Introduction

AI has now made its way in almost every field such as health, finance, defense and security, and social platforms. Among its applications, facial recognition technology is noteworthy for its high popularity but also clear violation of people's rights and privacy. This technology although improves security and comfort puts into question important issues of fairness of algorithms and personal data protection. Discrimination effects are a result of bias in the facial recognition system while privacy issues can also be stated, such as the unauthorized collection, storage and possibly misuse of people's data. These concerns lead to increasing user stress, which is indicative of user concerns about privacy and the inability to manage personal information (Dilmaghani et al., 2019). This research is designed to explore two main areas, the bias and privacy issues with facial recognition technology and how these can cause users to have anxiety.

Research Question

This research aims at identifying the potential sources of specialty, privacy concerns, and consequently felt anxiety arising from using facial recognition technology.

- What is the diverse bias that occurs in the facial recognition algorithms? This question looks at how facial recognition technology is likely to be either more likely to misidentify a

person or fail to recognize them based on their ethnic background or sex or any other demographic facet. This paper explains that understanding these biases can help call out possible discrimination and unfairness of AI.

- What risks and concerns are associated with utilization of facial recognition technology? This question explores whether facial recognition systems violate individual rights, particularly the right to privacy, by analyzing their practices of data collection, sharing, and retention.It aims at discovering how these systems manage personal information and threats coming from misuse or unlawful access when facial recognition technology is used.

- In what ways do these biases and issues with privacy affect and contribute user stress or anxiety?

This question focuses on the psychological aspect, researchers want to examine how much users know about the biases and privacy issues related to FRT and also the degree of trust users have when using this technology, their feelings of being controlled and the anxiety this might cause.

Answering these questions, the research will contribute to the understanding of the ethical and social impacts of the implemented facial recognition technology and foster the creation of the advanced and socially friendly AI.

Literature review

Facial Recognition Technology (FRT) is a technology that recognizes and authenticates a user using the face mapping technology. Some of the popular uses of biometrics are applied in security systems, smartphones, healthcare and safety of the public in general. However, FRT is not ethically and socially benign; in fact, it has a variety of issues. Some of them are loss of

privacy because data is collected from various sources without permission, mistreatment in line with algorithms preferred by minorities and stress resulting from constant monitoring. This literature will explore the societal impact of FRT by examining three critical areas: that can make people uncomfortable with the idea, including privacy issues, or illustrate that an algorithm used to assess learning might have biased results and create psychological issues such as technostress in learners. Based on the literature analysis and survey of 43 firms with FRT implementation, this study contributes to the literature regarding a preliminary and comprehensive evaluation of FRT.

Privacy Concerns in Facial Recognition Technology

Privacy is one of the most important ethical concerns likely to be connected with Facial Recognition Technology (FRT). The use of the technology in cases where it captures, processes and stores biometric information has triggered security concerns about individual rights and freedoms. Zuboff (2019) has put this discussion under the category of 'surveillance capitalism,' and pointed out that FRT is used to accumulate data about people without their permission. This results in creating conditions of people's permanent supervision, to which people remain exposed and their sense of individual freedom is weakened. It is stated that in settings such as public places where people cannot choose whether to leave their privacy open to inspection, implementation of FRT is an absolute invasion of privacy.

To these concerns, Solove (2010) has elaborated a deficit in transparency in handling the collected data. Most people are likely unaware that their facial data is being collected, processed or even sold to third parties. This erasure of how these FRT systems function thereby prevents individuals from being able to consent to, or opt out of, the use of their biometric data. The lack

of informed consent is especially problematic where it is unclear whether an organization is a public entity or a company: both may misuse this technology. For instance, the private sector may use facial data to sell their products and services, but on the other hand, the government may use it for surveillance purposes with little or no regard at all on the consequences.

This is made worse by the idea of 'function creep' which adds complexity to the ethical use of FRT. According to Nissenbaum, (2004) contextual integrity holds that privacy is violated where information collected in one context is used in a different one without the parties' consent. Function creep is apparent in FRT applications because a tool adopted for security may later be applied for marketing, monitoring employees or policing. These other uses are not only different from the intended use but also take the little public trust that exists in ethical usage of FRT away.

A third major issue from a privacy concerns perspective relates to the pathological, that is, the inability to change biometrics data once captured. Schneier (2015) has noted that unlike a password, compromised facial data cannot be changed or replaced by someone whose facial data has been compromised is compromised for life. Such data if exposed to breaches or unauthorized access, increases chances of identity theft, fraud and impersonation. This is made worse by inadequate advanced mechanisms to secure the stored biometric data so as to lock the users into long-term risks.

The same can be said about the regulation of FRT concerning the insufficient means to tackle the issue of privacy. Regulatory gaps still persist with many jurisdictions-including those whose laws governing biometrics having little or no provision for the special problems that biometric technologies like facial data may present. Because the regulation of FRT remains insufficient, there is no brake that can slow down the growth of such an aberration; simultaneously, privacy

violations and power dysphoria are regularly repeated, including between those who use FRT and those on whom the corresponding decision is made.

