PIONEER
ACADEMIC PUBLISHING LIMITED

Journal of Research in Social Science and Humanities
ISSN 2709-1910
www.pioneerpublisher.com/jrssh
Volume 3 Number 1 January 2024

Facial Recognition Technology: College Students' Perspectives in China

Yi Wu[1]

[1] UC Berkeley, CA, US
Correspondence: Yi Wu, UC Berkeley, CA, US.

doi:10.56397/JRSSH.2024.01.07

Abstract

This study explores the perspectives of college students aged 18-25 in China regarding Facial Recognition Technology (FRT). Amidst an era of rapid technological advancements and privacy concerns, this paper examines the nuanced views of young adults on the deployment and implications of FRT. Utilizing a combination of surveys, focus groups, and interviews, the research delves into students' awareness, acceptance, and apprehension towards FRT. It highlights a complex interplay of recognizing FRT's benefits in security and convenience against significant privacy concerns and potential misuse. The findings indicate a cautiously optimistic attitude towards FRT with a strong call for balanced development, robust legal frameworks, and ethical considerations in technology deployment. This paper contributes to the broader discourse on technology, privacy, and youth perceptions, offering insights for policymakers, technology developers, and educational institutions.

Keywords: Facial Recognition Technology (FRT), privacy concerns, technological acceptance, college students' perspectives, China, surveillance, ethical considerations, policy and regulation

1. Introduction

Human rights and privacy are both sensitive terms in China. According to Mozur, Fu, and Chien (2022), in constructing one of the world's most sophisticated surveillance apparatuses, the Chinese police force has strategically installed millions of cameras at key points like street corners and building entryways, integrating advanced facial recognition software specifically programmed to identify local citizens, all while employing specialized software that meticulously processes and analyzes the extensive data and imagery gathered from these myriad sources. Some strongly believe that three consecutive years of zero-clearance policy has given the Chinese government a powerful excuse to access the data of 1.5 billion people (Chin et al., 2022): facial information for facial recognition, personal identity (attached to ID cards), cellphone numbers, travel and network information, and even financial information. Chinese citizens are living and working under pervasive government surveillance (Roth & Wang, 2019; Wang, 2021).

The exciting news in August 2023 is that China released draft rules, half a step ahead of America (Costigan, 2023, paragraph 2), to curb the use of Facial Recognition Technology (FRT), an important step to limit the expansion of FRT's misuse and afford individuals the ability to shield their personal data — notably the uniquely personal data of their facial features —

from commercial entities that could exploit this information for profit. However, some argued that "leaving large carve-outs for national-security-related uses" (Hao & Lin, 2023, paragraph 1), with the concern that it perpetuates state-level surveillance and explicit governmental exemptions that regulations are in effect restraining one of the significant groups looking for citizens' data (Costigan, 2023, paragraph 1&2). What do Chinese people think amid social relationship transformation, especially college students between 18 and 25?

In approaching this research, I consciously refrained from harboring any preconceived notions, such as the presumption that facial recognition technology in China inherently infringes upon citizens' privacy rights. Equally, I was cautious not to assert, undiscriminatingly due to my upbringing and background in China, that facial recognition here does not violate privacy rights. My study is grounded in a fundamental inquiry: What are the attitudes of Chinese university students aged approximately 18 to 25 towards facial recognition technology? This simple yet profound question forms the basis of my research.

The research examines the deployment and perception of facial recognition technology (FRT) in China following the three-year lockdown of COVID-19 and the "new" rules in August 2023, marked by significant changes in public behavior and technology use. It seeks to offer current insights into the nuanced impact of FRT on individual privacy and human rights, as reflected in the varied attitudes of college students aged 18 to 25. All the respondents, including questionnaires, focus groups, and individual interviews, are Chinese citizens living in China now and are identifying with IP addresses. The findings aim to contribute to developing policies and regulations that safeguard individual rights and freedoms in an era increasingly influenced by advanced technological integration.

2. Literature Review

In recent years, China has become one of the most significant users of FRT in the world; it is estimated that 200 million monitoring CCTV cameras of the "Skynet" system have been put to use in mainland China, four times the number of surveillance cameras in the United States (Mozur et al., 2018). The coronavirus pandemic has accelerated the implementation of mass surveillance as it has provided a plausible pretext to do so (Chin et al., 2022). These cameras are used for various purposes, including monitoring public spaces, tracking individuals' movements, and identifying criminal suspects. Despite the potential benefits of FRT, its widespread use in China has raised significant privacy concerns. One major issue is (before Aug 2023) the lack of legal protections for personal data, which can be easily collected, stored, and analyzed using FRT. There is no comprehensive data protection law in China, and existing regulations are often poorly enforced (Geller, 2020). This lack of legal protections has led to widespread abuse of personal data, including the sale of sensitive information on the black market (Creemers, 2022).

According to Asher-Schapiro (2021), one of the most notable examples of human rights violations related to facial recognition technology in China is the government's use of the technology to track and suppress the Uighur Muslim minority in the Xinjiang region. The Chinese government has used facial recognition technology to track Uighur Muslims and monitor their activities, including their religious practices and political views. This has led to the arbitrary detention and imprisonment of millions of Uighur Muslims in "reeducation" camps, where they are subjected to forced labor, indoctrination, and other forms of abuse. In addition to its use in Xinjiang, facial recognition technology is also used to monitor political dissidents and activists in China. For example, in 2019, the Chinese government used facial recognition technology to track and arrest pro-democracy protesters in Hong Kong (Mozur, 2019). Human rights activists argue that using facial recognition technology in this manner violates the right to privacy and freedom of expression.

Moreover, using facial recognition technology in China to monitor compliance with COVID-19 prevention measures has raised concerns about human rights violations. For example, facial recognition technology in some cities monitors whether individuals wear masks in public spaces. Some areas have also implemented facial recognition technology to track the movements of people infected with COVID-19 or suspected of being infected (Kharpal, 2020). Another example of the use is in contact tracing. In some areas, authorities have used facial recognition

technology to identify and track individuals who may have come into contact with someone who has tested positive for COVID-19 (Tan, 2020). While these measures have been implemented to control the spread of COVID-19, they have also raised concerns about privacy and civil liberties. Some critics argue that using facial recognition technology for COVID-19 prevention measures may become permanent and could be used for broader surveillance purposes in the future (France-Presse, 2021).

3. Research Design

The initial phase of this study involved a comprehensive survey, meticulously crafted with 15 questions that employed multiple-choice and single-choice formats. This survey was administered to a diverse sample of 101 college students from 15 provinces, ensuring a broad representation of perspectives. The questionnaire was designed to explore various dimensions of FRT, encompassing societal applications, levels of awareness regarding accuracy, impacts on privacy, perceptions of security, willingness to share facial data, concerns regarding the scope of usage, and perceptions of FRT's role across diverse sectors.

Upon detailed analysis of the initial survey data, a prominent concern regarding privacy emerged within the responses. To delve deeper into this critical issue, a second survey was conducted. This subsequent survey, comprising 14 single-choice questions, aimed to gather comprehensive demographic data, including gender, age, and location, from an expanded pool of respondents across 25 provinces, including municipalities. The age range of participants was between 18 to 25 years old, aligning with the typical university student demographic. This survey further examined the participants' experiences with FRT, their perceptions of privacy and security, and their attitudes towards applying FRT in various contexts. The sample size of 100 college students provided valuable insights into the younger generation's attitudes within a rapidly evolving digital landscape.

A focus group was conducted to augment the understanding from the surveys and enrich the study with qualitative data. This group consisted of ten students, each representing a different province, ensuring a wide range of viewpoints. The focus group session was instrumental in capturing the nuanced opinions and experiences of the participants regarding FRT, particularly in terms of privacy concerns.

Additionally, in-depth interviews were conducted with ten other students individually. These one-on-one interviews allowed for a deeper exploration of personal perspectives and provided a more detailed understanding of individual experiences and attitudes toward FRT.

Combining surveys, focus groups, and individual interviews, this methodological triangulation offered a comprehensive view of the subject matter, ensuring both breadth and depth in the research findings.

4. Results

Survey 1

Applications and Awareness: Balancing Utility with Privacy and Security Concerns

The survey revealed a high awareness of FRT's diverse applications, particularly in identity authentication (95 respondents), payment verification (93), and security (81). However, this acknowledgment was juxtaposed with significant privacy concerns. A majority perceived FRT as having a moderate to substantial impact on personal privacy (92 respondents), reflecting an acute awareness of privacy issues.

The willingness to use FRT varied, with higher acceptance in utilitarian contexts like access control systems (82) and mobile unlocking (76) but lower in more personal domains like social media (22). This suggests a nuanced understanding among students: they recognize FRT's benefits in enhancing security and convenience while remaining cautious about its intrusion into personal spaces.

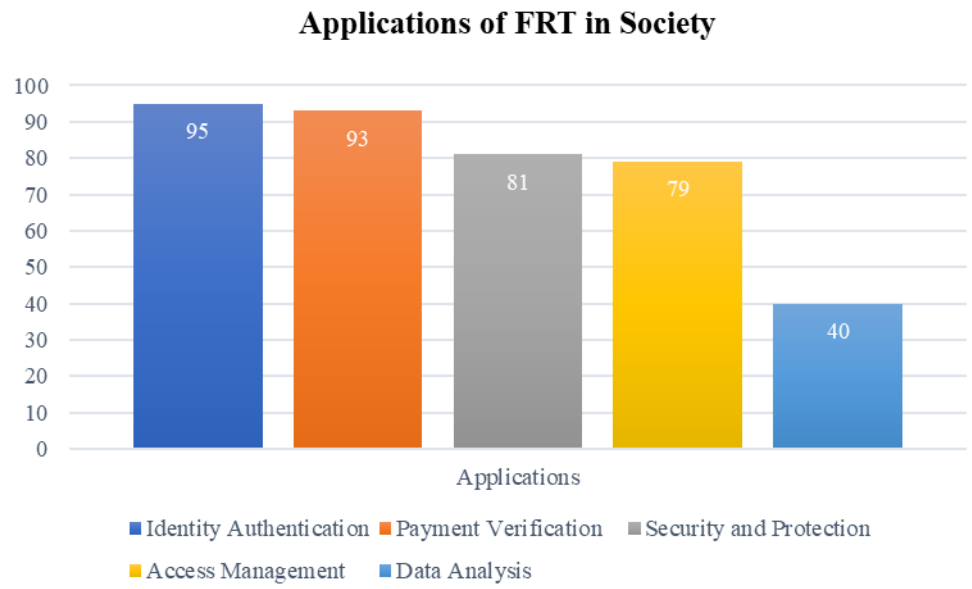

Figure 1. Applications of Facial Recognition Technology in Society

95 out of 101 respondents identified "Identity Authentication," and 93 acknowledged "Payment Verification" as primary use, indicating a high awareness and acceptance of FRT in daily transactions and security measures. Additionally, 81 respondents pointed out its role in "Security and Protection", suggesting a widespread belief in its effectiveness in enhancing safety. Besides, 79 chose "Access Management," 40 chose "Data Analysis," and "Others" got 0.

