Austin Lang, Rosen Iliev
Professor Netter
CSCI 1952B Final Project
5 May 2024

Revising Facial Recognition Technology in China

Prototype: https://github.com/alang8/cs1952b-final-project/tree/main

Introduction

In our project, we chose to focus on the use of facial recognition technology in China, a country where this technology is extensively employed across a variety of scenarios, ranging from event entry to the surveillance of everyday citizens. Complemented with this technology, China has established a social credit system which assigns credit scores to individuals, businesses, and government entities based on their trustworthiness and adherence to the law. However, the use of FRT is not limited to legal compliance; it is also being increasingly utilized in workplaces to analyze employee performance and efficiency. Higher performance often translates into higher salaries and bonuses. This dystopian utilization of facial recognition, where people do not have the opportunity to provide consent to their data being processed and sold, motivated us to develop a pseudocode prototype of a consent-based facial recognition for event entry.

Literature Review

In order to draw inspiration for our project, we examined a research paper called “Policy designs for adaptive governance of disruptive technologies: the case of facial recognition technology (FRT) in China”. The authors, Zhizhao Li, Yuqing Guo, Masaru Yarime & Xun Wu, analyze the inadequacies of recent Chinese regulations on big data technologies like facial recognition, proposing alternative policies as more effective strategies for addressing the challenges posed by these technologies. All in all, this paper helped us develop a framework for addressing these technological issues through a political lens.

Methodology

As responsible computer science students, we explored a technology-based approach to supplement what we learned from the paper. This area is a challenge for responsible computing since there are many intricacies when designing facial recognition software such as how data is handled and stored, and how consent is provided. If done wrong, those can impact millions of people’s lives and potentially pose a threat to their personal privacy.

Report Outline

In our report, we will begin by analyzing the difficulties involved in designing a socially responsible facial recognition system, with a focus on the issues of privacy and power. Subsequently, we will introduce our pseudocode prototype and outline the technical decisions we needed to make while developing our artifact. In doing so, we will discuss how our approach aligns with the analytical, ethical frameworks of utilitarianism and Kantian Deontology. Finally, we will explore the trade-offs and downsides of our approach, offering a balanced view of its potential impacts.

Problem Space, Conflicts, and Tensions

Developers of facial recognition technology confront a wide range of difficult moral, legal, and technical issues. Since users frequently are unaware that their data is being collected and exploited, privacy and consent are the most ethically problematic issues. This raises serious concerns regarding users' right to privacy. Aligning with worldwide data protection regulations presents a legal difficulty since they differ greatly by area and may contradict with local customs. From a technical standpoint, it is critical to guarantee that facial recognition algorithms are precise and devoid of prejudices that can unfairly impact particular populations. Furthermore, because this technology has two purposes—improving security and possibly being invasive for surveillance—developers must strike a balance between security requirements and individual liberties, frequently in the face of competing stakeholder demands. However, it is vital to navigate these complex challenges since the results have an impact on individual rights and broader cultural standards in addition to functionality.

Navigating Tensions and Understanding the Problem

We can call on a variety of ideas and concepts covered this semester to help us understand the complexities and conflicts inherent in facial recognition technology. This scenario is specifically related to data protection and personal privacy. We chose to approach the issue from a Kantian perspective, where privacy would be seen as an instrument for fostering individual autonomy. Therefore, people should have the right to have informational self-determination. From this viewpoint, knowing and determining how your information spreads is a material prerequisite for democracy.

The current implementation of facial recognition in China does not meet this privacy standard, as it undermines personal autonomy by collecting and using data without consent, thereby transforming the issue into one of state power. Since surveillance cameras are not privately owned but rather property of the state, such high-level surveillance puts a disproportionate

amount of power in the hands of government officials. Ultimately, collecting people's facial recognition data has the potential to end in a totalitarian state in which individualism is highly neglected.

Our project's design aims to mitigate the state's power over its citizens by allowing them to decide whether their facial recognition data should be used. After talking to an expert, Austin's father, we realized that facial recognition technology is widespread in the country, even being used to replace transportation tickets. One notable example that Austin's relatives faced was the integration of this technology with other systems such as drones and surveillance cameras to monitor COVID-19 isolation within local communities. Notably, one issue that came up from our conversation was that people in China have no way of providing meaningful consent to their information being collected for facial recognition databases. Hence, we needed to design a consent-based facial recognition system.

Our Approach to Navigating Tensions

Protecting people's privacy when handling their data is our first objective when it comes to the topic of facial recognition and its implications. Protecting individual liberty in the digital age is morally required, and this goal is in keeping with that. We have developed a framework in our project that gives meaningful consent top priority in order to properly satisfy this requirement. Instead of being subjected to monitoring and data collection in a passive manner, our solution gives users the active choice over whether or not their facial data is used.

By giving consumers power over their personal information, this method tackles privacy and consent head-on. By putting in place a consent-based system, we are upholding moral standards as well as encouraging an open society that values people's rights. This approach gives people the power to decide whether or not to participate in face recognition technology systems, empowering them and lowering the possibility that their data would be misused.