In addition, privacy is NOT independent of issues of fairness and bias and the invasion of privacy disproportionately targets marginalised groups. This is especially so because minority groups such as blacks are over-policed in settings within which FRT is operated, thus contributing to existing socio physical bias. It is for this reason that this intersection highlights
the fact that privacy violation is as relevant a discussion as algorithmic abuse and its
accountability, more of which is discussed in the next section.

When privacy is placed within these ethical technological and legal perspectives, it is evident that the deployment of FRT could be a real threat to privacy and social and individual liberty. The absence of such considerations means that the challenges not only erode the public's trust but also create the conditions for further pervasive ethical breaches, which can be examined in the analysis of algorithmic bias below.

Algorithmic Bias and Discrimination in FRT

Although privacy is an important factor abounding the ethical issues on Facial Recognition Technology (FRT), so it is for algorithmic bias and discrimination. It has become evident that most of these FRT systems were trained from data sets that do not have much diversity, and therefore, the models are performing so poorly for any women and specifically, those with dark skin. These are not only issues about the stability of the technology in question, but also about making people from the vulnerable groups suffer double.

The biases listed above have been studied comprehensively among academic and corporate

researchers, and Buolamwini and Gebru (2018) were the pioneers in providing an organized account of them in the case of gender classification systems. They realized that dark skin women were misclassified at 34.7% while light skin males were less than 1%. They are due to the fact that datasets used for training FRT belong to predominantly white male subjects and do not allow machine algorithms to generalize the results. The inaccuracies caused by the technologies can be lethal in certain high index usage such as security and policing since they could misidentify people leading to wrong apprehensions or exclusions in immigration.

Grother et al. aimed at investigating the demographic impact of FRT systems in a work environment they undertook at the National Institute of Standards and Technology (NIST) in 2019. What they found out was that false match rates were higher among Asian and African Americans as compared with whites. This implies that FRT systems are not blind but are rather a result of trained bias and these are escalated by the systems. The bias is not only a problem from a technological point of view but generates important ethical issues related to fairness and responsibility.

They found that FRT system bias highly correlates with bias in society and amplifies the marginalization of the affected groups. Noble states this as “algorithmic oppression” about how these computerised systems reinforce as well as augment power relations. For example, the application of FRT in policing has been logically associated with racially profiling people of color, who are always monitored and supervised proportionately more heavily. These biases do not only affect the more rational application of FRT but also risk the credibility of institutions that adopt such technology.

Algorithms and FRT system biases originated from the system development and use procedures.

O’Neil (2016) affirms that such skewed consequences stem from non-prejudice training data sets and inadequate supervision and responsibility in the design. There is also the problem that developers can accidentally write bias into their algorithms—by not using diverse data, or by not auditing the model for fairness. Meeting these demands does demand a more proactive strategy for increasing the diversification of the dataset, along with proper auditing to determine as well as correct biases before use.

Bias in FRT systems also can be presented as a question of the ethical usage of non-human agents in decision making. According to Leslie (2020) it is hard to weigh or contest the outcomes in many machine learning models due to the obscurity of the models used. The problem can be referred to as a “black box” issue because it is challenging to understand how FRT systems make specific decisions; specifically, it is desirable to know why, for example, a credit or entry to a particular area should be provided. This means that transparency and accountability in these systems must be safely guarded in order to retain the public trust.

It is therefore important to make a difference between the bias inherent in technological design and bias emerging from the way in which FRT is introduced into society. For instance, when FRT is applied to security in crowds, the ensuing supervision is viewed with a high likelihood towards discriminated groups of the population. This only perpetuates the culture and practice of discrimination and exclusion to people with disabilities, as well as deepens existing social inequalities. To address these concerns, the policymakers in collaboration with the developers need to come up with ethical measures of measuring the performance as well as regulation policies that can fully accommodate fairness to all.

Some of the major ethical problems implementation of FRT systems present include:

Algorithmic bias whereby the system tends to make unfair decisions based on race or gender thus violating the parties privacy while at the same time perpetuating social injustices currently taking place in the society. Solving the problem, therefore, needs the coordinated efforts of using diversified training datasets, enhanced audits, and more responsible and accountable processes and systems. These solutions are of significant importance not only for the enhancement of FRT ‘s reliability and minimization of bias but also for the proper functioning of the technology without causing negative impacts on all the individuals involved.