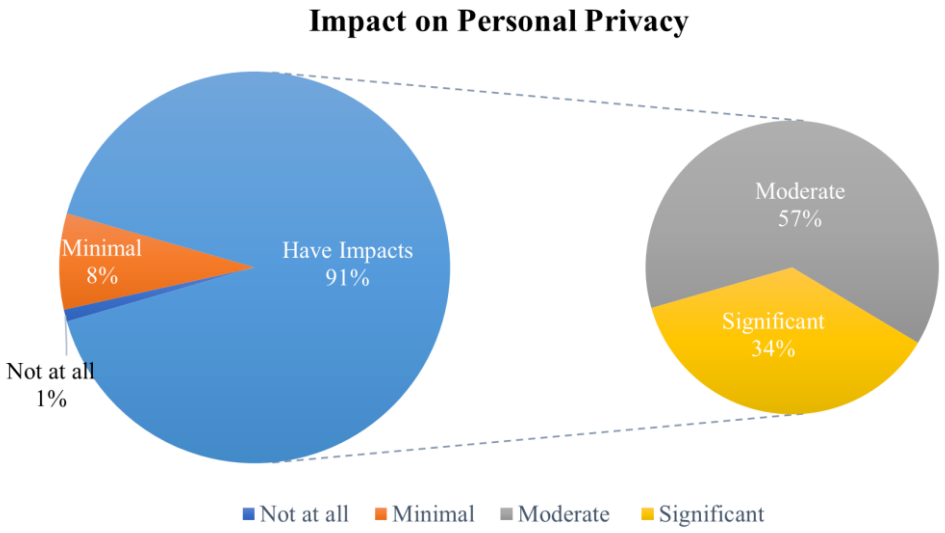

Figure 2. Perceived Impact of Facial Recognition Technology on Personal Privacy

Privacy concerns were evident, in 101 respondents, with 34 believing FRT has a "Significant Impact" on personal privacy and 58 seeing a "Moderate Impact." This indicates a prevalent concern among students about how FRT could infringe on individual privacy.

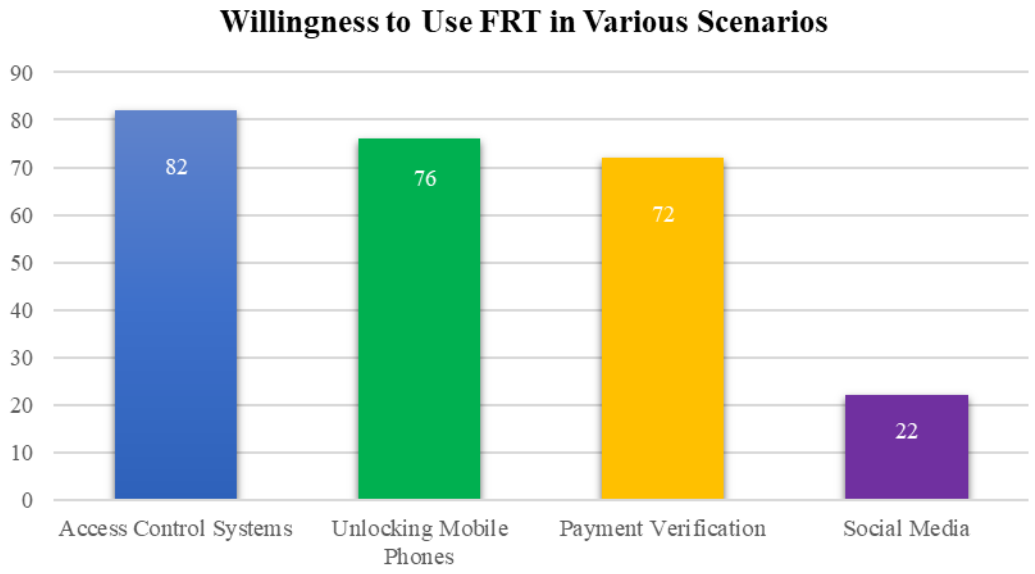

Figure 3. Willingness to Use Facial Recognition Technology in Various Scenarios

The desire to use FRT varied across different scenarios. Of 101 respondents, most (82) were willing to use FRT for "Access Control Systems" and 76 for both "Unlocking Mobile Phones" and "Payment Verification". However, only 22 respondents were comfortable with its use in "Social Media," highlighting potential reservations in more personal or social contexts.

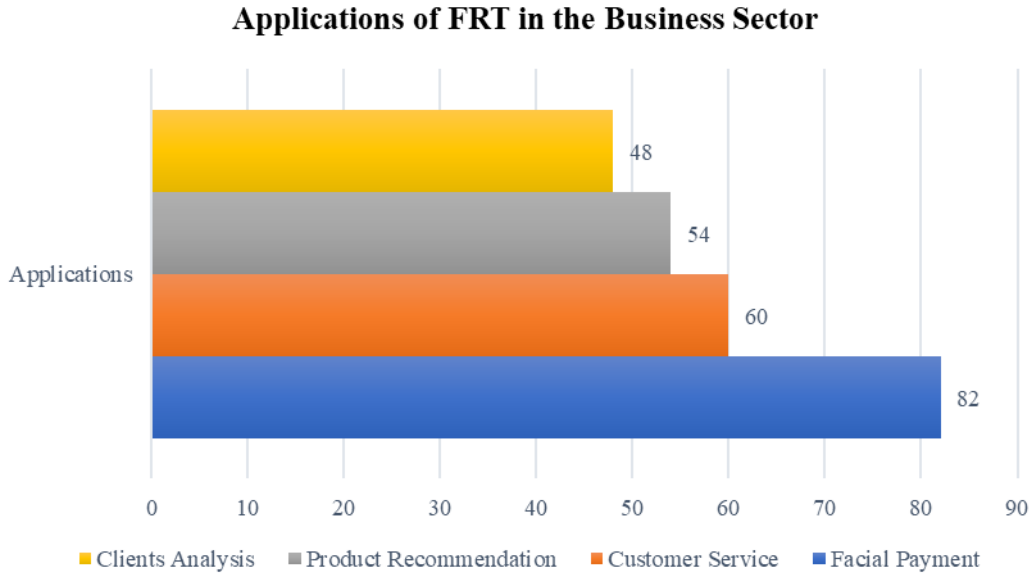

Figure 4. Applications of Facial Recognition Technology in the Business Sector

The most recognized application was "Facial Payment" (82 respondents), followed by "Customer Service" (60 respondents), indicating a belief in FRT's potential to streamline commercial interactions, followed by "Product Recommendation" (54), Clients Analysis (48) and others (1).

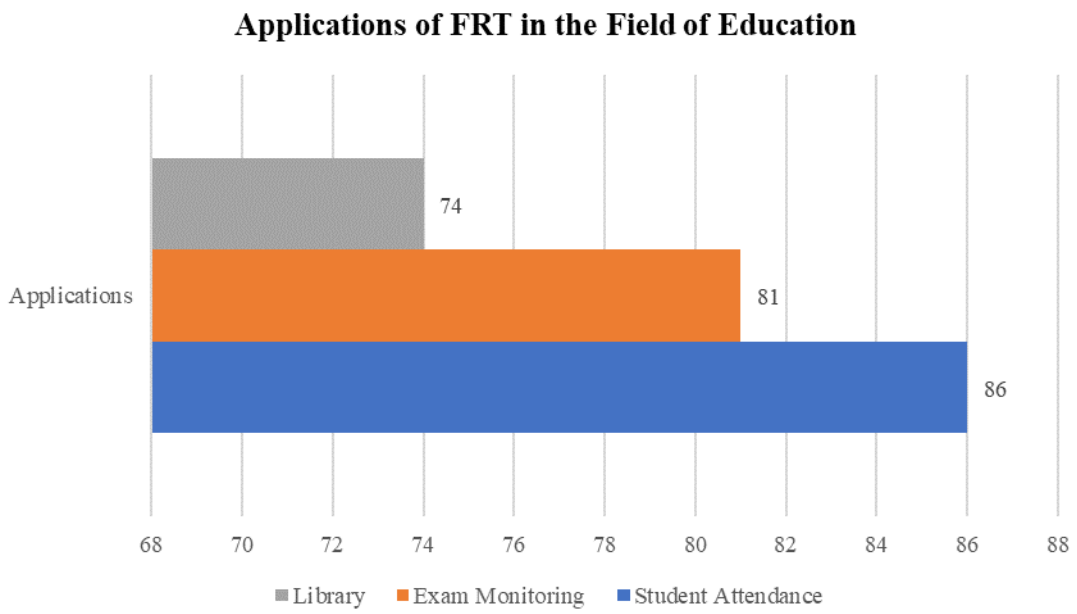

Figure 5. Applications of Facial Recognition Technology in the Field of Education

The majority saw significant applications of FRT in education, with 86 respondents identifying "Student Attendance" and 81 for "Exam Monitoring", suggesting an acceptance of FRT as a tool for enhancing administrative efficiency in educational settings.

Security Perceptions and Personal Data Sharing

Students exhibited mixed feelings about FRT's security. While a considerable number deemed it at least moderately secure (96 respondents), a notable fraction still expressed security concerns. This ambivalence extends to their willingness to share personal facial data, with a majority willing (73) yet a significant minority hesitant (28), indicating a conditional trust in FRT's security mechanisms.

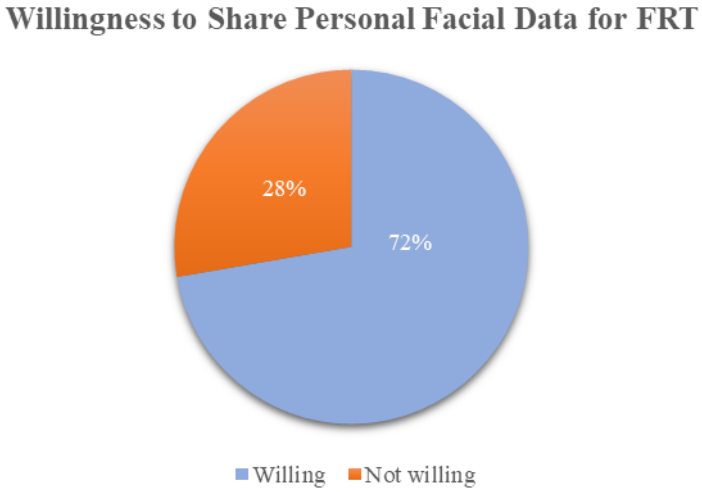

Figure 6. Willingness to Share Personal Facial Data for Facial Recognition Technology

A substantial number of respondents (73) were willing to share their facial data for FRT, indicating a level of trust or acceptance of the technology in exchange for its perceived benefits.

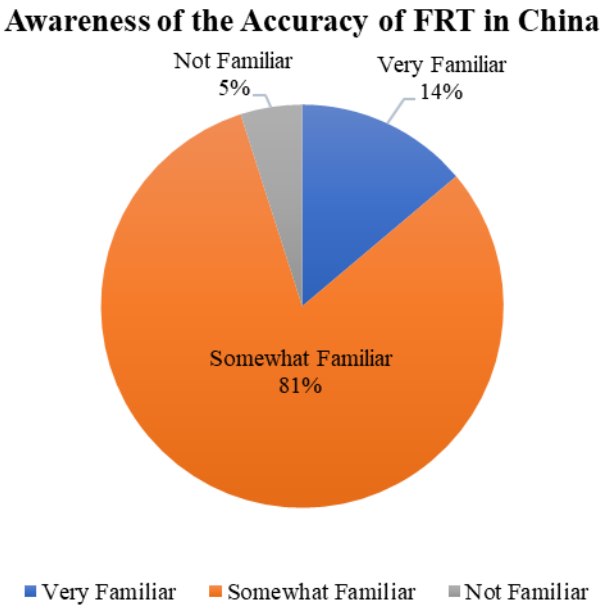

Figure 7. Awareness of the Accuracy of Facial Recognition Technology

Regarding the accuracy of FRT, the majority (82 respondents) indicated they were "Somewhat Familiar" with it, while only 14 claimed to be "Very Familiar." This suggests a general awareness of the technology's capabilities, although in-depth knowledge may be limited among the student population.

