountered a striking revelation regarding facial recognition software. As a person of color, specifically Black, she experienced the technology's failure to detect her facial features accurately. In a remarkable turn, the software only responded when she covered her face with a white mask. This disconcerting experience shed light on a critical issue: facial recognition technology's struggle to recognize and identify individuals with darker skin tones.

Buolamwini's investigation delved deep into this matter, revealing a fundamental flaw in the datasets employed to train facial recognition algorithms. These datasets predominantly comprise images of white individuals, predominantly men, which reflects an inherent bias

stemming from the unconscious tendencies within the industry. This bias is a result of the field being predominantly dominated by white male programmers, who inadvertently create datasets that align with their physical characteristics. Consequently, this lack of diverse representation perpetuates a significant limitation within facial recognition technology. Individuals with darker skin tones, including Buolamwini herself, are underrepresented and overlooked in these datasets. The technology fails to acknowledge their existence, rendering them virtually invisible in the digital realm. Such biases can perpetuate systemic discrimination and reinforce existing societal inequalities, posing a threat to fairness and justice and creating a larger base for misidentification.

Various real-life cases have highlighted the grave consequences of FRT misidentifications. One such case was reported and highlighted by the American Civil Liberties Union (ACLU) in 2018 when they reported a study on Amazon's FRT software Rekognition (Snow 2018). They stated that the technology was being used by law enforcement and that when they ran the software it incorrectly identified 28 members of the Congress by matching them to individuals who had been arrested for crimes. The test stated that out of the incorrect matches, there were almost 40% of People of Color (PoC) present (Snow 2018). This also highlighted the utilization of FRT as a potential privacy and security risk if misused by law enforcement as historically, PoC has been discriminated against by law enforcement and incorrect identification based on a technology system that should provide accurate results, could cost an individual their freedom. The ACLU's article further reports that Amazon is allowing multiple law enforcement agencies to utilize its software and that Amazon's employees protested against its sale to law enforcement, especially to United States Immigration and Customs Enforcement (ICE) as this was under Trump's administration and the employees believed that the technology could be

misused for children immigrant surveillance (Cagle and Ozer 2018). There was another study undertaken by MIT researchers, Deborah Raji and Joy Buolamwini, that resulted in outlining the software's incorrect matching percentage which leans towards it being gender and racial biased (Al-Heeti 2019). In response to most of the allegations, Amazon has always maintained the same stance of not backing down and continuously defending itself and its technology. However, during the Black Lives Matter protests, under pressure and to maintain their reputation, as well as to show their support and solidarity Amazon announced that they are deciding to place a moratorium on law enforcement's utilization of Rekognition "until further notice".

Another case and one of the early instances of wrongful arrest resulting from FRT misidentification is the case of Robert Williams. Williams, a resident of Detroit, experienced the harrowing consequences of being wrongfully arrested based on a facial recognition match in 2020. The system erroneously identified him as the suspect in a shoplifting incident, leading to his unjust apprehension by the Detroit Police Department (Manjoo 2020). This case underscores the deeply rooted biases present in FRT algorithms and their potential to disproportionately impact marginalized communities. The misidentification of Williams highlights the systemic discrimination faced by individuals of color within law enforcement practices. By relying on flawed technology, law enforcement agencies risk perpetuating existing racial biases and reinforcing societal inequalities. This case underscores the deeply rooted biases present in FRT algorithms and their potential to disproportionately impact marginalized communities. The misidentification of Williams highlights the systemic discrimination faced by individuals of color within law enforcement practices. By relying on flawed technology, law enforcement agencies risk perpetuating existing racial biases and reinforcing societal inequalities. Additionally, the case raises concerns about the lack of transparency and accountability in the use of FRT by law

enforcement agencies. The incident with Williams sheds light on the potential for misuse and abuse of this technology, particularly when it comes to targeting and profiling individuals based on biased algorithms.

Both the cases mentioned above, Amazon's software misidentifying members of Congress and the wrongful arrest of Robert Williams due to misidentification highlights the crucial intersection of bias and accountability within the development and deployment of facial recognition technologies. This case serves as a stark reminder of the biases embedded in facial recognition technology and its potential implications for marginalized communities. The misidentification of public figures in positions of power underscores the broader issue of racial bias within these systems. By disproportionately misidentifying individuals of color, the technology perpetuates harmful stereotypes and contributes to the disproportionate targeting and scrutiny faced by these communities. This case also underscores the urgent need for robust accountability measures in the development and deployment of facial recognition technology. It highlights the importance of comprehensive testing, independent audits, and ongoing evaluation to identify and mitigate biases. Companies and developers must take responsibility for the ethical implications of their technologies and actively work towards addressing biases to ensure fairness and justice.