Psychological Impacts of Facial Recognition Technology

This research reconstructs the psychological impact of FRT on all people, in terms of stress, mistrust, and a sense of disempowerment. Even though FRT is marketed for ease and security features, constant application of FRT results into rather high psychological pressure. One great concern is technostress, which stems from a change process to accommodate new technology and the consequent monitoring that such technologies allow. According to Zuboff (2019), FRT conceals constant watching, and undermining people’s freedom and trust. The fully implemented FRT in the airports or public surveillance in city centers; is placing individuals in fairly helpless positions thus they cannot choose when and how their data is being collected and analyzed – which leads to increased anxiety. It is even worse for FRT systems because they are mostly not transparent about how they make their decisions. According to Nissenbaum(2004), contextual integrity is violated where people cannot anticipate or influence how their information will be applied. Skepticism is aggravated by the fact that FRT uses ‘black box’ systems (O’Neil, 2016) whereby people again remain in doubt as to whether their biometric data will be processed appropriately or inappropriately. This mistrust is especially heightened among marginalized groups, as explained in the previous section, that not only might they undergo prejudiced

misidentification but also systematic prejudice. The psychological burden is not only the individuals' issue but also the social issue. Zuboff (2019) also predicted the world as a surveillance society in which individual and society freedom of expression is suppressed and fear is promoted. This results in self- censorship and recluse behavior that negates the social fabrics as well as human flourishing. To avoid these effects, more transparency, strong data protection legislation, and users' access to biometric information are obligatory. In order to decrease stress and mistrust, ethical frameworks should respect user responsibility, and be as open as possible to everyone as possible to establish more objective relation between person and FRT.

Existing Solutions and Gaps in Research

The issues raised by FRT have occasioned numerous measures designed at managing privacy threats, issues of bias in the algorithms, and the stress induced by technology. One primary solution therefore is to design AI models that are: Annotate; Auditor; ATM. Transparency helps users and regulators know how FRT systems work to reduce the extent of mistrust and technostress (O'Neil, 2016). But achieving true transparency becomes an issue of concern especially when analyzing many FRT algorithms since many of them are complex. Another way of dealing with algorithmic bias has also been suggested by using auditing systems. For example, Buolamwini and Gebru , insist on yearly audits of algorithms to reduce bias of the model over different groups of people.

Another method of increasing the FRT is related to the use of various datasets. Research also points out that racially-biased FRT algorithms are often a result of bad quality training data. The implementation of FRTs from different datasets has been found to eliminate chances of errors for the disadvantaged groups, making FRT applications less discriminative (Noble, 2018). FRT

concerns also involve legal and regulatory aspects that are a central consideration in improvements in this area. Some jurisdictions have however placed limit or banned the use FRT in policing due to rising concern of misuse (Benjamin, 2019).

However, these solutions still leave wide gaps. In many areas there are no exhaustive set of rules to govern the protection of privacy thus making protection a fragmented issue across regions (Solove, 2010). Furthermore, there is an expectation of algorithmic explainability even if they are black box, which may be hard because the technical process of FRT makes it challenging for other stakeholders to analyze to be able to oversee and hold accountable. Current literature also fails to address adequately or consider medium to long term psychosocial effects like Technostress on users of FRT. Closing these gaps however will necessitate more interdisciplinary studies that will entail the input of both technologists and ethicists and policymakers. As it progresses in these fields, potential FRT developments in the future may enhance their consideration of user privacy, erase bias, and bring down technostress.

Methodology

In this study, the approach used is intended to examine issues of privacy, prejudice in algorithms, together with psychological effects of Facial Recognition Technology (FRT). To this end, the following objectives were done and a mixed research design was used, involving both quantitative and qualitative research methods. These two enable an appreciation of FRT's social values and returns both in macro and micro contexts at the same time.

The quantitative part is an online questionnaire, which has been created to capture a range of participants' gender, age, education, occupation, and ethnicity, as well as their Self-perceived fairness, trustworthiness, and psychological impact of FRT (Benjamin, 2023). To augment this

knowledge, semi-structured interviews were carried out to obtain rich descriptions on how people have encountered FRT and the violations, prejudices, and technostress encountered.

This methodological framework guarantees that the phenomenon is most likely covered comprehensively, and statistical data received is enriched with the idea of the context. The following sections provide a full account of the design and data collection methods used in this study, key ethical considerations and analytical procedures used in the analysis of data.

Research Design

This study employs both quantitative and qualitative research to assess the privacy, biased and psychological effects of integrated Facial Recognition Technology (FRT). This paper uses a survey as the main quantitative tool while the literature review is considered the qualitative data to answer the research questions exhaustively, both quantitatively and qualitatively.

The questionnaire was developed with an aim of collecting data on FRT concerns among the public, specifically the following concerns; trust on organizations, privacy, and psychology of technostress. The use of Likert scales of questions aimed at capturing trends while open ended questions offered supplementary qualitative results. This method was vital because of the potentiality in gathering a wide demographic's opinion (O'Neil 2016; Buolamwini & Gebru 2018). For the first qualitative indicator, a broad literature review was carried out to better understand the survey results in more detail. Sources were credible with the majority being academic articles, books and documented reports; these included aspects related to algorithmic risk, privacy infringement and psychological impact of surveillance systems. This technique enabled the occasions of the study to amplify on theoretical and empirical analysis that already

existed, filling gaps in the primary data.

In this research, survey data is cross-checked with data from the existing literature to ensure reliability and to present multiple perspectives on the social/ethical and psychological implications of FRT. This design will ensure a notion of encompassing coverage of the research question by arguing the views of the public together with those of scholars.