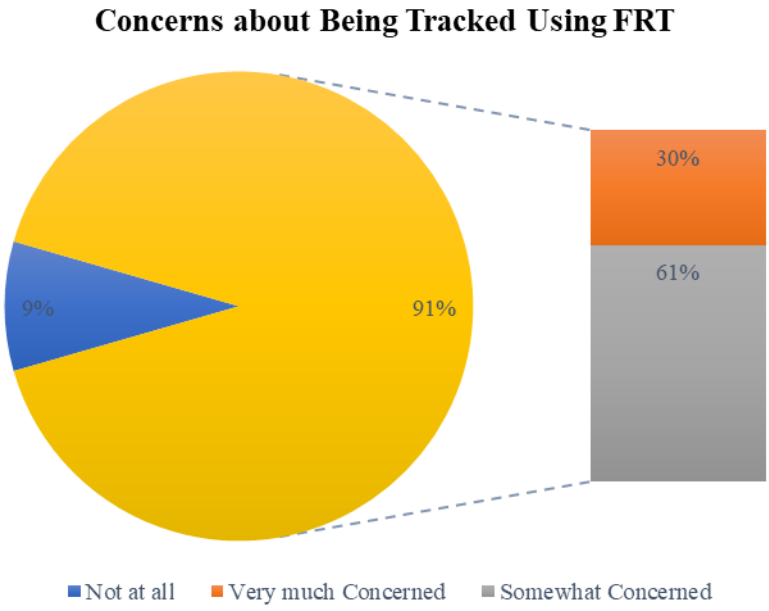

Figure 8. Concerns About Being Tracked Using Facial Recognition Technology

Privacy again emerged as a significant concern, with 30 respondents being "Very Concerned" and 62 "Somewhat Concerned" about being tracked using FRT, highlighting apprehensions about surveillance and personal freedom.

These mixed feelings among students highlight the importance of addressing security and privacy concerns in the further development and deployment of FRT. It underscores the need for robust security measures, transparent data practices, and clear regulations to ensure the ethical use of facial recognition technology.

Developers and policymakers must engage with these concerns to build trust among users and ensure that FRT deployment is responsible and respectful of individual privacy.

Concerns About Overreach and Future Outlook

Concerns about FRT's scope of use were predominantly centered around privacy breaches (74 respondents), indicating apprehension about the technology's potential overreach and misuse. Despite these concerns, the future outlook of FRT was generally positive, with most students expressing optimism (96 respondents), suggesting a belief that the benefits of FRT can be harnessed responsibly in the future.

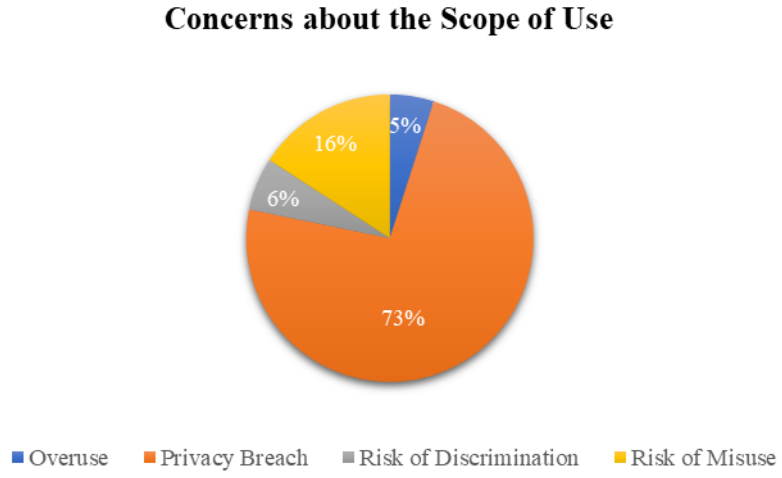

Figure 9. Concerns About the Scope of Use of Facial Recognition Technology

The privacy breach was the most prominent concern, with 74 respondents highlighting it. This underscores the importance students place on privacy in the context of FRT's expanding scope.

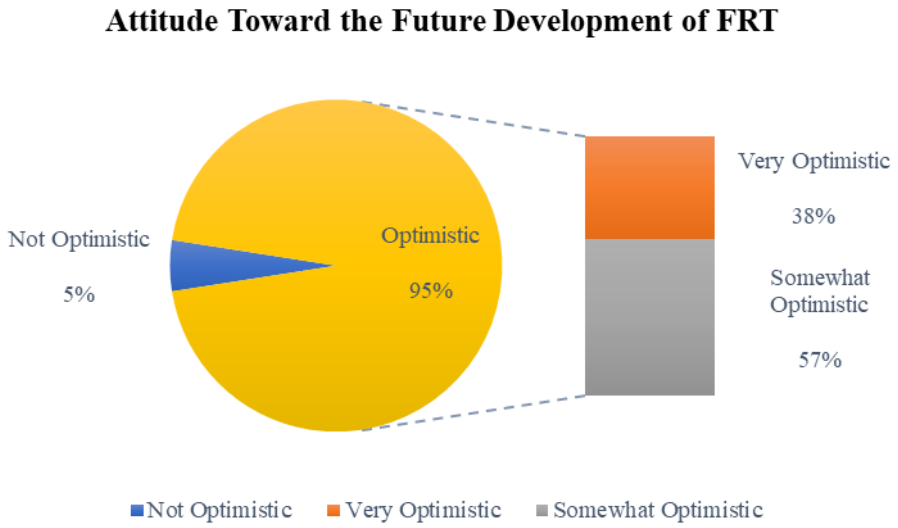

Figure 10. Attitude Towards the Future Development of Facial Recognition Technology

The future of FRT was viewed positively, with 38 respondents being "Very Optimistic" and 58 "Somewhat Optimistic," indicating a general optimism about the technology's development and its role in future societal advancements.

The split opinion on FRT's appropriateness in public spaces (61 appropriate vs. 40 inappropriate) underscores the ongoing debate between public safety and individual privacy, reflecting broader societal discussions.

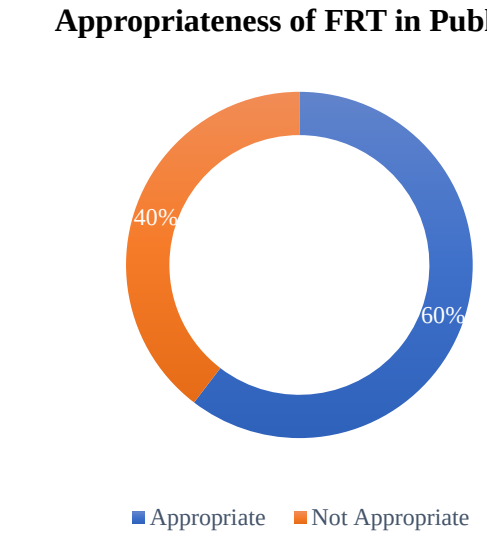

Figure 11. Appropriateness of Facial Recognition Technology in Public Spaces

The opinions were divided on the appropriateness of FRT in public spaces: 61 respondents found it "Appropriate," while 40 considered it "Inappropriate." This split reflects the ongoing debate about balancing public safety and individual privacy rights.

Sector-Specific Applications and Understanding of Technology

The survey highlighted a broad recognition of FRT's applications across various sectors, such as education (notably in student attendance and exam monitoring), business (with a focus on facial payment), and healthcare (patient identity verification). This broad acknowledgment underlines the technology's perceived versatility.

However, an almost even split in understanding FRT's working principles (50 understanding vs. 51 not understanding) suggests that while students know its applications, a deeper understanding of the technology may be lacking.

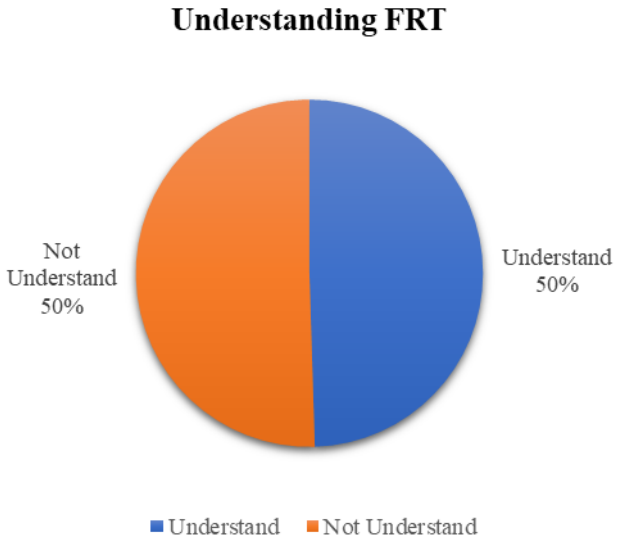

Figure 12. Understanding of the Working Principles of Facial Recognition Technology

The survey showed an almost even split in understanding the workings of FRT, with 50

respondents indicating "Understanding" and 51 "Not Understanding." This suggests that while FRT is widely used, the general student population may not understand its technical aspects well.

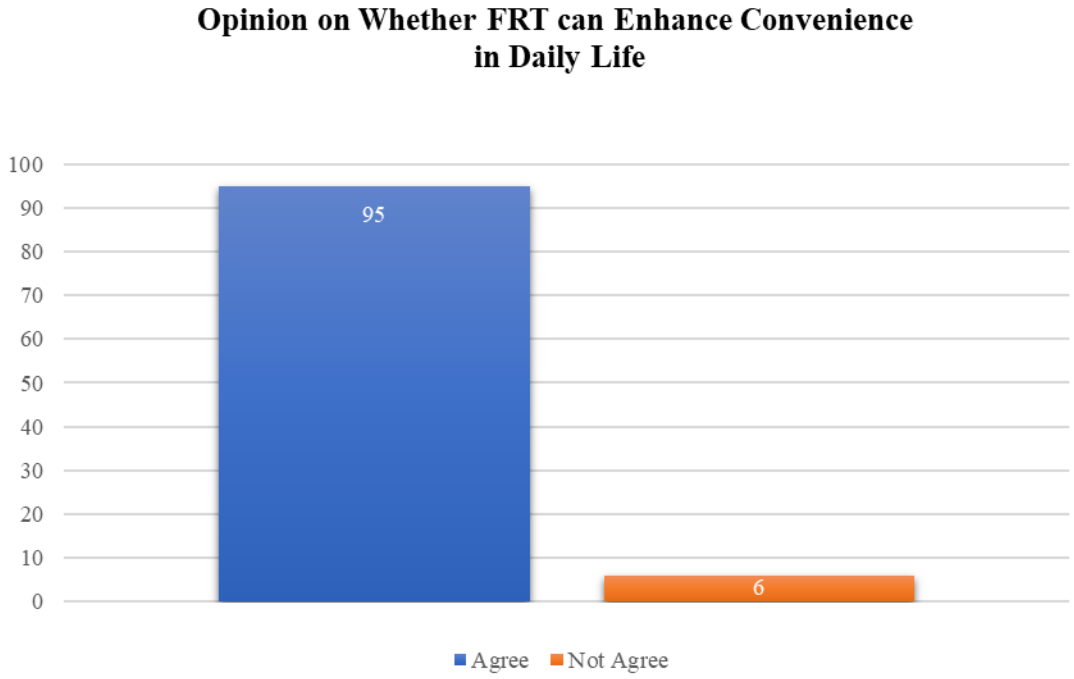

Figure 13. Opinion on Whether Facial Recognition Technology Can Enhance Convenience in Daily Life

Of 101 students, a vast majority (95 respondents) believed that FRT can enhance convenience in daily life, reflecting a solid perception of its practical benefits.

Survey 2

Privacy Concerns Versus Contextual Acceptance

Students' attitudes towards FRT were marked by a complex interplay between privacy concerns and acceptance based on context. While 32 respondents felt FRT did not infringe on privacy, a nearly equal number (38) expressed the need to confirm its safety, and 26 voiced concerns over potential privacy breaches. This indicates a prevailing ambivalence towards FRT's impact on personal privacy.