Surveillance and Privacy Invasion

Facial recognition technology poses a significant threat to personal privacy. The ability of these systems to track and monitor individuals without their consent or knowledge raises serious concerns about surveillance and the erosion of personal freedoms. Coded Bias highlights the

potential for facial recognition technology to intrude upon the private lives of individuals in various contexts. A real-life case mentioned in the documentary is related to Clearview AI.

In 2020, NYT reported an article (Hill 2020) in which it was publicized that law enforcement agencies were using a facial recognition algorithm to search for images on the internet to identify suspects. This algorithm was developed by Clearview AI, a company that created a database of over 3 billion images by scraping them from various social media applications such as Facebook, Instagram, and Twitter, without the knowledge or consent of the individuals involved. This vast database of images allows Clearview AI's facial recognition algorithm to identify and track individuals in real-time, even if they have no prior association with the company or its services. Clearview AI also offers its facial recognition software to private companies such as Walmart, AT&T, Bank of America, Best Buy, and the NBA, to aid them in their security measures (Smith and Miller 2022). This raised a huge controversy with multiple lawsuits and a class action being filed against the company for breaching privacy rights, violating terms of use of several websites, violating California Consumer Privacy Act (CCPA) and Biometric Information Privacy Act (BIPA), and selling access to biometric information to third-party entities without consent (Smith and Miller 2022). Clearview AI, in 2020, also had its database breached by hackers (BBC News 2020), which goes on to show that there is always a possibility of our data falling into incorrect hands. Such indiscriminate data collection and surveillance raise significant questions about consent, data ownership, and the boundaries of personal privacy.

Furthermore, the pervasive use of facial recognition technology by both private and public entities amplifies the invasion of privacy. From retail stores and airports to public spaces and government agencies, the deployment of facial recognition systems has become increasingly

common. These systems can capture and analyze facial data without individuals' awareness, making it possible to track people's movements, and interactions in public areas. This constant surveillance can create a chilling effect, discouraging individuals from freely expressing themselves or engaging in activities they perceive as private.

Another concerning aspect of the invasion of privacy and constant surveillance is the potential for unauthorized access and misuse of facial recognition data. If databases containing facial biometrics are compromised or fall into the wrong hands, individuals' privacy can be compromised on an unprecedented scale (Smith and Miller 2022). The accumulation of facial data can enable various forms of identity theft, fraud, and unauthorized surveillance. Additionally, the integration of facial recognition systems with other technologies, such as social media profiles or public records, can lead to the creation of comprehensive digital profiles without individuals' knowledge or control, infringing upon their autonomy and right to privacy.

In conclusion, the examination of bias, discrimination, misidentification, privacy, and surveillance concerning Facial Recognition Technology reveals a complex array of challenges that demand immediate attention. The highlighted concerns emphasize the importance of proactive measures before the widespread adoption of FRT by various entities. Insights from the documentary "Coded Bias" and real-life examples demonstrate the tangible consequences that result from unregulated deployment and misuse of this technology. To ensure responsible and ethical integration of FRT, it is crucial to establish comprehensive regulations, implement robust oversight, and prioritize transparency. Addressing inherent biases, safeguarding privacy rights, and mitigating misidentification risks is imperative. By actively addressing these concerns and

taking decisive action, we can strive to maximize the potential benefits of FRT while upholding the fundamental rights and values of individuals and society as a whole.

Figure 2: Coded Bias's Poster

Portfolio: Future Section

Facial Recognition Technology has become a naturalized part of our world and has seamlessly integrated into various aspects of our world, becoming a normalized and almost ubiquitous presence. From smartphones and social media platforms to airports, public spaces, and even law enforcement agencies, FRT has become a routine tool for identification, authentication, and surveillance. The widespread use of Facial Recognition Technology raises a multitude of concerns regarding privacy, civil liberties, and the ethical implications that accompany its extensive adoption. In this section, there is an examination of the current legislation with the ethical implications surrounding this technology in different sectors such as government, law enforcement agencies, and corporations. Discussions about how this technology could look in the future based on the implementation of the potential solutions to ensure its responsible use in the future.