Data Collection Methods

The methodology used for data collection in this research was meant to exhaustively examine FRT's ethical, social and psychological issues. Both quantitative data; based on a structured survey and qualitative data; obtained through a review of relevant literature were used (O'Neil, 2016). Such an approach helps to grasp the research questions systematically, and, therefore, to lend the results a sophisticated perspective.

The survey was the main source of quantifying the data that was required for this study. The information, was disseminated through the internet, email list, and social networking sites that would ensure it got to those interested in the information. The questions that were formulated were intended to elicit personal details about the participants like their age, gender and ethnicity, then their perception on issues of FRT. Concerns such as privacy invasion, fairness, and psychological consequences were other issues discussed and technostress was singled out. People were asked how much confidence they have in the organizations that operate FRT, how fair and accurate any FRT is across demographics, and their level of support in certain fields, including the police, and banking institutions. Instant, free-form questions were also posed to ensure that participants had additional means to express their opinions and expand the amount and quality of

the data. The survey administration was conducted using self-administered questionnaires and the sampling technique utilized the surveys was convenience sampling, power constrained by the available resources. Although, this approach had its limitations regarding perceived demographic representativeness, extra efforts were made to enlist people from all sectors to get different perspectives. The questionnaire generated a high level of response and the responses provided a rich data set on which the study could be based and which also indicated how the public could be expected to view FRT.

The qualitative part of the research included a rather detailed analysis of the existing literature. This method was chosen as it would inform the survey findings in an expanded view supported by other research. The literature review focused on three main areas: Privacy issues, issues to do with fairness in algorithm and psychological aspects of FRT such as technostress. Theoretical information was obtained from peer-reviewed articles, books and industry reports, focusing on the theoretical and empirical analysis of the ethical and social aspects of FRT. The contemporary discursive field was framed by prior works, including Nissenbaum's contextual integrity theory as well as Zuboff's research on surveillance capitalism. The case of algorithmic bias by Buolamwini and Gebru got into the performance difference of FRT across the demography of people On the broader perspective of the impacts of surveillance technologies, the technostress study depicts the physiological effect of the technologies.

The choice of articles for the literature review was based on their connection to the study questions; reliability; and the degree to which they addressed FRT. To examine common threads and areas of future research opportunity, the review combined data from ethic, computer science, and psychology literature. This qualitative component gave a better explanation to the findings of

the survey in as much as the theory behind those findings. Combining the survey and literature review, there was data collection model used in the study. Where the survey gathered concrete data coherent with general population sentiments, the literature review achieved theoretical density and situatedness, presenting a semiotic and conceptual grounding out of which the diverse effects of FRT may be read. This dual approach was useful to make sure that the research not only covers the statistical side of the technology, but the social side of it too.

Sampling Strategy

Based on the research objectives, the sampling strategy for this research was to capture variation and generalizability in the interaction of the public with FRT. Convenience sampling approach was used in the quantitative survey where the respondents were contacted through emails and social media handles. One potential limitation of convenience sampling is related to external generalizability, however, considering time and resource constraints, convenience sampling was chosen. An attempt was made to find as many participants of different age, gender and ethnicity in order to have a broad spectrum of opinions on privacy issues, algorithmic fairness, and mental effects of FRT (O'Neil, 2016).

For the qualitative component of this study, the sample for the literature review was selective and intended to be purposive in that it only used scholarly work. Besides, the selection of articles and papers was concerned with ethical and social issues of FRT, such as biases, privacy invasion, and psychological impact. The kind of sources that were used in this study were selected depending on how closely they were associated with the research questions, the credibility of the sources and whether they have been published in academic or professional scholarly journals.

In both components, the diversity was backed to capture the broad effects of FRT on individuals

of different strata. The study achieved enhanced comprehensiveness through the use of convenience sampling to obtain survey participants while using purposive sampling to select the literature sources related to FRT.

Limitations

- It was conducted using a convenient sampling technique, which limits the study to portraying the views of a specific population on FRT. Respondents were mostly those, who were able to attend online programs, which might decrease range of demographic variation.
- The qualitative part of the reseaech is limited by the materials available in the body of literature for review. Despite the fact that only diversified and reputable sources were used, the findings might not give a broad picture of emerging problems and different viewpoints.
- Answering a survey, people can be overoptimistic, or their answers can reflect their limited knowledge of FRT. They include Political, social, economical, method and purpose or sample biases which may affect the accuracy of the collected data.
- That FRT could not be explained with first-person and qualitative sources, such as interviews or focus groups, does not allow to identify and convey some cultural experiences and attitudes towards firearm use.
- The evidences can only be generalised when finding the gaps that exist in the study but can point towards the populations and contexts not represented in this study.

Research findings

Facial recognition systems technology FRT is a system used in the modern society for security purposes, law enforcement, financial services as well as in the social media platforms. The use of FRT has been extensive and under criticism given its ethical, social and psychological impacts. Issues to do with likelihood of privacy invasion, the correlated prejudice in the algorithms, and the resultant mental health implications of surveillance, have emerged as key social issues of concern in the conversations regarding acceptable and humane use of this technology.