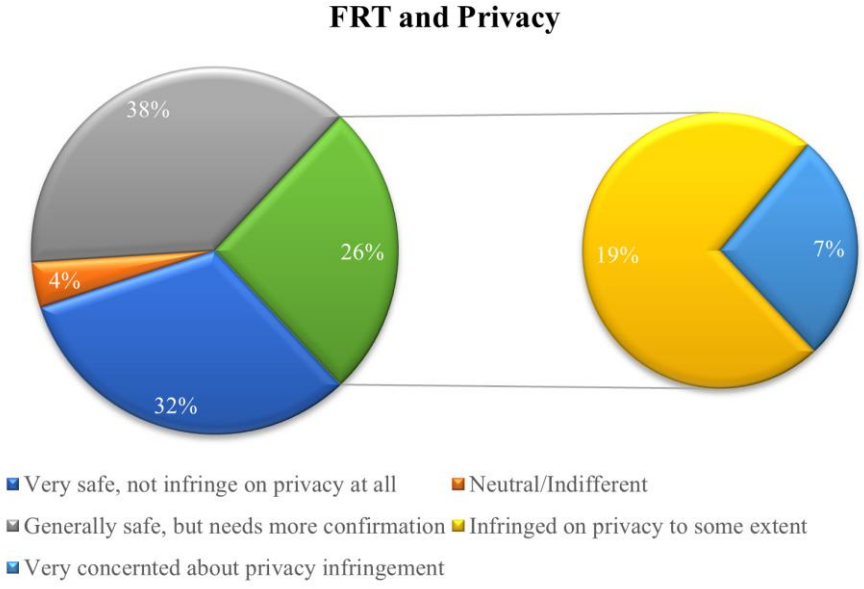

Figure 14. Facial Recognition and Privacy Rights

32 respondents felt it was very safe and did not infringe on privacy, 38 believed it was generally safe but required confirmation, 19 thought it infringed on privacy to some extent, 7 were very concerned about privacy infringement, and 4 held a neutral stance.

The acceptance of FRT varied significantly across different settings, suggesting that context plays a crucial role in shaping perceptions. In state-controlled environments and educational institutions, a higher degree of acceptance was noted (32 and 30 respondents fully accepting, respectively), contingent on clear signage or legal compliance. Conversely, residential areas witnessed more divided opinions, emphasizing the sensitivity of FRT in personal spaces.

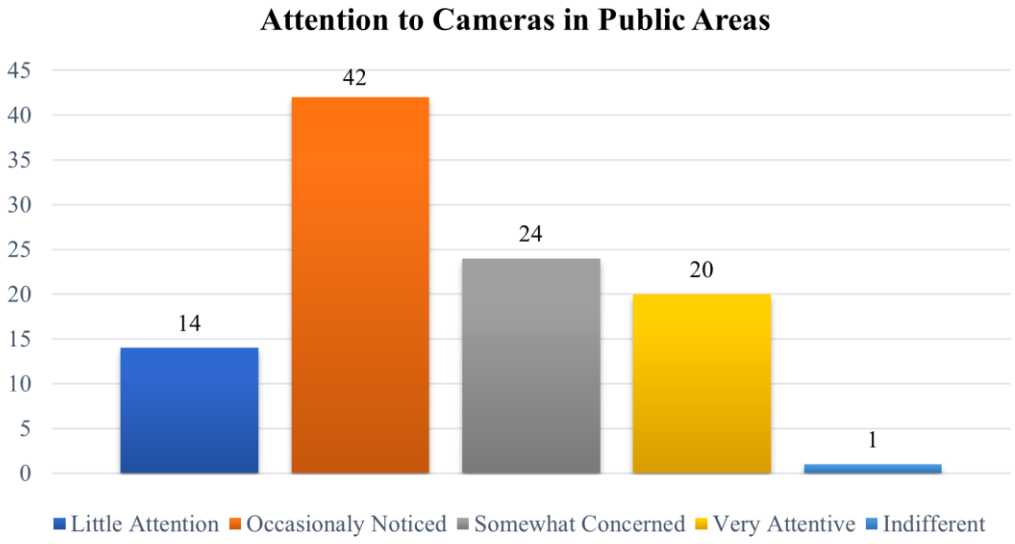

Figure 15. Attention to Cameras in Public Areas

Of 100 students, 14 respondents paid little attention, 42 occasionally noticed, 23 were somewhat concerned, 20 were very attentive, and 1 was indifferent.

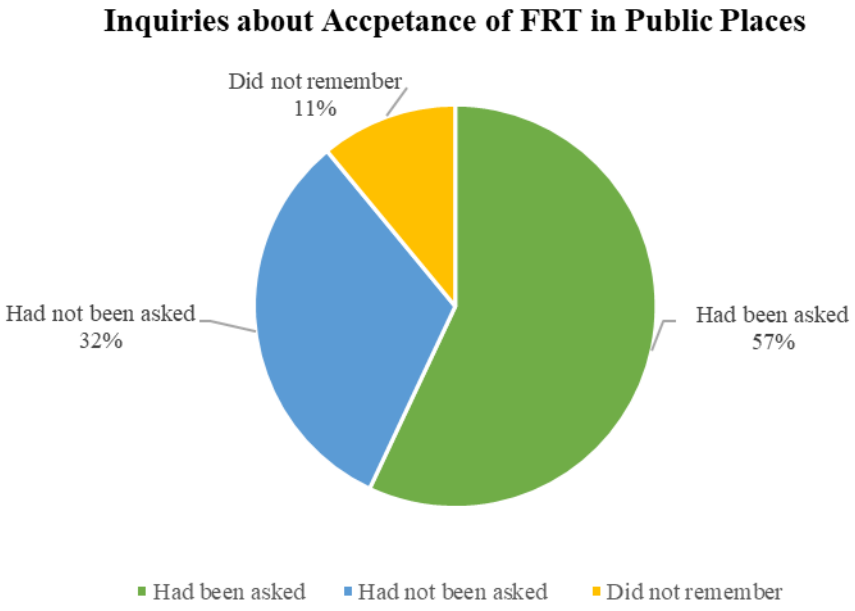

Figure 16. Inquiries About Acceptance of Facial Recognition in Public Places

Of 100 students, 57 had been asked, 32 had not, and 11 did not remember.

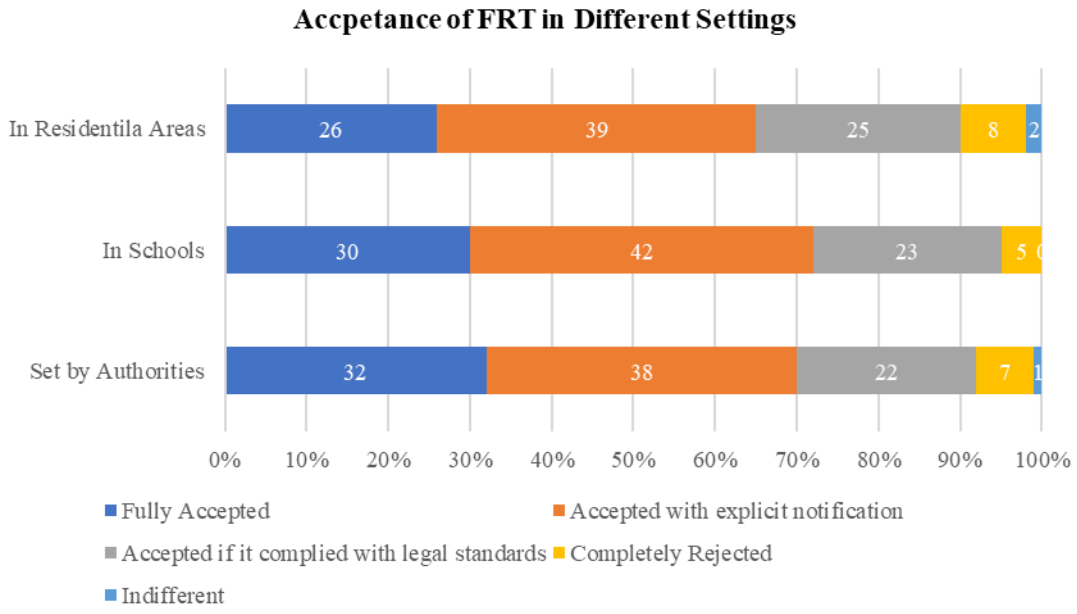

Figure 17. The single-choice survey answers on the acceptance of facial recognition

Set by Authorities: 32 were entirely accepted, 7 were fully rejected, 38 were accepted with clear signage, 22 were accepted if compliant with legal standards, and 1 was indifferent. In Schools: 30 were entirely accepted, 5 were fully rejected, 42 were accepted with clear signage, 23 were accepted if compliant with legal standards, and none were indifferent. In Residential Areas, 26 were entirely accepted, 8 were fully rejected, 39 were accepted with clear signage, 25 were accepted if compliant with legal standards, and 2 were indifferent as long as it did not affect their lives.

The survey also revealed a cautious openness to integrating FRT with personal identification, such as bank cards (36 respondents found it convenient) and ID cards (39 respondents viewed it as an inevitable trend). However, concerns about privacy and security were evident, reflecting a conditional acceptance of FRT in these areas.

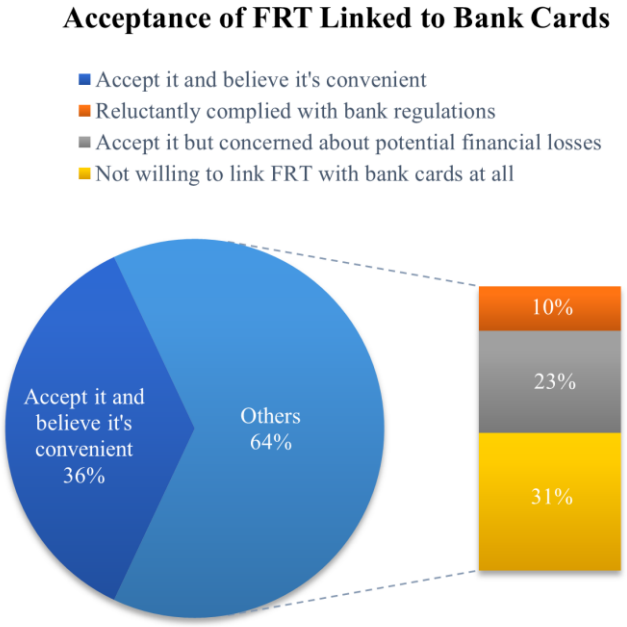

Figure 18. Acceptance of Facial Recognition Linked to Bank Cards

Of 100 respondents, 36 found it convenient, 10 reluctantly complied with bank regulations, 31 did not want to link facial recognition with bank cards, and 23 accepted it but were concerned about potential financial losses.

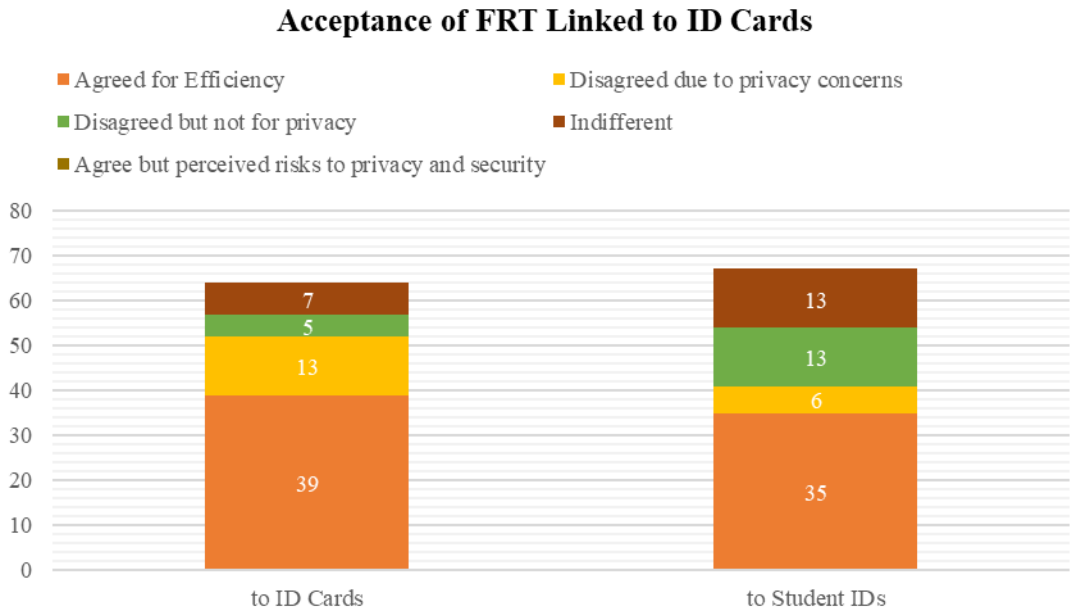

Figure 19. Acceptance of Facial Recognition Linked to ID Cards and Student IDs

For FRT linked to ID Cards, of 100 students, 39 saw it as an inevitable trend, 13 objected due to privacy concerns, 7 were indifferent, 36 accepted but perceived risks to privacy and security, and 5 objected not due to privacy but disliked the linkage; For FRT linked to Student IDs, 35 agreed for efficiency, 33 accepted but had privacy concerns, 13 were indifferent, 6 objected due to privacy invasion, and 13 objected not for privacy reasons but disliked the linkage.