The utilization of Facial Recognition Technology by government agencies, law enforcement agencies, and private and public agencies are all unregulated creating uncertainties and blurring the lines between its ethical usage. The absence of regulatory measures permits government and commercial entities to operate with minimal legal restrictions and self-regulation. Through FRT, these corporations can detect and track consumers' online behavior without their knowledge or consent.

When it comes to legislation, currently there are no federal regulations concerning FRT or biometrics data in the United States; however, there are a few states that have implemented their own set of regulations. On 3rd October 2008, Illinois became the first state to establish regulations for biometric data by passing the Biometric Information Privacy Act (BIPA). In

essence, BIPA mandates that corporations must inform individuals when they gather their biometric data and justify their intentions for using the information in addition to taking their permission (ACLU 2022). Furthermore, BIPA stipulates that any private organization possessing biometric data of its consumers should create and publicly release a retention schedule and set of guidelines for securely destroying that information (Rowe 2020). In addition, it also provides various standards for storing, transmitting, and protecting information (Rowe 2020).

Due to a lack of federal action, a few state and local governments have implemented their bans, especially concerning this technology being used by law enforcement. Following in Illinois's footsteps, Texas and Washington have "broad biometric privacy laws" and California, Colorado, Connecticut, Utah and Virginia have passed "comprehensive consumer privacy laws" which once implemented will govern biometric data. San Francisco, in 2019, was the first US city to ban the use of Facial Recognition Technology. In 2020 Oakland, California and Somerville, Massachusetts banned the use of facial recognition technology by government and law enforcement agencies (Rowe 2020). The US Senate proposed the Commercial Facial Recognition Privacy Act on March 14, 2019, which, if approved, would mandate that companies must seek explicit user consent before gathering any facial recognition data (Hawkins 2019). Additionally, the proposed law would necessitate informing users about the technology's use and its capabilities and limitations. Microsoft president Brad Smith also supported the inception of this Bill in the Senate.

Big-tech Corporations also appear to be the driving force behind the call for regulatory measures, indicating a shared concern among stakeholders regarding the need for biometric data regulation (Rowe 2020). However, opinions vary on the specifics of what such regulation should entail and the reasons for implementing it. CEOs of major American corporations are promoting

the implementation of federal privacy laws that would regulate the collection, usage, and distribution of personal data across industries, to preempt state-level laws. The Business Roundtable, an association of top executives from prominent American companies, has developed a Framework for Consumer Privacy Legislation, which outlines various provisions that wish would be covered in future legislation (Business Roundtable 2019; Rowe 2020).

It is worth noting that companies engaged in the creation of facial recognition software are urging Congress to regulate it, with Amazon being a prominent example. Amazon's policy team has developed a legislative proposal that it hopes Congress will adopt to ensure the continued use of its facial recognition technology, "Rekognition." Given Amazon's vested interest, some may question the motivations behind the proposal. Amazon has called for transparency and constructive discussions among all stakeholders to ensure the appropriate use and ongoing improvement of the technology (Rowe 2020). Amazon's proposed legislation outlines five main guidelines for the use of facial recognition technology (Stromberg 2019):

1. "Facial recognition should always be used in accordance with the law, including laws that protect civil rights."
2. "When facial recognition technology is used in law enforcement, human review is a necessary component to ensure that the use of a prediction to make a decision does not violate civil rights."
3. "When facial recognition technology is used by law enforcement for identification, or in a way that could threaten civil liberties, a 99% confidence score threshold is recommended."
4. "Law enforcement agencies should be transparent in how they use facial recognition technology."

5. "There should be notice when video surveillance and facial recognition technology are used together in public or commercial settings."