In exploring the FRT effects, this study considers three broad domains of research interest. Data privacy is an essential concern; more so the use of biometrics data without express permission and more so with doubts over organizational capacities to handle such data appropriately. The problem of how bias is introduced into algorithmic solutions also affects the use of FRT; studies prove that facial recognition algorithms work incorrectly for particular subjects, provoking discussion on fairness issues. Moreover, the psychic effect of FRT, especially the feelings of fear and awkwardness associated with pervasive surveillance as well as potential abuse of the facial data constitutes a major threat to utilitarian uptake and confidence.

Within this study, survey data is analyzed alongside literature review as a means of attaining maximal methodological variety. The fact is that the survey gives substantial proof of the general population judgement that can help in identifying their understanding of the issue, and the literature review places the findings of the survey in more academic context. That way, no aspects of social and ethical relevance to FRT are overlooked. Through these themes, the research hopes to bring valuable insights to the current work that is being done to address issues of bias, opacity, and user-centrism in facial recognition technology. The results emphasise the

necessity for the development of legal standards, ethical standards, and technology solutions for privacy, fairness and psychological concerns related to FRT.

Survey

Considering the survey results, responses will be split into three basic sections that will help to reveal the audience's attitudes towards FRT. The demographic portrait of the respondents will be analyzed by ethnicity and gender in the first stage since such a breakdown would enhance the understanding of the distribution of attitudes towards FRT and possible differences among the population subgroups. Second, attraction between fingerprint implement and FRT will be compared to understand the level of public trust and acceptance towards the two distinct biometric technologies (Benjamin, 2023). Finally, attitude towards FRT usage in public areas will be measured to determine the perceived ratio of security gains to privacy losses. It organizes the volume in a thoughtful and logical manner to encourage sharpened perspectives on the social and ethical implications of FRT.

i. Distribution of Responses by Ethnicity or Gender

There were participants from different ethnic and gender backgrounds to ensure that assumptions regarding the impact of demographics on perception and usage of FRT were tested. Out of the 50 respondents, 36 said that they were White, while 5 said Black, 4 Asian, 3 Mixed ethnicity and 1 Arab. Seven respondents did not want to specify their ethnicity. This distribution shows a concern as we reported more white participants, although it offered understanding of their perceptions toward the given issue, yet cannot be a good representation for other underrepresented ethnic groups. It is also important to note that Black and Mixed minority participants especially showed

higher levels of concern and perceived unfairness and inaccuracy of FRT. This is in consonance with prior research finding that FRT systems are less accurate or even targeting those in these categories, and as such, algorithmic technologies are not free from bias.

The survey also got responses from 29 females and 21 males. The FRTs' privacy concerns and psychological discomfort were more often reported by female participants than males. Most of them expressed concerns of apprehension which they attributed to FRT as being invasive. Interestingly, male respondents were slightly more inclined to the use of FRT in public areas with references to security being more common. These learning point to the essence that, FRT has been perceived differently under the different sexes; whereby the 'female' sex was more sensitive to the potential misuse of Surveillance technologies.

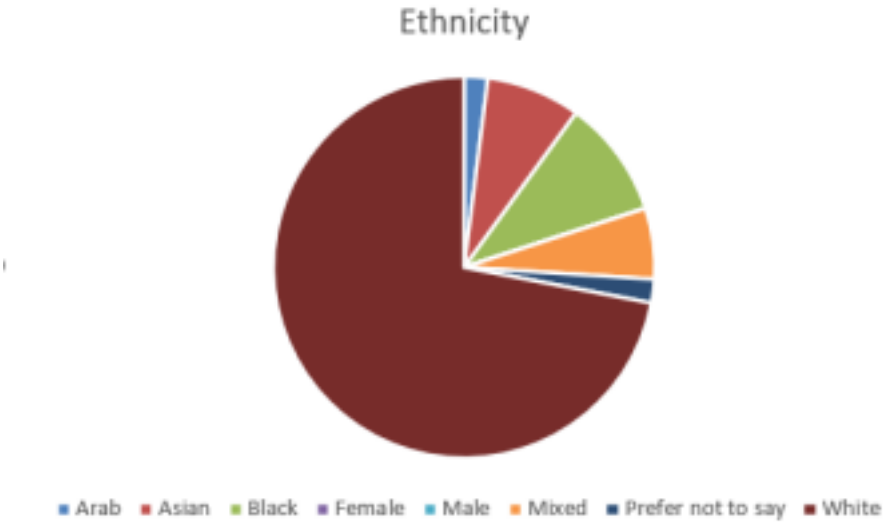

Figure 1 Distribution of Survey Respondents by Ethnicity and Gender

When ethnicity and the gender were analyzed further, it was found that minority women were the most skeptical of FRT. Some of the subthemes that emerged from the discussion of this group include; Privacy violation, Fairness, and Malice, which is the intersectional bias whereby several prejudice experiences with technology are worsened due to other prejudice. The above results

provide insights on inequities of FRT across constituencies affirming a call for fairness and inclusion in development and application of FRT.