Overall Attitude: Cautious Optimism with Underlying Reservations

When asked to rate their support for FRT, most students leaned towards moderate to high support (3 to 5 on the scale), with 35 respondents giving a neutral rating of 3 and 54 combined, giving higher ratings of 4 and 5. This suggests a general inclination towards accepting FRT, albeit with some reservations. However, lower scores (1 and 2 by 11 respondents) underscore a significant minority with apprehensions or opposition towards the widespread use of FRT. This group's concerns likely stem from issues related to privacy, data security, and potential misuse of the technology. Their apprehension could be influenced by heightened awareness of digital privacy rights and skepticism about how authorities and corporations handle personal data.

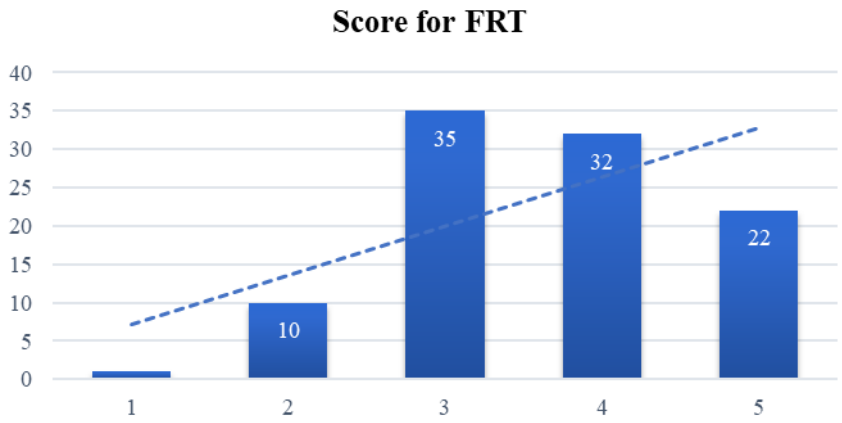

Figure 20. Support for Widespread Use of Facial Recognition in Society

When asked to rate their support for the widespread use of facial recognition on a scale from 1 (least supportive) to 5 (most supportive), the responses were: 1 point - 1 student; 2 points - 10 students; 3 points - 35 students; 4 points - 32 students; 5 points - 22 students.

The results reflect optimism and reservations and underscore the need for a balanced approach to the further development and implementation of FRT. Policymakers and technology developers should consider these diverse viewpoints, ensuring that FRT is used to maximize its benefits while safeguarding individual privacy and rights.

The mixed responses also indicate the necessity for ongoing dialogue between technology providers, policymakers, and the public. Engaging with the concerns of those skeptical or opposed to FRT is essential for building trust and developing more responsible and acceptable forms of technology.

Focus Group & Interviews

The following perspectives, garnered from interviews and the focus group, reveal the FRT's complexities and controversies. While FRT is lauded for enhancing efficiency and security in various applications, from securing personal devices to bolstering public safety, its widespread integration into everyday life raises significant privacy and ethical concerns. Students in these discussions offer diverse viewpoints, ranging from strong support for the technology's convenience and safety benefits to apprehensive skepticism about its potential for privacy infringement and misuse. This exploration seeks to navigate the nuanced debate on FRT, balancing the enthusiasm for technological innovation with the imperative to protect individual privacy and uphold societal values.

Consciousness of Surveillance Camera

Observations and Motivations. A common thread among the responses is a blend of curiosity and security consciousness. Several students noted that their observation of cameras stemmed from a desire to understand the extent and purpose of surveillance. This curiosity is often aligned with a safety concern, where cameras are viewed as tools that record criminal activities and assist in public safety. For some, cameras serve as a deterrent to crime and a means to ensure personal and communal safety. On the other hand, some students expressed a general indifference towards surveillance cameras, viewing them as standard fixtures in the modern landscape. This group trusts the intention behind camera installations, considering them essential for security and monitoring purposes. A lack of detailed attentiveness to their surroundings was also cited for not actively observing these cameras.

A few respondents highlighted their natural inclination towards technological gadgets, with surveillance cameras capturing their interest due to their prevalence and significance in modern society. These individuals are not just passive observers but are keen on understanding the technical aspects and implications of surveillance, considering the balance between security and privacy.

Privacy Concerns and Compliance. Privacy emerged as a significant concern in the discussions. While some students consider cameras necessary for security, others are wary

of their potential to intrude on personal privacy. This dichotomy reflects a broader societal debate on the trade-off between security enhancements and the right to privacy. Interestingly, some individuals actively avoid cameras, driven by discomfort at the thought of being constantly monitored and recorded.

Security and Community Well-being. The role of surveillance cameras in fostering a sense of security within communities was a recurring theme. Respondents who live in residential areas with surveillance cameras often feel safer, citing the cameras' potential to deter crime. This sense of security extends to public spaces like train stations and libraries, where cameras are perceived as a means to effectively manage and monitor people and property.

In summary, the responses highlight various attitudes towards surveillance cameras. While curiosity, safety concerns, and technological interest drive some individuals to observe these devices actively, others exhibit indifference or privacy concerns. The overarching consensus is that surveillance cameras have become an integral part of the modern landscape, critical in ensuring public safety and security. However, this comes with the need for a balanced approach that respects individual privacy rights and addresses the potential ethical implications of ubiquitous surveillance.

Attitudes Towards FRT and Privacy

Diverse Perspectives on Privacy and Security. Some respondents do not view FRT as a violation of privacy. They argue that the technology enhances security and helps prevent crime, especially in public spaces. These individuals highlight FRT's efficiency and convenience in daily tasks, such as making payments or accessing accounts. They assert that as long as the technology adheres to legal frameworks, respects privacy policies, and is used with explicit consent, it does not infringe on privacy rights.

Conversely, other participants expressed concerns about privacy infringements due to facial recognition systems' extensive collection and use of personal data. They worry about potentially using data for commercial purposes or other exploitative means. This group is particularly apprehensive about unwarranted surveillance and tracking, leading to an unreasonable invasion of personal freedom and autonomy. They also highlight the risks of misapplication or abuse of the technology, which could result in unfair discrimination or false accusations, ultimately harming an individual's reputation and rights.

Balanced Viewpoints and Conditional Acceptance. Some students adopt a more balanced perspective, acknowledging the advantages and risks of FRT. They note that while the technology poses security and privacy risks, such as data leaks or hacking, it also has beneficial applications in specific contexts like managing people flow in malls or office buildings. This group emphasizes the importance of explicit consent and the necessity of employing the technology responsibly and ethically.

A recurrent theme among several responses is that the issue with FRT is not inherent but lies in its application and management. They suggest that appropriate technical and regulatory measures can harmonize the relationship between privacy protection and public safety.

Concerns About Data Management and Legal Frameworks. Many participants express unease about how facial recognition data is managed, shared, and protected. They are particularly wary of scenarios where personal information is shared without consent or used for purposes beyond the original intent, like discrimination or harassment. There is a call for robust legal frameworks and strict regulations to safeguard individual privacy rights in the face of growing technological advancements.

In conclusion, the responses reveal a spectrum of attitudes towards facial recognition technology, ranging from acceptance under specific conditions to outright concern for privacy infringement. While some see it as a tool for enhancing security and efficiency, others are cautious about its potential to erode personal privacy and freedom. The overarching sentiment is the need for a balanced approach that respects individual rights while leveraging the benefits of technological advancement. This balance requires thoughtful consideration of ethical implications, robust legal frameworks, and responsible use of technology.

FRT in Various Scenarios

The integration of FRT in daily life, particularly in scenarios like face-scanning payments and pandemic-related verifications, has prompted diverse opinions regarding its security and reliability. The following compiles and

summarizes the viewpoints of various students interviewed or involved in focus groups.

Trust in Technology's Security. Many students express confidence in the security of FRT. They cite its advanced algorithms, extensive data training, and high accuracy in individual differentiation, reducing the chance of misidentification. Significant technology companies' substantial investment and continuous improvements in this domain are also noted, especially in contexts requiring stringent security measures like banks and government institutions. These respondents trust the technology's ability to enhance security in specific application scenarios.

Concerns and Skepticism. Contrastingly, some participants harbor skepticism about the security of facial recognition. They highlight its challenges, such as privacy violations, data breaches, and susceptibility to hacker attacks. Despite its high algorithmic accuracy, factors like similar facial features and makeup can affect its reliability. Additionally, the potential for fraudulent activities and identity theft by malicious actors raises concerns. In public scenarios like transportation and retail, they worry about privacy and ethical issues, foreseeing general dissatisfaction and resistance.

Conditional Acceptance and Risk Awareness. A group of respondents displays conditional acceptance of the technology, acknowledging both its benefits and potential risks. They recognize the continuous technological advancements and improvements, including liveness detection features, which enhance defenses against fraud. While acknowledging the technology's role in public safety and crime prevention, they remain wary of the risks, emphasizing the need for adherence to legal and ethical standards and cautioning against potential misuse or privacy infringements by organizations or businesses.

Recognition of Technology's Dual Nature. Several participants perceive facial recognition as a dual-edged sword, offering convenience and efficiency while posing potential security risks. They point out that while the technology has been widely applied and validated for accuracy, its security is not absolute and is closely linked to data privacy protection. The risks of attack methods like fake face or photo attacks are acknowledged, stressing the importance of security measures to protect against vulnerabilities.

Balancing Security with Privacy. The students collectively suggest balancing the technology's utility with privacy and security concerns. There is an understanding that while facial recognition can streamline processes and enhance public safety, its application must be carefully managed. The call for robust legal frameworks, strict regulations, and continuous monitoring of its safety and privacy implications is a recurring theme among the responses.

In summary, the attitudes toward facial recognition technology security in various scenarios vary, ranging from trust and confidence to caution and skepticism. While its technological advancements and applications reassure some, others are apprehensive about its potential risks and privacy implications. The overarching consensus is the necessity of a balanced approach, ensuring that the benefits of facial recognition technology are harnessed without compromising individual privacy and security.

Willingness to Use Facial Information for FRT

Willingness Anchored in Convenience and Security. Many students desired to utilize facial information for facial recognition, primarily driven by its convenience and enhanced security. They highlight its efficiency in daily tasks, such as streamlined security checks and simplified payment processes. The perception that facial recognition technology could reduce the risks associated with traditional identity theft and fraud further bolsters their confidence and willingness. This group tends to trust technological advancements and their ability to provide safety measures, like liveness detection, to prevent deception and forgery.

Privacy and Security Concerns. Conversely, some participants are reluctant to use facial information in such technologies. Their hesitation stems from concerns about privacy breaches, potential misuse of their data, and the inherent risks associated with the technology, including data breaches, hacking, and system vulnerabilities. The fear of personal data being used for unauthorized purposes or falling into the hands of malicious actors leads to a cautious or negative stance toward providing their facial data for recognition purposes.