Amazon argues against a blanket ban on facial recognition technology due to its potential to enhance public safety and emergency response but emphasizes the importance of safe and effective implementation and regulation. Notably, Amazon does not support fully automated decision-making using facial recognition technology and suggests that facial recognition matches should be considered alongside other evidence, rather than used as the sole basis for action. The American Civil Liberties Union (ACLU) has voiced concerns about the use of Amazon's Rekognition tool by police across multiple jurisdictions, citing potential threats to civil liberties (ACLU 2021). This criticism may be pertinent to a few members of Congress, as the software has previously misidentified 28 of their colleagues as individuals who had been arrested for criminal activities, with a disproportionate number of false matches involving people of color in Congress (Snow 2018). Some major tech firms have expressed worries over the absence of regulations in the realm of facial recognition technology. Microsoft has urged governments worldwide to take the initiative and regulate this type of technology, whereas Facebook has opposed several state-level proposals aimed at regulating the usage of biometric data (Rowe 2020).

Figure 3: Facial Recognition by Steve Greenberg [3]

Facial recognition technology has the potential to revolutionize surveillance in the future. With the increasing proliferation of cameras and the exponential growth of digital data, it will become easier and more cost-effective to track people's movements and activities using this technology. However, this raises serious concerns about privacy and civil liberties. There are worries that this technology is being used to monitor individuals' political and religious affiliations, suppress dissent, and reinforce existing social inequalities. The comic above (Figure

[3] Cartoon Movement. (2019, May 23). Facial Recognition. Cartoon Movement. Retrieved from https://cartoonmovement.com/cartoon/facial-recognition-0

3) gives us a glimpse into what a future under constant surveillance would look like. Living under constant surveillance will most probably have a significant negative impact on individuals' well-being, privacy, and freedom. The widespread use of surveillance technologies in public spaces, workplaces, and private settings could create a society where individuals are constantly watched and monitored. This constant scrutiny can lead to feelings of anxiety, stress, and paranoia, and can have serious implications for mental health. Moreover, being under constant surveillance can infringe on individuals' right to privacy and freedom of expression, and can create a culture of self-censorship and conformity. Additionally, surveillance can be used to discriminate against individuals based on their race, gender, religion, or political views, which can reinforce existing social inequalities and exacerbate systemic injustices. Therefore, there must be comprehensive regulations created to prevent the misuse of facial recognition technology and to ensure that its use is in line with the principles of democracy, transparency, and accountability. Without proper safeguards, the use of facial recognition technology in surveillance could lead to a dystopian future where privacy is non-existent, and individuals are constantly under surveillance, like in the comic above.

Based on my readings and understanding of the proposed legislation around the technology as well as keeping in mind the problems and benefits of the technology I propose the following should be included in some form when proper legislation regarding FRT is being discussed and proposed. The following are a few regulations that I think should be considered:

1. **Transparency Requirements:** Companies must inform individuals that facial recognition technology is being used, why it is being used, and how long the data will be

stored. Additionally, individuals should have the right to access and delete their data (United States GAO 2016).

2. **Limitations on Law Enforcement Use:** Law enforcement agencies should be required to obtain a warrant before using facial recognition technology to identify individuals, and the use of the technology should be limited to specific crimes (United States GAO 2016).
3. **Bias Testing and Mitigation:** Companies should be required to test their facial recognition technology for accuracy and bias, and take steps to mitigate any identified biases.
4. **Prohibition on Certain Uses:** Facial recognition technology should not be used to identify individuals based on their political views, religion, or other sensitive personal characteristics.

In conclusion, the pervasive presence of Facial Recognition Technology in our society has brought about a range of complex ethical considerations and legal implications. While it has undoubtedly offered convenience and efficiency in identification and authentication processes, the widespread adoption of FRT has raised valid concerns regarding privacy and civil liberties. The examination of current legislation and ethical implications across various sectors has shed light on the need for responsible use and regulation of this technology. Moving forward, it is crucial to implement potential solutions that strike a balance between security and individual rights, ensuring that Facial Recognition Technology evolves in a manner that respects privacy, protects civil liberties, and fosters ethical practices in the future. Only through thoughtful and responsible deployment can we truly harness the potential of this technology while safeguarding the values and principles that define our society.

Conclusion

Facial recognition technology has emerged as a powerful tool in recent times however, its adoption raises numerous social, ethical, technical, and legal considerations that require careful deliberation and action.

From a social perspective, facial recognition technology raises questions about its impact on individual privacy, civil liberties, and human dignity. The use of this technology can lead to invasive surveillance, stigmatization, and discrimination, particularly for marginalized groups. As such, any deployment of facial recognition technology must be conducted with a deep understanding of the societal implications and the measures to mitigate any adverse effects.