The results of demographic analysis of this survey illustrate the need for diverse representation in FRT both in research and practical contexts. It is evident that there are trust and fairness deficits in current communication that have to be interdisciplinary in nature: the increased level of suspicion and concern among both minorities and female participants needs to be met for strategic communication to be effective. Based on these findings, FRT implementing organizations should step up the process of eliminating algorithm bias and enhancing the technology's visibility to the population, especially the vulnerable groups. This data also portrays the need to have responsible and fair FRT systems that meet the needs of the other users apart from the most commonly used ones.

ii. Preferences for fingerprint biometrics vs. FRT.

The survey conducted for the purpose also pointed out that respondents preferred fingerprint biometrics than FRT. The participants were asked to indicate their preferred modality of data collection if not FRT, with a vast number of the participants choosing fingerprint recognition due to its accuracy. This trend correlates with people's expectations' increase of FRT ethical and technical restrictions, including its vulnerability to manipulation and biases. There is more trust in fingerprint biometrics, mainly because people feel that with this method they are safer and it is more reliable. Fingerprints are considered to be static and owned by a person, and there are fewer believed threats of wrong identification or misuse compared to faces data. A large number of participants linked fingerprint systems with lower chances of surveillance misapplication because these systems are localized, being used only in workplace security, and personal device

identification. On the other hand, FRT was reported to be invasive and easily misused especially in the public domain or by private organization without appropriate legal frameworks.

Figure 2 Preference for Fingerprint Biometrics vs. Facial Recognition Technology (FRT) Among Survey Respondents We identified four main themes as resonating with respondents' answers, with an important one referring to data harvesting by facial recognition systems. Interviewees also raised concerns on FRT being applied for other uses apart from its intended use, a case that is termed as 'Function Creep." These questions made fingerprint recognition popular, as this method is already considered as more organized and clear compared to other ways of personal data collection.

Another reason for such preference is the relationship of FRT with algorithmic bias, which is another major driver considered to be driving the market for fingerprint biometric. Several respondents described their knowledge of problems associated with FRT systems, including their low accuracy compared to mugshots. These biases are also unethical and reduce the reliance on the technology by people. In comparison, the use of fingerprint recognition is considered as less endurced as a bias since the methods functioning is based on physical attributes which are not susceptible to misinterpretation by the methods functioning. This renewed preference of

fingerprint biometrics over the FRT also embraces the underlying issues of psychological consequences. All of the participants associated FRT with increased stress and discomfort, fear originating from the impression of being constantly watched and loss of control over the personal information (Benjamin, 2023). Fingerprint systems are people's recourse considered less invasive as compared to others hence fewer people complained about it.

iii. Opinions on FRT implementation in public places.

The survey also showed there was a split between the population in the use of Facial Recognition Technology (FRT) in public places, due to supporting the benefits, though worried about the overall impact. A significant number of participants approved the FRT use in public areas and stressed the effectiveness increase of security measures, especially in airports, law enforcement, and events monitoring. Again, these respondents expounded that; FRT can help give real timely alerts of possible dangers, replace time-consuming procedures including boarding or access control, and help enhanced public security. Some of them argued that FRT is much more useful than it is dangerous, especially when precautions are taken with the technology.

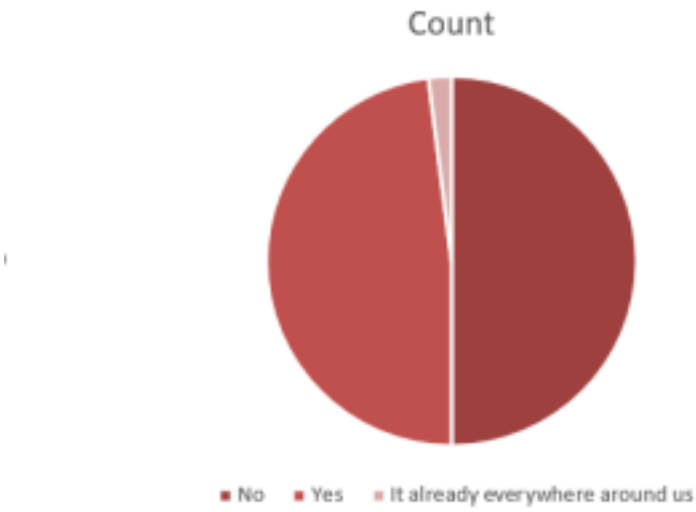

Figure 3 Public Opinions on the Implementation of Facial Recognition Technology (FRT) in Public Places

On the other hand, a similar proportion of the respondents was against FRT being installed in public places with privacy infringement being their main complaint. Some made concerns based on privacy and referred to the state as one of surveillance. This group also expressed various concerns about how facial data is obtained, stored & applied especially by private industries & or government departments. Concern with invasions of privacy-some kind of resale of data to other companies or other uses of data for purposes which were not intended, added to the concerns.