Complex Perspectives and Conditional Acceptance. Some individuals exhibit a complex viewpoint, balancing the benefits of facial

recognition with its potential risks. They recognize the conveniences offered in various scenarios, like access control and payment systems, where facial recognition enhances efficiency and security. However, the sensitivity of facial information and the possibility of its misuse or leakage prompt a more reserved attitude. This group advocates for stringent privacy protection measures and robust legal frameworks to safeguard individual data.

Emphasizing the Need for Protective Measures and Regulation. Across the responses, a recurring theme underscores the need for protective solid measures and regulatory oversight when using FRT. While recognizing its benefits, respondents stress the importance of ensuring that personal information is securely handled and that privacy is not compromised. They call for greater transparency from organizations using facial recognition and the need for informed consent from individuals whose data is being used.

In conclusion, the willingness to use facial information for FRT varies among individuals, influenced by their assessment of the technology's benefits against its potential risks. While the convenience and security enhancements entice some, others are apprehensive about privacy violations and data misuse. The consensus points towards a cautious approach, underlining the necessity for improved security measures, legal protections, and ethical considerations in using facial recognition technology.

About the Use of FRT by Authorities and in Public Spaces

Advocacy for Regular Reviews and Legal Compliance. A common suggestion among respondents is the need for regular reviews and updates of facial recognition systems. This includes timely identification and resolution of potential security risks and vulnerabilities. Many emphasize the importance of penalizing actions that violate relevant laws and regulations, upholding the authority of the law. Additionally, establishing a complaint mechanism is advised to address public grievances and suggestions regarding facial recognition technology, ensuring prompt response and resolution.

Legal Framework and Third-Party Oversight. Several participants propose formulating specific laws and regulations to clearly define the conditions, procedures, and responsibilities for using facial recognition technology. This legal foundation is critical in providing a basis for its application. Introducing third-party supervision is also recommended to oversee and manage the technology's use, ensuring its legality and standardization. Before employing facial recognition, obtaining explicit user authorization and adhering to the principle of least privilege is advised, coupled with data encryption and secure storage to protect personal privacy.

Scope and Purpose Limitations. A recurring theme is the need to clearly define the scope and purpose of using facial recognition to prevent misuse and personal information leakage. Strengthening governmental oversight and management of the technology and establishing a comprehensive security management system are suggested. Respecting individual privacy rights and implementing effective protective measures are deemed crucial. Increasing the transparency of FRT and enhancing public education are also highlighted as essential steps to foster trust and understanding.

Addressing Privacy and Security Concerns. The potential impact of facial recognition on personal privacy and information security is a concern shared by many students. Suggestions include enhancing the technology's security to prevent misjudgments or recognition failures and strengthening management and oversight. Establishing comprehensive safety management systems and technical standards is necessary to safeguard personal information and privacy. There is a call for robust legal protections and increased penalties for privacy violations, promoting industry self-regulation and social monitoring.

Comprehensive and Balanced Approach. Overall, the responses call for a complete and balanced approach to implementing FRT by authorities and public spaces. This includes legal, regulatory, educational, and technical measures to ensure the technology's lawful, secure, and practical application. Recognizing facial recognition as a global issue, participants suggest international cooperation, standard-setting, public engagement, and informed consent to safeguard citizens' rights and promote technology's healthy development.

In conclusion, while recognizing the potential benefits of FRT in enhancing security and

efficiency, students strongly advocate for measures to mitigate risks to personal privacy and data security. The suggestions reflect a consensus on the need for a cautious, regulated, and transparent approach to deploying FRT, ensuring its alignment with public interests and legal standards.

About Private Companies Using FRT

The potential use of FRT by private companies such as WeChat, Weibo, game apps, banks, etc., raises important questions about user consent, privacy, and security. The following is a synthesis of various viewpoints expressed by individuals regarding their willingness and suggestions for these companies to use FRT.

General Willingness with Emphasis on Security and Consent. A common sentiment among respondents is a willingness to use facial recognition technology due to its convenience and enhanced account security. They suggest that applications inform users about the purpose, data collection and usage methods, and facial recognition technology's data storage and protection measures. Providing users with the choice to use or not use facial recognition and ensuring the security of collected facial data through proper encryption and safety measures are emphasized.

Others express their willingness to use facial recognition for its convenience in facilitating quick logins without passwords or other verification methods. However, they suggest providing users with a clear option to opt out of facial recognition and establishing effective ways to handle errors and complaints arising from its use. They advocate for strengthening education and awareness about the technology's pros and cons and ensuring that applications comply with all relevant laws and regulations.

Regular Audits and Multiple Verification Options. Participants suggest regular audits of facial recognition systems to ensure accuracy and reliability. They advise offering multiple verification methods, including passwords and SMS verification, for users who distrust or dislike facial recognition. Applications should not repeatedly promote or coerce users into changing their choice if they decide not to use facial recognition. Clear guidelines are also proposed on how and when users' facial data can be deleted.

Reservations and Recommendations for Privacy, Transparency and User Autonomy. While recognizing facial recognition's convenience and security benefits, there are reservations about its implications for personal privacy and data security. The need for clear user information about the technology's purpose, scope, and protective measures is highlighted. Respecting user autonomy is crucial; users should have the right to choose whether to use facial recognition technology and disable it at any time. Another common perspective is ensuring user awareness and consent for facial recognition technology. Applications should explicitly inform users in their agreements about using facial recognition and obtain explicit consent. Strict protection of user personal information and privacy is crucial, along with establishing comprehensive information security management systems.

Legal Compliance and Ethical Considerations. The need for companies to comply with relevant laws and ethical standards is highlighted. Participants call for a clear explanation of the data collection, usage, and limitations to users, along with obtaining explicit consent. Strengthening data security and privacy protection measures, such as data encryption and restricted access, is emphasized. Companies should actively address risks and challenges posed by facial recognition technology, such as data security, privacy protection, and ethical dilemmas.

User Rights Protection Mechanism. Establishing a user rights protection mechanism, including a grievance mechanism, is suggested to address issues and disputes raised by users. Companies should maintain transparency, public disclosure of facial recognition usage, and data protection measures to enhance user trust and corporate reputation. They should respect users' choices, allowing them to decide whether to use FRT and provide appropriate mechanisms for opting out.

In summary, private companies are generally willing to use FRT, but it is contingent on ensuring user security, privacy, and informed consent. The suggestions reflect a demand for transparency, ethical use, and robust data protection measures. Companies are advised to respect user autonomy, comply with legal standards, and provide alternatives to facial recognition, ensuring a balance between technological innovation and user rights and interests protection.

Perspectives on FRT in Schools

Integrating FRT in educational settings has sparked diverse opinions, reflecting a blend of enthusiasm for its potential benefits and concerns over privacy and data security. The viewpoints can be broadly categorized into willingness, reservations, and the need for stringent regulatory frameworks.

Balancing Efficiency with Privacy Concerns. A notable segment of students is willing to adopt FRT in schools, driven primarily by its efficiency and convenience. This technology streamlines various school operations, such as entering academic buildings, attending classes, and dining in cafeterias, thereby saving time and enhancing campus security. However, this enthusiasm is tempered by significant privacy concerns. Participants stress the importance of safeguarding sensitive personal data, suggesting that schools undertake rigorous measures to protect collected facial data from breaches and misuse. This duality reflects a keen awareness of the benefits of technological advancement, coupled with an understanding of the potential risks to individual privacy.

Advocacy for Informed Consent and Alternative Options. Across the responses, there is a strong emphasis on the need for informed consent and respect for individual autonomy. Students advise that schools should transparently communicate the purposes and mechanisms of FRT to students, ensuring they have a comprehensive understanding and the ability to make informed choices. Moreover, providing alternative options for those who opt not to use facial recognition is essential to accommodate diverse preferences and concerns. This approach underscores the importance of balancing technological implementation with ethical considerations and protecting students' rights.

Call for Robust Regulatory Oversight and Data Protection. Another prevailing theme centers on strict regulatory oversight and data protection. Participants recommend regular audits of facial recognition systems for accuracy and reliability, offering various verification methods to cater to all students. The concern for potential misuse or leakage of facial data leads to suggestions for schools to establish stringent data management protocols and security measures. This perspective highlights the critical need for schools to embrace technological innovation, prioritize safeguarding student data, and uphold ethical standards.

In conclusion, the sentiments towards using FRT in schools are multifaceted, blending enthusiasm for its practical benefits with caution over privacy and security implications. The consensus leans towards a cautious, regulated approach, advocating for informed consent, respect for student autonomy, and rigorous data protection. These perspectives underscore the necessity for schools to navigate the fine line between leveraging technological advancements and upholding ethical responsibilities toward their students' rights and privacy.

Advantages of FRT in Everyday Life

The discussion on the role of FRT in various aspects of daily life reveals a spectrum of perceived benefits. Participants shared their insights on the advantages of this technology, ranging from enhanced convenience and security to more innovative applications.

Enhanced Security and Convenience in Transactions and Access Control. A prevalent view is that FRT is a secure verification method, particularly in financial transactions and account logins, mitigating identity theft risk. It ensures swift and accurate identity confirmation in residential and office settings, thus boosting security. Social media platforms leverage this technology for more precise friend recommendations and interest matching, while retail, entertainment, and healthcare sectors utilize it for personalized services. In emergencies like fires or terrorist attacks, facial recognition aids in individuals' rapid identification and location. Moreover, it streamlines shopping processes, enabling automated payments.

In transport hubs such as airports and train stations, FRT facilitates speedy security checks and payments at toll stations. It enhances the security and accuracy of medical records and medication management in the healthcare sector. Integration with smart home systems allows for personalized control and security. In virtual reality, gaming, and film production, facial recognition offers more realistic interactive experiences. Online education platforms use it to accurately assess students' learning status and needs, while community management benefits from its ability to respond to residents' needs quickly.

Accessibility and Environmental Monitoring. In the contemporary era, facial recognition offers numerous advantages. It provides convenient, barrier-free services for individuals with special needs. In environmental conservation, it aids in the rapid identification and tracking of wildlife and pollution. Urban managers gain a more accurate understanding of citizens' needs and challenges through FRT. It bolsters public safety measures in public parks, squares, and museums.

Case Examples: Payment Systems and Phone Security. A highlighted example by students is FRT in payment systems, notably "face-pay" technology. This innovation eliminates the need for cash or cards, simplifying and securing payment. Its uniqueness effectively prevents identity theft and fraud. Another commonly cited example is FRT for unlocking smartphones. This feature allows users to unlock their devices swiftly without needing passwords or other verification methods, enhancing both convenience and security by ensuring that only the phone's owner can access it.

Diverse Applications and Modern Experience. Facial recognition's ability to rapidly and accurately identify individuals without physical credentials enhances convenience and efficiency. For instance, it expedites identity verification in examination settings.

Technology also plays a significant role in surveillance and security, quickly identifying individuals and promptly addressing abnormal situations. In retail and tourism, it facilitates payment verification and speedy access to attractions, avoiding queues. Its application in mobile payments offers a secure and convenient method for transactions, eliminating the need for password entry or card insertion. This heightens transaction security and reduces the risk of password breaches or card theft.

FRT is hailed for more robust authentication than traditional passwords, given each person's unique facial features. It offers a modern experience, evident in applications like virtual reality gaming and unmanned stores, showcasing technological advancement and appeal. In smartphone technology, facial recognition is widely used for unlocking devices, offering greater convenience than traditional passwords or fingerprint recognition. This technology simplifies the unlocking process and reflects the convenience it brings to everyday life.

In summary, FRT is viewed by students positively for its myriad benefits in daily life. It enhances security and convenience in financial transactions, access control, and personal device usage. Its unique applications extend to various sectors, creating a more modern and efficient lifestyle. The responses reflect an appreciation for the technology's ability to simplify and secure everyday activities, indicating its growing integration into various aspects of modern life.

Detrimental Examples of FRT

The discussion surrounding the potentially harmful aspects of FRT in daily life, as heard by participants, reveals concerns primarily related to privacy infringement and data leakage. This summary encapsulates various perspectives and incidents highlighting the negative aspects of this technology.