Ethically, the use of facial recognition technology raises concerns over its accuracy and potential bias. The technology's reliability and accuracy depend on several factors such as the quality of the data used, lighting conditions, and facial expressions. This means that there is a risk of false positives or misidentifications, which can lead to wrongful arrests or accusations. Additionally, facial recognition technology can perpetuate bias and discrimination based on race, gender, or other factors, leading to unfair treatment of certain groups. It is, therefore, essential to ensure that ethical considerations are at the forefront of any decisions regarding the deployment of this technology.

Technically, facial recognition technology presents challenges related to data privacy, cybersecurity, and algorithmic bias. As with any technology that collects and processes personal data, facial recognition technology is vulnerable to data breaches and cyber attacks, which can lead to significant harm to individuals and organizations. Moreover, algorithmic bias can lead to errors in identifying individuals, perpetuating societal biases and prejudices. It is necessary to

address these technical challenges to ensure that facial recognition technology is reliable and secure.

Legally, the use of facial recognition technology raises concerns related to data protection, human rights, and legal liability. The legal framework surrounding the use of facial recognition technology remains patchy, with different jurisdictions having different rules and regulations. However, the development of comprehensive laws and regulations that govern the use, storage, and sharing of facial recognition data is critical in ensuring that individuals' privacy and data protection rights are upheld. Moreover, the deployment of facial recognition technology in public spaces must be evaluated in light of human rights laws, such as the right to privacy and freedom of expression. Finally, legal liability considerations must be taken into account in the event of errors or misuse of facial recognition technology.

To address these challenges, it is necessary to strike a balance between the benefits of the technology and its potential risks. This can be achieved by ensuring transparency in the deployment of facial recognition technology, allowing individuals to opt out of its use, and conducting regular audits to ensure that the technology is not perpetuating bias or violating privacy and data protection laws.

In conclusion, the adoption of facial recognition technology requires careful consideration of its social, ethical, technical, and legal implications. While this technology presents potential benefits, such as improving security and convenience, it must be deployed responsibly and ethically. To achieve this, it is necessary to establish clear legal frameworks, implement technical measures to address potential biases and engage in open and transparent discussions with all stakeholders. Ultimately, the deployment of facial recognition technology must be guided by the principles of fairness, accountability, and respect for human dignity.

Reflection

During my research on Facial Recognition Technology (FRT), I have acquired extensive knowledge about the risks associated with its implementation in our daily lives. Specifically, I have gained a deeper understanding of concerns related to surveillance, privacy, bias, and the various legislations surrounding this technology and its diverse applications. Furthermore, I have become more cognizant of the potential impact of FRT on marginalized individuals and groups, emphasizing the importance of considering their perspectives in the development of ethical guidelines and regulations.

Looking back, it would have been beneficial to include more case studies and real-world examples of ethical dilemmas to bolster my arguments. Although I provided a comprehensive review of the literature and conducted thorough analysis and discussions, incorporating additional examples would have illustrated the practical implications of the ethical considerations discussed in the paper.

As FRT continues to be increasingly integrated into society, it is crucial to ensure its usage aligns with individual privacy and rights, promotes social justice, and mitigates potential biases and risks. Research in this field should focus on developing more accurate and unbiased algorithms, enhancing transparency and accountability, and fostering public awareness and education regarding the implications of FRT. Moreover, an interdisciplinary collaboration among experts in computer science, ethics, law, and social sciences is necessary to address the complex and multifaceted ramifications of FRT.

Bibliography

ACLU. (2021, July 15). Stopping Face Recognition Surveillance. Retrieved from https://www.aclu.org/news/topic/stopping-face-recognition-surveillance

ACLU of Illinois. (2022). Biometric Information Privacy Act (BIPA). Retrieved from https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa

Al-Heeti, A. (2019, January 25). Amazon's facial tech shows gender, racial bias, MIT study says. CNET. Retrieved from https://www.cnet.com/tech/tech-industry/amazons-facial-tech-shows-gender-racial-bias-mit-study-says/

Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI and Ethics, 2(3), 377-387.

BBC News. (2020, February 27). Facial recognition: EU considers ban of up to five years. BBC News. Retrieved from https://www.bbc.com/news/technology-51658111

Buolamwini, J. A. (2017). Gender shades: intersectional phenotypic and demographic evaluation of face datasets and gender classifiers (Doctoral dissertation, Massachusetts Institute of Technology).