The concerns related to fairness and bias were ringing throughout the arguments against FRT in public places. Some of the respondents especially the minority ethnic ones suggested that at times FRT systems are so wrong that they can be used to enforce discrimination in that people will be identified wrongly. The failure to trust the technology to be accurate and fair exposes the primary reason why its introduction to the public domain was fiercely fought (Benjamin, 2023).

The remaining set participants had so rare attitudes, which are essentially preoccupied with both the advantages and disadvantage of FRT. Others argued that FRT is everywhere in one form or

another and therefore extending its use in public places will be continuous. But they urged that regulation must be tight in other to curb misuse while encouraging ethical use.

More generally, the current study suggests two distinct attitudes towards the use of FRT in public areas which depends on the nature of benefits that is associated with the application of this technology, privacy concerns, and reliability of the technology. To mediate this disparity, it is useful to discuss the limitations and vices of FRT which provokes corresponding ethical and technical issues, primary ways of their solution, such as establishing appropriate regulations, revealing certain practices, and dealing with algorithmic bias. To achieve the equitable and proper use of FRT in public domains, crucial to gain public trust.

Literature review

The existing literature on FRT provides evidence of its duality and serves as both an innovative technological solution and a potential source of extensive ethical, social, and psychological problems. Another area of interest in the currently available literature is the dual nature of the technology, with its functionality and potential to cause privacy concerns, Algorithmic bias, and potential psychological effects such as technostress. These issues are hence crucial in identifying all the other impacts of FRT to the society.

Privacy is currently one of the biggest issues of contention concerning FRT. Zuboff (2019) and Solove (2010) have argued that consent is slippery virtually, meaning that the technology works and leverages personal data without the consent of the owner, thus denying them right over their data. Nissenbaum's (2004) theory of contextual integrity presents an issue because FRT takes facial data and improperly flows it through appropriate channels. One of the perennial problems mentioned in the literature is 'function creep' by which FRT systems that are initially intended

for security are subsequently used for other purposes, for instance marketing or mass surveillance and hence diminishing public trust. Also, as Grother (2019) and Schneier (2015) observed, face templates cannot be ‘reset’; thus, compared to other biometric data breaches, violated facial data poses individuals to identity theft and impersonation. It is also important to understand that many of these privacy concerns stem from a relative legal absence of considerable legal rules that govern the FRT application as Grother (2019) pointed out, and this makes users susceptible to misuse. Algorithmic bias presents yet another challenge which can be understood as a major one. Research by Buolamwini and Gebru (2018) shows that POC are over-estimated and their gestures mis-interpreted by the FRT systems more often than lighter males, thereby proving that the respective error rates are far more acute for them. This bias

comes from non diverse training data and strengthens unique social disparities. Possible negative outcomes of misidentification resulting from algorithm bias include arrest of wrong suspects or failures to provide services such as loans, which are discussed by Grother et al. (2019) reviews indicate that solving this problem will involve the need for varied data sets, more frequent audits and ways for developers and organizations that incorporate FRT systems to be held to account. However, none of these proposed solutions provides detailed explanations of how they can be implemented and, thus, many systems continue to display discriminative characteristics.

Other effects on the psychological well-being of individuals have also expressed interest, especially technostress. Technostress from Zuboff (2019) is attributed to the surveillance features of FRT which makes users uncomfortable, uncomfortable and dependent. It is crucial for these authors to point out that the relative invisibility of the processes of data collection aggravates this stress by creating the feeling of lack of control by the user over their data. This sort of strain is

especially significant since such populations suffer higher misidentification and targeting by FRT systems. Noble's contribution in the area of technological alienation shows that the kinds of experiences lead to an avoidance of technologies using FRT and mistrust of digital systems.

Discussions

The implications and arguments from this study combinedly serve to identify and analyse the function and consequences of FRT on privacy, discrimination, and psychological health as well as the potential perception and concern of the people towards its applicability in different sectors. These ideas are based on survey responses and a review of the literature that present a fair assessment of the difficulties associated with FRT.

The survey established that there is a general public preference for fingerprint biometrics than FRT based on the likelihood of effectiveness in that people feel that fingerprint biometrics is more reliable, has more privacy and cannot be misused than FRT. A significantly large number of respondents saw FRT as intrusive and mentioned worries about unauthorized gathering of information and its use, which the present research backed up. The oppositionists of FRT include Zuboff and Solove who beg to endorse FRT on the grounds of surveillance of people and nurturing of suspicion. This is in support about responses to the survey where most of the participants expressed discomfort with having FRT in public domains especially when consent and anonymity is not well articulated.

Another key focus was algorithmic bias that developed as a complex topic in the last few years. While testing the app, the female and minorities were less less confident with FRT's impartiality; some cited the prejudiced results mentioned by Buolamwini as well as Gebru. Such biases are not only prejudiced with the social stratification system, but they also diminish public confidence in

the utilization of the technology. The most clear solution from the survey responses and the literature was the requirement for diversified training datasets and rigorous audits.