Privacy Invasion and Unconsented Usage. One Student mentioned instances where merchants used FRT to record customers' shopping behaviors and preferences without their knowledge, leading to feelings of unease and privacy violation. Social media platforms automatically tagging and recommending friends using FRT without user consent infringed on users' privacy rights. In public spaces like parks, squares, or shopping centers, facial recognition used for tracking individual movements sparked public privacy concerns. The use of technology in job recruitment processes led to discrimination and exclusion of certain groups.

Some students shared that FRT was used to monitor and record family members' behaviors and interactions without consent, causing discomfort and privacy invasion. Identifying and tracking individuals with specific diseases without their knowledge or consent violated their privacy rights. The technology was also used to identify crime suspects or terrorists, but misidentification incidents led to innocent people being wrongfully detained or judged.

Political Surveillance and Misuse in Relationships. Some students discussed that there were reports of FRT being used to track and monitor opposition figures or dissidents in political activities, leading to persecution and oppression. In tourism sites or museums, personalized guided services or exhibit recommendations using facial recognition,

without informing visitors or obtaining their consent, violate their privacy. The technology's use in relationships to monitor partners' movements and fidelity strained and sometimes broke marital bonds in film production; automatic tagging and categorizing actors' roles and performances without their knowledge or consent infringed on their privacy rights.

Data Breaches and Lack of Protection. One student raised a notable example involving an "AI + Security" company in Shenzhen, where a facial recognition database leak exposed over 2.5 million individuals' facial data, accessible without restrictions. This incident is a classic case demonstrating the risks of massive personal information leakage due to inadequate database protection in FRT.

Some students were unaware of specific harmful instances related to FRT, possibly due to its limited application and strict adherence to relevant laws, regulations, and privacy policies.

Vulnerability to Deception and Societal Impacts. FRT is susceptible to deception and forgery attacks, such as using synthesized or disguised facial images for identity impersonation. Its performance in complex environments (like low light or with obstructions) may be limited, reducing recognition accuracy. The technology might lead to excessive social surveillance and personal information collection, negatively impacting society.

Nearly all the students mentioned that FRT must adhere to relevant laws and regulations and ensure legal and ethical use to protect individual rights and privacy. It may lead to societal surveillance and excessive personal information collection, negatively affecting society. The technology is also vulnerable to deception and forgery attacks, like using synthesized or disguised facial images for identity impersonation.

Risks of Data Leakage and Unauthorized Use. Facial recognition systems may have security vulnerabilities in data storage and processing, leading to personal information leakage. For instance, one student mentioned that in 2017, a company named "Clearview AI" was exposed for claiming a database of over 3 billion facial images sourced from social media and other public channels, raising concerns about privacy protection and data security.

Another student recalled a shopping center installing a facial recognition system to identify customers' purchasing habits and interests without clear notification or explicit consent. Customers' activities were recorded, and their facial data was used for commercial purposes like personalized advertising and product recommendations, potentially violating their privacy. They were neither informed nor consented to such use.

Despite the widespread application of FRT in recent years, it has sparked controversies over privacy and data security. Students discussed that governments or enterprises might install numerous cameras in public places for facial recognition in some countries and regions, potentially violating citizens' privacy. For example, in 2019, a Chinese AI face-swapping app named "ZAO" stirred social media discussions for allowing users to replace their faces with movie characters, potentially involving unauthorized use of others' portraits.

Ethical Dilemmas and Societal Implications. The deployment of FRT often presents ethical dilemmas, mainly when used in sensitive areas such as law enforcement and public surveillance. There are instances where its implementation has led to societal debates over the balance between security and individual freedoms. Concerns revolve around the potential for mass surveillance and the erosion of anonymity in public spaces, raising questions about the extent to which such technologies should be employed.

Misidentification and Discrimination. A significant concern with FRT is the risk of misidentification, especially in diverse populations. There are documented cases where the technology has shown biases against certain racial or ethnic groups, leading to wrongful identifications and accusations. This misidentification poses risks of unjust treatment and highlights the limitations of current technologies in accurately recognizing diverse facial features.

Impact on Children and Vulnerable Groups. Concerns about using FRT in schools and other environments involving children have been raised. The potential for monitoring and profiling young individuals raises ethical questions about consent and the long-term implications of such surveillance on children's development and privacy rights.

Data Security in a Digital Age. With the increasing digitization of personal information,

data security collected through facial recognition technologies has become a paramount concern. High-profile data breaches involving facial data have underscored the vulnerability of this sensitive information and the need for robust cybersecurity measures to protect individuals' digital identities.

In summary, while FRT offers numerous benefits, its application in everyday life has raised significant concerns, primarily around privacy infringement, data security, ethical use, and potential biases. These concerns necessitate carefully considering the ethical implications, legal frameworks, and societal impacts of deploying facial recognition technologies. Ensuring transparency, securing consent, and implementing robust data protection measures are crucial in addressing these challenges and maintaining public trust in these rapidly evolving technologies.

Perspectives on the Development of FRT

The perspectives on the evolution of FRT span a spectrum from acknowledging its positive impacts to expressing caution due to its potential drawbacks. The following are various viewpoints on this subject.

Positive Impacts and Applications. Students all mentioned that FRT has a beneficial role in enhancing security and protection levels by aiding in crime prevention and criminal apprehension. It enriches user experiences in social media, advertising, and entertainment. In healthcare, it assists in diagnosing and treating specific diseases, improving medical service quality and efficiency. The technology facilitates rapid location and contact of individuals, enhancing social interaction efficiency. In transport and tourism, it offers expedited and convenient passage experiences for travelers.

The development of FRT is perceived to have merits and demerits. It offers more intelligent and convenient interfaces and controls for smart homes and IoT devices. In education and training, it aids in personalized teaching and learning, enhancing educational quality and outcomes. However, concerns include potential invasions of personal privacy and freedom and the need for reasonable regulation and oversight. Its accuracy and reliability require further improvement, as misjudgment and discrimination are risks. The technology could also be misused for illegal purposes, such as identity theft, surveillance, and infringement of others' rights.

Benefits Outweighing Risks. Students view the development of FRT as more advantageous than disadvantageous. In transportation hubs like airports and train stations, it streamlines identity verification, reducing wait times. It enables contactless payments in stores and restaurants, enhancing payment efficiency and security. Intelligent access control systems in homes and offices offer convenience and increased security. In significant events or public places, it assists in quickly locating specific individuals, such as lost children or elderly persons.

Convenience and Security vs. Potential Risks. While FRT brings convenience and security, it poses latent risks and challenges. In security and defense fields, it aids in rapidly identifying suspects, enhancing public safety. Its widespread use in everyday life, such as unlocking phones and access control systems, offers significant convenience. However, the leakage or misuse of this information could severely threaten personal privacy and security.

Rapid Development and Wide Applications. FRT's rapid development and broad application prospects are acknowledged due to its non-contact, non-invasive, and automated nature, significantly improving identity verification and recognition accuracy and efficiency.

Feasibility and Future Development. The future development of FRT is deemed feasible, with room for enhanced accuracy and reliability. With the widespread application of deep learning and other technologies, its accuracy and reliability are expected to improve, aiding its application across various fields. As awareness of privacy protection grows, the technology will increasingly focus on privacy safeguards, such as anonymization and encryption, to ensure data security and privacy. Its integration with IoT, smart homes, and autonomous driving is anticipated to create more intelligent and convenient living experiences.

Promising Outlook and Technological Integration. The development outlook for FRT is considered promising, with continuous technological advancement and expanding application scenarios. Integrating facial recognition with IoT, smart homes, and autonomous driving will create more intelligent and convenient living experiences. For instance,

smart homes could automatically identify family members, enabling personalized home control.

Efficiency and Accuracy in Diverse Fields. Students discussed that the advancement of FRT dramatically enhances the efficiency and accuracy of identity recognition, providing robust support in security, finance, and other areas. Its widespread application in transportation, education, medicine, policing, and e-commerce significantly facilitates daily life. However, challenges such as privacy protection and data security arise. Balancing the benefits with personal privacy and data security challenges becomes crucial to its future development. Technology's progress plays a vital role in societal advancement, but attention to its challenges and issues is necessary to ensure it serves society beneficially.

Cautious and Responsible Approach. A careful and responsible approach is advocated for developing FRT. Ensuring lawful, transparent, and accountable usage, alongside necessary measures to protect personal privacy and data security, is emphasized. Strengthening research and regulation to align the technology's development with ethical and legal requirements is vital for societal benefit and value. The development of facial recognition technology is a complex issue, necessitating a comprehensive perspective. It must balance its convenience with privacy protection and ensure lawful, transparent, and responsible use.

Enhancing Technological Standards and Ethical Considerations. The advancement of FRT necessitates improving technological standards, including enhancing its accuracy in various environmental conditions and reducing susceptibility to deceptive tactics. Ethical considerations are crucial, particularly societal surveillance and personal data collection. These advancements should focus on minimizing potential negative societal impacts.

Importance of Legal and Ethical Compliance. The development of FRT requires strict adherence to legal and ethical standards. Ensuring the technology's deployment is lawful and ethical is crucial to safeguarding individual rights and privacy. This approach will involve balancing technological innovation with ethical considerations, ensuring facial recognition aligns with societal norms and values.

Interdisciplinary Integration and Innovation. The potential of facial recognition technology lies in its multidisciplinary integration and innovation. Its convergence with other emerging technologies, such as IoT, artificial intelligence, and big data, opens possibilities for creating more sophisticated, efficient, and user-friendly systems. This cross-disciplinary approach can lead to breakthroughs in various sectors, including healthcare, security, and consumer services.

Addressing Privacy and Security Challenges. An integral aspect of FRT's development is addressing privacy and security challenges. Protecting personal data and preventing unauthorized access or misuse is paramount. This involves implementing robust cybersecurity measures and maintaining transparency in data handling and user consent processes.

In conclusion, the development of FRT is viewed as a balance between its potential benefits and the need for careful consideration of privacy, security, and ethical implications. While it offers significant advancements in various fields, responsible and regulated use, technological improvements, and interdisciplinary innovation are essential to harness its full potential while safeguarding individual rights and societal values.

5. Discussion

The primary focus of this research was to explore and understand the attitudes of college students aged 18 to 25 in China towards FRT. This exploration was centered on assessing the societal impact of FRT and delving into the privacy concerns associated with its use. Through extensive surveys, interviews, and focus group discussions, the study aimed to capture diverse perspectives, highlighting how students perceive, interact with, and conceptualize the implications of FRT in their daily lives. This approach provided a multifaceted understanding of technology's role in modern society, particularly in the context of young adults who are often the most affected by and engaged with digital innovations. The following discussion aims to unpack these findings, situating them within the broader context of technology's evolving role in society and its intersection with individual rights and ethical considerations.

The results from two surveys on college students' perspectives in China regarding FRT highlight a complex and nuanced view of this

emerging technology. The first survey revealed high awareness of FRT's various applications, particularly in identity authentication and payment verification, underscoring its perceived benefits in enhancing security and convenience. However, this awareness was accompanied by significant privacy concerns, with a notable number of students apprehensive about FRT's impact on personal privacy. The willingness to use FRT varied depending on the context, indicating a preference for its use in functional scenarios like access control while exhibiting caution in more personal domains. Concerns about FRT's security and the potential for privacy breaches and overreach were prevalent, despite a generally optimistic outlook about its future applications.

The second survey further emphasized the conditional acceptance of FRT based on context, with higher approval in state-controlled and educational settings contingent upon regulatory compliance and clear signage. In contrast, opinions were divided regarding its use in residential areas, highlighting the sensitivity of FRT in personal spaces. Students were cautious about integrating FRT with personal identification, tempered by privacy and security concerns. The overall attitude leaned towards careful optimism, with moderate to high support for FRT balanced by significant reservations due to privacy, data security, and potential misuse concerns. These findings underscore the need for a balanced approach in developing and applying FRT, ensuring maximized benefits while safeguarding individual privacy and rights.