Business Roundtable. (2019). Consumer Privacy Legislation Framework. Retrieved from https://s3.amazonaws.com/brt.org/privacy_report_PDF_005.pdf

Cagle, M., & Ozer, N. (2018, May 22). Amazon Teams Up with Government to Deploy Dangerous New Facial Recognition Technology. ACLU. Retrieved from https://www.aclu.org/news/privacy-technology/amazon-teams-government-deploy-dangerous-new?redirect=blog%2Famazon-teams-law-enforcement-deploy-dangerous-new-facial-recognition-technology

Cartoon Movement. (2019, May 23). Facial Recognition. Cartoon Movement. Retrieved from https://cartoonmovement.com/cartoon/facial-recognition-0

Chilson, N. A., & Barkley, T. D. (2021). The Two Faces of Facial Recognition Technology. *IEEE Technology and Society Magazine*, *40*(4), 87-100.

Garvie, C., Bedoya, A. M., & Frankle, J. (2019). The perpetual line-up. Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology.

Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test (fvrt): Part 3, demographic effects*. Gaithersburg, MD: National Institute of Standards and Technology.

Hamann, K. & Smith, R. (2019). Facial Recognition Technology: Where Will it Take Us?, Criminal Justice 34.1 (2019): 9-13.

Hawkins, A. J. (2019, March 14). Senators introduce facial recognition bill that would force Big Tech to tell you how they're using it. The Verge. Retrieved from https://www.theverge.com/2019/3/14/18266249/facial-recognition-bill-data-share-consent-senate-commercial-facial-recognition-privacy-act

Hill, K. (2020). The secretive company that might end privacy as we know it. New York Times. Retrieved from https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Klosowski, T. (2020, July 15). How Facial Recognition Works. Wirecutter. Retrieved from https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/

Kostka, G., Steinacker, L., & Meckel, M. (2023). Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. Government Information Quarterly, 40(1), 101761.

Leong, B. (2019). Facial recognition and the future of privacy: I always feel like… somebody's watching me. *Bulletin of the atomic scientists*, *75*(3), 109-115.

Maguire, M. (2009). The birth of biometric security. *Anthropology today*, *25*(2), 9-14.
NEC New Zealand. (n.d.). A brief history of facial recognition. Retrieved from https://www.nec.co.nz/market-leadership/publications-media/a-brief-history-of-facial-recognition/

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

Miller, K. W. (2023). Facial Recognition Technology: Navigating the Ethical Challenges. *Computer*, *56*(1), 76-81.

Milligan, C. S. (1999). Facial recognition technology, video surveillance, and privacy. *S. Cal. Interdisc. LJ*, *9*, 295.

Mulholland, J. (2020)Tracing the History of Biometrics. Retrieved from https://www.govtech.com/public-safety/tracing-the-history-of-biometrics.html

Orwell, G. (2021). Nineteen eighty-four. Penguin Classics. (Original work published 1949)

Rowe, J. M. (2020). Regulating Biometric Surveillance: Comparative Lessons. Stanford Law & Policy Review, 24(STAN. TECH. L. REV. 1).

Scherer, K. (2005). Biometrics: Past, present and future. *Futurics*, *29*(3/4), 83.

Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019, January). Fairness and abstraction in sociotechnical systems. In *Proceedings of the conference on fairness, accountability, and transparency* (pp. 59-68).

Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *Ai & Society*, 1-9.

Snow, J. (2018, July 26). Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots. ACLU. Retrieved from https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28

Stromberg, C. (2019, September 20). Some Thoughts on Facial Recognition Legislation. Amazon Web Services, Inc. Retrieved from https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/

Thales Group. (n.d.). History of Biometric Authentication. Retrieved from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-biometric-authentication

Unar, J. A., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. Pattern recognition, 47(8), 2673-2688.

United States GAO. (2016, May). Facial Recognition Technology: Current and Planned Uses by Federal Agencies. Retrieved from https://www.gao.gov/products/GAO-16-267

Wang, Y., & Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of personality and social psychology*, *114*(2), 246.

Appendix

Past Section Portfolio Element:

https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-biometric-authentication

Present Section Portfolio Element: https://www.netflix.com/title/81328723?source=35

Future Section Portfolio Element: https://cartoonmovement.com/cartoon/facial-recognition-0