Technostress and anxiety were evident as primary topics of concern in the forum. The survey showed that a majority of respondents were uneasy with FRT application in the public area in synergy with Zuboff ideas referring to the surveillance society as a space where state power reduces the decision-making scope. This is worse due to absence of control over biometric data, which in turn increases helpless situations.

Altogether, these conclusions point up to the necessity of ethic guidelines, legal controls, and technological advance solutions for FRT problems. Closing the trust, fairness and transparency gap is key to its proper and ethical use in society.

Conclusion

FRT stands for Facial Recognition Technology, which has become a rather sophisticated form of biometrics; the advantages of which are apparent in security expectations, convenience, and productivity. However, this study highlights three critical challenges associated with its adoption: those are privacy infringements, biase in the algorithms, and the psychological effects for example; technostress. These challenges are central to ethical and societal issues that need to be answered to guarantee safe application of FRT. That is because FRT entails the collection and processing of biometric information absent the best practices in informed consent. The issues experienced in this study show that data is processed and stored in opaque ways; this erodes trust and opens individuals to the likelihood of identity theft and foul use of their data. The rules are still largely disconnected and inadequate, which makes it impossible to shield the users' data. Algorithmic bias is another crisis level problem today. This paper and the previous research show

that FRT has considerable errors in various studies, and the recognition is worse for women and minorities. These biases perpetuate existing societal premis of unfairness, methods such as forensic searches and identification in cases like law enforcement, are highly sensitive and wrong identification leads to serious repercussions. Stress, anxiety, alienation added to the growing list of the negative psychological effects of FRT which makes the integration of FRT into society even more challenging. The use of FRT in public domains makes citizens become someone they are not in order to fit societal norms creating a surveillance society also kills societal trust. To overcome these challenges, therefore, there is need for multi-sectoral approaches. This means it is incumbent on developers to ensure fairness by creating a more diverse set of datasets for training models, and frequent auditing of algorithms. Policy makers should create sufficient legal barriers that would enhance the transparency, accountability and control of the biometric data among the users. Last but not least, integrated cooperation of specialists included technologists, ethicists, as well as psychologists is needed to reduce consequences in the sphere of FRT on the society level. These challenges can then be further resolved to ensure that FRT becomes far more ethical and integrated to social equity and human rights to technological advancement.

References

Benjamin, R. (2019). Race After Technology: Abolitionist Tools for the New Jim Code. Polity.

Brewer, P. R., Bingaman, J., Dawson, W., Painstil, A., & Wilson, D. C. (2021, August). Explaining public attitudes toward facial recognition technology. In TPRC49: The 49th Research Conference on Communication, Information and Internet Policy.

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 81, 1-15.

Dear, K. (2018). Towards a psychology of surveillance: Do ‘watching eyes’ affect behaviour? (Doctoral dissertation, University of Oxford).

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. National Institute of Standards and Technology.

Lai, X., & Rau, P. L. P. (2021). Has facial recognition technology been misused? A public perception model of facial recognition scenarios. Computers in Human Behavior, 124, 106894.

Leslie, D. (2020). Understanding bias in facial recognition technologies. arXiv preprint arXiv:2010.07023.

Matulionyte, R. (2024). Transparency of facial recognition technology and trade secrets. In The Cambridge handbook of facial recognition in the modern state (pp. 60-73). Cambridge University Press (CUP).

Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(1), 119-158.

Noble, S. U. (2018). Algorithms of Oppression: How Search Engines Reinforce Racism. New York University Press.

O’Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishing Group.

Robinson, J. P., Livitz, G., Henon, Y., Qin, C., Fu, Y., & Timoner, S. (2020). Face recognition: too bias, or not too bias?. In Proceedings of the ieee/cvf conference on computer vision

and pattern recognition workshops (pp. 0-1).

Roundtree, A. K. (2021, June). Ethics and facial recognition technology: An integrative review. In 2021 3rd World Symposium on Artificial Intelligence (WSAI) (pp. 10-19). IEEE.

Ruane-McAteer, E., & Prue, G. (2022). Psychological aspects of active surveillance. World Journal of Urology, 1-5.

Saluja, S., & Douglas, T. (2023). The Implications of Using Artificial Intelligence (AI) for Facial Analysis and Recognition. Journal of Student Research, 12(3).

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.

Solove, D. J. (2010). Understanding Privacy. Harvard University Press.

Steinacker, L., Meckel, M., Kostka, G., & Borth, D. (2020). Facial recognition: A cross-national survey on public acceptance, privacy, and discrimination. arXiv preprint arXiv:2008.07275.

Usha, S., Geetha, A., Santhakumar, J., & Sundaravadivazhagan, B. (2024). Biometric Facial Recognition and Ethics. In AI Based Advancements in Biometrics and its Applications (pp. 118-139). CRC Press.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

Link to survey

https://docs.google.com/forms/d/1EBtMzv3UIygBT78cXndR0ayO62RVBMHM9YmDv49BkPc/edit