Privacy and Informed Consent with Facial Recognition Software

Authors: Faris Ashriem, Michael Ta, Leah Mlakar, Levi McFetridge

Advisor: Jackie Woldering

Cleveland State University

Choose Ohio First

ABSTRACT

This expository research aims to highlight facial recognition software and the ethics around it. The data collected from these cameras have been utilized for a multitude of reasons, ranging from marketing to security and surveillance. We researched several case studies across different companies storing data on human faces and how it affected the overall safety of all stakeholders. The cost-benefit analysis between the advantages of facial identification databases and the obvious side-effects of collecting such personal information is discussed with respect to the moral dilemmas raised. We also studied the possibilities of how a breach in these systems can have serious consequences in the realm of security and law enforcement. As we become more reliant on facial recognition, we need to ensure that our personal data cannot be criminally exploited for capital gain and to ensure that the law can appropriately protect such privacies.

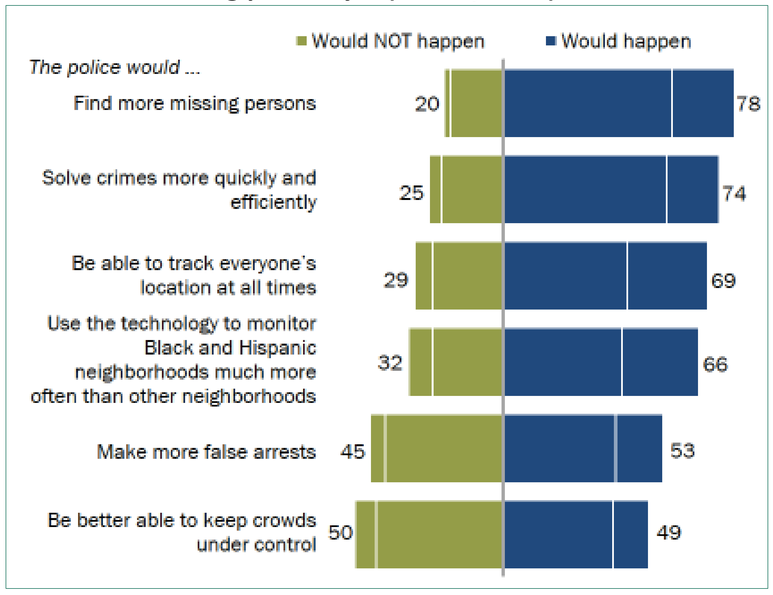
INTRODUCTION/OBJECTIVES

Facial recognition is currently being used in a multitude of ways such as finding missing people, identifying criminals, and recording eye movement for marketing research. However, there is much controversy surrounding the use of this technology. Using existing data, our goal is to find out if the use of facial recognition should be allowed to due privacy reasons. We also looked at potential security issues revolving around the storage of this information. Another objective of ours is to gain the knowledge of the potential risks if this data was leaked or stolen.

Methodology

- **The Cleveland State Michael Schwartz Library was used to reliably research in person**
- **We used Google Scholar for our online sources to keep our work validated.**
- **We only referred to sources like outlets, interviews, and online communities to gather different opinions and data.**

Figure 1. Percent of U.S. adults who say that the use of facial recognition technology by police becomes widespread, then the following probably... (Raline, 2022)



RESULTS

- **Facial recognition can be used for tasks such as identifying criminals by police and the government.**
- **Other potential uses include tracking people entering/leaving apartment buildings, or retail stores enhancing credit card security.**
- **Many people don't support the use of this technology due to the potential misuse or lack of privacy.**
- **Overall data that uses facial recognition is at a high risk of being breached.**

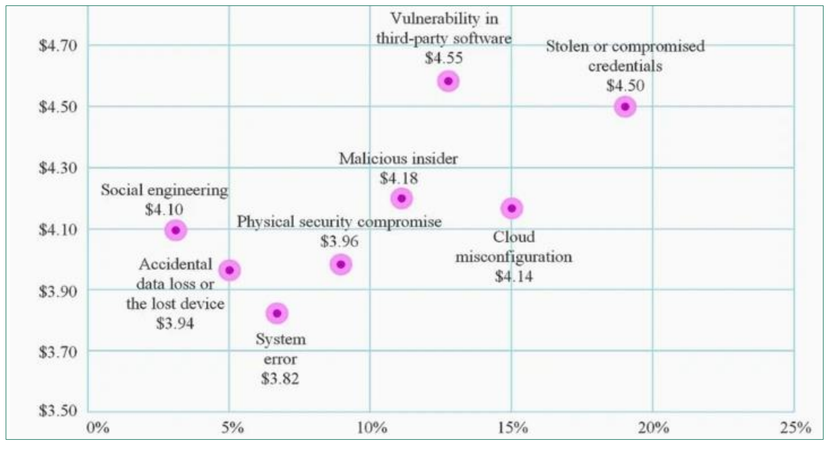


Figure 2. Measured in USD millions. The most common initial attack vector in 2022 was stolen or compromised credentials.(Wang, 2023)

DISCUSSION

Although facial recognition seems to have benefits, there are clear potential issues that would occur. These programs are not one-hundred percent accurate, so false identification is likely to occur. Since the technology is not fully developed, using it now could result in more harm than good.

Another issue with this is who gets access to this information, and who decides this. Some people might feel safer if only trusted authorities have access to their data but feel unsafe if social media sites or retail stores also have the same access. Many people feel uncomfortable with sensitive information about them being held by various agencies and corporations.

Storing all this sensitive data can be dangerous due to data breaches. There have been many large breaches in the past, including Facebook. Based off our research, we have found that facial data has been demonstrated to be vulnerable and easily breached, which shows that this data is not necessarily safe.

CONCLUSIONS

A lot of people already feel that they cannot live their everyday life without being tracked by the government, and the use of facial recognition would only add another layer to this. This would only make us feel like we have less privacy than we already have. In addition, this data could potentially be leaked or stolen due to how new this technology is. Based on our research, we believe that the use of facial recognition has high potential to cause more harm than good which justifies the need for legislation to be passed to regulate biometric data sharing and storage.

References

World, MAPL. "DO Security Risks Exist in Face Recognition Databases?" LinkedIn, 19 Oct. 2023, www.linkedin.com/pulse/do-security-risks-exist-face-recognition-databases-maplworld-1c.

"Facial Recognition Technology: What Are the Benefits and Risks? · Emsnow." EMSNow, 17 Aug. 2022, www.emsnow.com/facial-recognition-technology-what-are-the-benefits-and-risks/.

"2. Public More Likely to See Facial Recognition Use by Police as Good, Rather than Bad for Society." Pew Research Center: Internet, Science & Tech, Pew Research Center, 17 Mar. 2022, www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/.

Wang, Meng, et al. "Identifying Personal Physiological Data Risks to the Internet of Everything: The Case of Facial Data Breach Risks." Nature News, Nature Publishing Group, 8 May 2023, www.nature.com/articles/s41599-023-01673-3.