The interviews and focus group discussions with college students in China reveal a multi-faceted perspective on FRT. Participants displayed a high level of awareness about FRT's applications in various sectors, including identity authentication, payment verification, and security. While acknowledging FRT's convenience and efficiency, there was a strong undercurrent of privacy concerns. Students expressed varied willingness to use FRT, showing greater acceptance in functional applications like access control but caution in personal domains such as social media. Concerns about security and data privacy were prominent, with many students wary of potential privacy breaches and misuse of the technology. Overall, the responses indicate a cautious yet optimistic outlook toward FRT, emphasizing the importance of balancing its benefits with privacy and ethical considerations in its development and deployment.

Interpreting the findings from the interviews and focus group discussions with college students in China provides an insightful lens into the broader societal role of FRT. These findings resonate with existing literature and public opinion, reflecting a dynamic interplay between enthusiasm for technological advancement and apprehensions about privacy and ethical implications. The data reveals that while there is a high level of awareness and acceptance of FRT's practical applications, such as in security and identity verification, there is a concurrent and significant concern for personal privacy. This dichotomy aligns with the global debate on technological ethics, particularly the need to balance innovation with individual rights. The caution expressed by students, especially regarding FRT's use in personal domains, mirrors a broader societal trend toward questioning the unchecked proliferation of surveillance technologies. This trend indicates an evolving public consciousness that increasingly values privacy in the digital age.

The implications of these findings are profound. For policymakers, there is a clear message: the need for robust privacy laws and regulations that govern the use of FRT. Such laws should ensure that stringent safeguards against misuse and abuse accompany the deployment of these technologies. There is also an apparent need for transparency in how FRT is used and how data is managed, emphasizing the importance of informed consent and the right to opt-out. For technology developers, these insights underscore the necessity of incorporating ethical considerations into the design and deployment of FRT. This involves not just adhering to legal standards but also engaging in ethical self-regulation and considering the societal impact of these technologies. Developers should also focus on improving the accuracy and reducing biases in FRT systems, addressing one of the major concerns highlighted in the research. Additionally, the findings suggest a crucial role for public awareness campaigns. Such initiatives could educate the general public about the benefits and risks of FRT, fostering a more informed discourse on its use and implications. Educating the public could also demystify the technology, alleviate unfounded fears, and highlight legitimate concerns. This research

highlights the nuanced perceptions of FRT among young adults in China, encapsulating a microcosm of the larger global conversation on technology, privacy, and ethics. These insights are invaluable for technology, policy, and civil society stakeholders, providing a roadmap for navigating the complex landscape of modern technological advancements.

This research on FRT, while comprehensive in many aspects, has limitations. Firstly, the sample size and demographic scope of the interviews and focus groups may limit the generalizability of our findings. Secondly, the nature of qualitative research, while offering in-depth insights, can sometimes lead to subjective interpretations. The data gathered from interviews and focus groups are based on self-reported experiences and perceptions, which can be influenced by individual biases or the participants' current circumstances. This subjectivity might affect the objectivity and reliability of the findings. Furthermore, the rapidly evolving landscape of technology, particularly in FRT, means that the findings might quickly become outdated. Technological advancements and changing legal and ethical standards can alter public perceptions and the applicability of these findings over time. Another limitation arises from the focus of the study itself. The research primarily concentrated on personal attitudes and societal implications of FRT, potentially overlooking other critical aspects such as the technical efficacy, algorithmic biases, and economic impacts of the technology. Finally, the interpretation of findings was constrained by the existing literature and theoretical frameworks available at the time of the study. Emerging theories or future developments in FRT and its societal impacts might provide new insights not considered in this research. Recognizing these limitations is crucial for contextualizing the research findings and guiding future studies. Future research could benefit from a broader, more diverse sample, longitudinal studies to track changing perceptions over time, and an interdisciplinary approach that combines technical, sociological, and ethical analyses of facial recognition technology.

This research, centered on the attitudes of college students aged 18 to 25 in China towards FRT, opens the door to several areas for future investigation. One key area involves a deeper exploration of how perceptions of FRT may differ across various universities and regions within China. This could uncover unique cultural or regional factors influencing students' views. Additionally, longitudinal studies focusing on this demographic could provide valuable insights into how attitudes towards FRT evolve as these individuals transition from academic environments into the workforce. Understanding this transition could reveal shifts in perceptions of privacy, security, and technology reliance. Another promising area for future research lies in examining the impact of educational initiatives on students' understanding and perception of FRT. Investigating whether increased awareness and education about technology influences attitudes could inform future policy-making and educational programs. Furthermore, exploring the relationship between students' academic majors and their perceptions of FRT could offer exciting findings. For instance, do students in technology-related fields have different views than those in the humanities or social sciences?

In conclusion, this study focused on college students' perspectives in China, and it becomes evident that understanding attitudes toward FRT is crucial. This demographic, poised at the cusp of entering varied professional fields, will significantly shape and be shaped by technological advancements in their future careers and personal lives. The study underscores the need for a balanced approach to the deployment and governance of FRT. While recognizing the benefits it offers regarding security and convenience, it is imperative to consider the ethical implications, privacy concerns, and the potential for misuse. This is particularly relevant in the context of a young, digitally native population who will be the architects and beneficiaries of future technological developments. As China continues to emerge as a global leader in technology, the insights from this study highlight the importance of involving young voices in shaping policies and practices around emerging technologies like FRT. Balancing technological innovation with ethical considerations and respect for individual rights will ensure that such technologies are harnessed for the greater good, aligning with societal values and cultural norms.

Acknowledgement

I extend my profound appreciation to the Institute of East Asian Studies at the University of California, Berkeley, for bestowing me the esteemed fellowship for the 2023-2024 academic year. My gratitude extends to UC Berkeley's inherent ethos of democracy and freedom and the School of Public Policy for its rigorous training in objective and unbiased scholarly research. I am particularly indebted to Professor Rucker Johnson, whose guidance in the summer of 2022 profoundly shaped my research approach; he underscored the critical importance of eschewing preconceived notions as they compromise the integrity of academic inquiry. In the realm of research, I bear the responsibility to approach my studies with unswerving neutrality. My sincere thanks go to the former Dean of the School of Information, Professor AnnaLee Saxenian, for her unwavering support of my initial research plan and research proposal, conducted under the mentorship of relentless guidance and corrections during the initial phases of my project were invaluable. I am also profoundly grateful for the astute and insightful contributions of Professor Morgan G. Ames throughout the progression of writing my research proposal. Additionally, my acknowledgments would be incomplete without mentioning Professor Jane Mauldon, the Emerita Professor at the Goldman School of Public Policy at UC Berkeley, whose support and advice over the last eighteen months have been indispensable.

This research, as well as my concurrent studies on attitudes toward FRT among American college students, a comparative analysis of Chinese and American students' viewpoints on FRT, and a historical exploration of divergent perspectives on human rights in China and the Western world could not have been realized without the invaluable support from the Institute of East Asian Studies and all the distinguished professors mentioned above. These ancillary topics will be elaborated in forthcoming separate papers. I am genuinely open to and welcome constructive feedback for any possible oversights in this study. I would appreciate communication for any amendments or clarifications.

References

Agence France-Presse. (2021). Chinese City Using Facial Recognition Tech to Fight Coronavirus. NDTV. July 13, 2021. https://www.ndtv.com/world-news/china-using-facial-recognition-tech-to-fight-coronavirus-2485824 [accessed Jan 17, 2023].

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 Ethics*, 2, 377–387. https://doi.org/10.1007/s43681-021-00077-w [accessed Jan 17, 2023].

Anja Geller. (2020, December). How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective. *GRUR International, 69*(12), 1191-1203. https://doi.org/10.1093/grurint/ikaa136.

Arjun Kharpal. (2020). Coronavirus could be a 'catalyst' for China to boost its mass surveillance machine, experts say. CNBC. February 24, 2020. https://www.cnbc.com/2020/02/25/coronavirus-china-to-boost-mass-surveillance-machine-experts-say.html.

Avi Asher-Schapiro. (2021). Chinese tech patents tools that can detect, track Uighurs. Reuters. January 13, 2021. https://www.reuters.com/article/us-china-tech-uighurs/chinese-tech-patents-tools-that-can-detect-track-uighurs-idUSKBN29I300.

Chin, Josh; Lin, Liza. (2022). Surveillance State: Inside China's Quest to Launch a New Era of Social Control (1st ed.). New York. ISBN 978-1-250-24929-6. OCLC 1315574672.

Conger, K., Fausset, R., & Kovaleski, S. F. (2019). San Francisco bans facial recognition technology. *The New York Times*, pp. 1-3. [accessed Jan 17, 2023].

Costigan, J. (2023, August 09). New Chinese Facial Recognition Regulations Could Shield Citizens from Surveillance Capitalism. Forbes. https://www.forbes.com/sites/johannacostigan/2023/08/09/new-chinese-facial-recognition-regulations-could-shield-citizens-from-surveillance-capitalism/?sh=51c39da13cc2 [accessed Dec 30, 2023].

Hao, K., & Lin, L. (2023, August 8). After Feeding Explosion of Facial Recognition, China Moves to Rein It In. *The Wall Street Journal*.

https://www.wsj.com/articles/china-drafts-rules-for-facial-recognition-use-4953506e [accessed Dec 30, 2023].

Jane Zhang. (2019). In Chongqing, the world's most surveilled city, residents are happy to trade privacy for security. South China Morning Post. Tech / Policy. Oct 4, 2019. [accessed Mar 5, 2023].

Kostka, G., Steinacker, L., Meckel, M. (2021). Between security and convenience: facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Underst. Sci., 30*(6), 671-690. https://doi.org/10.1177/0963662521100155 [accessed Jan 17, 2023].

Mozur, P., Fu, C., & Chien, A. C. (2022, December 2). How China's Police Used Phones and Faces to Track Protesters. *The New York Times*. https://www.nytimes.com/2022/12/02/business/china-protests-surveillance.html [accessed Dec 30, 2023].

Mozur, Paul. (2018-07-08). Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras. *The New York Times*. ISSN 0362-4331. Archived from the original on 2019-10-16. [accessed Mar 5, 2023].

Paul Mozur. (2019). In Hong Kong Protests, Faces Become Weapons. *The New York Times*. July 26, 2019. https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html.

Phoenix New Media Limited. (2018). China Sky Net has built, 200 million cameras millisecond level to find people. Archived from the original on 2018-05-04. https://tech.ifeng.com/a/20180504/44980719_0.shtml [accessed Mar 5, 2023].

Rogier Creemers. (2022). China's emerging data protection framework. *Journal of Cybersecurity, 8*(1), tyac011. https://doi.org/10.1093/cybsec/tyac011.

Roth, K., & Wang, M. (2019, August 16). Data Leviathan: China's Burgeoning Surveillance State. New York Review of Books. https://www.hrw.org/news/2019/08/16/data-leviathan-chinas-burgeoning-surveillance-state [accessed Dec 30, 2023].

Sabbagh, D. (2020). South Wales Police Lose Landmark Facial Recognition Case. The Guardian, August 11. https://www.theguardian.com/technology/2020/aug/11/south-wales-police-lose-landmark-facial-recognition-case [accessed Jan 17, 2023].

Solarova, S., Podroužek, J., Mesarčík, M. et al. (2022). Reconsidering the regulation of facial recognition in public spaces. *AI Ethics*. [accessed Jan 17, 2023]. https://doi.org/10.1007/s43681-022-00194-0.

The new normal: China's excessive coronavirus public monitoring could be here to stay. (2020-03-09). *The Guardian*. [accessed Mar 5, 2023].

Wang, M. (2021). China's techno-authoritarianism has gone global: Washington needs to offer an alternative. *Foreign Affairs*. https://www.hrw.org/news/2021/04/08/chinas-techno-authoritarianism-has-gone-global [accessed Dec 30, 2023].