Artifact Description

Our system is purposefully made to satisfy the needs of Chinese government regulators as well as citizens, with the dual goals of protecting citizens' right to privacy and improving security.The system has consent processes that are customized for various scenarios. For specific events, there is a clear consent-giving process where participants can opt in or out of having their facial data used.In the case of public transportation, consent is integrated with ticket buying procedures by being correlated with the length of the passenger's public transport pass.

This design addresses the rapid advancement and societal impact of facial recognition technology in China through adaptive governance, regulatory sandboxes, and stakeholder engagement, integrating the relevant policies proposed by the research paper.

The system consists of four main modules. The database operations module handles data storage, retrieval, consent logs, and compliance checks. The facial recognition engine manages facial recognition operations and ensures accuracy and fairness. The consent and compliance system manages consent interactions and ensures compliance with Chinese data protection laws. Finally, the feedback and incident response module processes and responds to user feedback and complaints.

Technical Limitations

Our artifact has an innovative design, but there are some technological constraints that require balancing security and usability. The first one concerns user experience and security. Improving security frequently makes the setting of the system more difficult, which could lead to longer wait times or more stages in the admission process. But we think that in order to guarantee user safety and data integrity, this trade-off was essential. The second contrasts immediate data deletion with long-term data preservation. We made the decision to keep data for longer in order to study trends, increase future event security, and improve system learning. To limit the risk of potential privacy breaches, stringent data protection measures are necessary with this technique.

Ethical Frameworks

Our project is informed by two major ethical frameworks: utilitarianism and deontological ethics, specifically Kantian deontology.

Utilitarian ideas emphasize the maximization of pleasure, the maximization of utility for the relevant population, and the evaluation of activities only on the basis of their results, not their intentions. In specific, rule utilitarianism aims to maximize overall utility by enforcing rules that, in general, advance the greatest good. While facial recognition technology can optimize utility by offering ease to users, there are long-term consequences that could erode social cohesion by establishing a mass surveillance state, as seen in China. A state that violates citizens' rights may be considered unethical from a utilitarian standpoint if it causes widespread harm. Therefore, by guaranteeing that the state cannot use people's facial recognition data without their express consent, our design seeks to prevent going to this unethical extreme. Our consent-based facial recognition software is made to prevent the possible long-term negative effects of this technology.

Categorical imperatives, which urge people to behave in ways they would like to be universally accepted, are the driving force behind Kantian ethics. People should never view other people as mere means to an end, but rather as ends in and of themselves. When it comes to face recognition, people could end up being seen as nothing more than tools, and their information could become a valuable resource for businesses. This is especially relevant in societies such as

China, where people's "worth" is frequently assessed by how well they follow predefined standards. Our technology makes sure that facial recognition is only used with meaningful, informed permission in an effort to restore individual autonomy. This architecture makes sure that personal information is only used to train the facial recognition algorithm in accordance with ethical standards, and is neither sold nor exploited. By adhering to these principles, our design respects each person's inherent worth and autonomy, aligning with Kant's principle of humanity.

Key Technical Choices

We prioritized responsible technology during the creation of our facial recognition system by making a number of crucial technological choices that guarantee the integrity and equity of the system. The informed consent method, which ensures that all users are aware of and consent to how their data will be collected and used before any processing takes place, is essential to our design. Additionally, users are empowered and may ensure that ethical standards are followed because they have the simple ability to withdraw their consent at any moment.

We put strong security measures in place to safeguard private face recognition data, such as sophisticated data encryption, safe storage options, and frequent security assessments. These steps are essential for protecting user data by averting breaches, illegal access, and data leaks.

We also used a variety of training sets to mitigate potential biases in our facial recognition AI. By greatly lowering false positives and negatives, this method guarantees the accuracy and equity of the system across various demographic groups.

In order to respond to consumer complaints and feedback quickly and uphold confidence, we also put in place a framework for doing so. In addition to encouraging transparency, this feedback system enables us to continuously develop and enhance our technology.

Limitations of Our Approach

A number of theoretical and practical obstacles stand in the way of our consent-based facial recognition system's possible implementation by the Chinese government. Complicating governmental buy-in and execution, authorities used to more liberal access to surveillance data may oppose the enforcement of consent policies. Social factors are also important; for example, people may feel pressured to agree to face recognition at airports in order to fit in with their friends or avoid delays, which could compromise the idea of informed consent.

Security threats are still another major obstacle. Threats can arise in any system, and hackers and other bad actors are bound to be drawn to a collection of private face recognition data. Data breaches are still possible even with strong security measures like encryption and security audits.

Aside from that, our system has to be updated often due to the changing regulatory frameworks governing surveillance and data protection, which can be unstable and complex. Furthermore, there's always a chance that, once widely used, this technology may be abused by a government that decides to take control of it for other purposes, turning it against its citizens.

Conclusion

In conclusion, our consent-based face recognition system emphasizes how crucial it is to have informed consent, implement strong security measures, and reduce biases in order to guarantee accuracy and fairness. In spite of obstacles, especially in areas where surveillance is commonplace, such as China, our initiative serves as an example of the critical intersection between ethical governance and technical progress. We show how technology may both improve security and preserve individual rights by incorporating adaptive governance and highlighting user control over personal data. This way, technology serves to uphold rather than violate democratic norms and human rights.