Pitch Controlled Pong

(Technical Report)

Limiting Privacy Incursion from Facial Recognition through De-identifying Face Images in the Public Domain

(STS Research Paper)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

John Phillips

Fall, 2022

Technical Project Team Members

Charlie Hess

Isaac Duke

Teddy Oline

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Introduction

Facial recognition technology has seen profound advancements in recent years. This evolution has allowed this technology to be developed into tools with severe implications regarding individual privacy. These privacy concerns are juxtaposed against this technology's massive potential for good. For instance, "Chinese police were able to identify and apprehend a criminal at a music concert attended by 60,000 people" (Walsh, 2022). In New Delhi, facial recognition "reunited nearly 3,000 children with their parents" (Walsh, 2022). Even in the United States, facial recognition is being used for good. A Florida man was wrongly accused of vehicular homicide and facial recognition software was used to exonerate him. After spending "hundreds of hours" looking for the sole witness to the accident, this technology located the witness "within two seconds…at some club in Tampa" (Hill, 2022). This example differs from the previous two in a fundamental way – the dataset used to "match" faces. The criminal at the music concert had a known mugshot on file. The children reunited with their parents were matched against photos submitted for the specific intention at hand. However, the database of images used to identify the witness that exonerated the Florida man is owned and operated by a New York based startup – Clearwater AI. This company has created a database "of people's faces from across the internet, such as employment sites, news sites, educational sites, and social networks including Facebook, YouTube, Twitter, Instagram, and even Venmo " (Hill, 2020). The witness was found using a photo posted on Facebook – a photo collected and used without their consent.

Facial recognition technology is a novel use of artificial intelligence. This technology employs machine learning models: these models are algorithms that find patterns or make predictions based on a set of data. There have been many facial recognition algorithms created, and each have their advantages. However, these algorithms can only be as powerful as the data

they are trained with. For this reason, facial recognition technology poses a grave danger to individual privacy. This can be seen through Clearwater AI; this company has taken to scraping pictures – storing photos along with associated information – from the public domain. This is a powerful tool in amassing a database of individuals who may not have a face photo available by other means. The capabilities this platform offers is unprecedented, however, it comes at the expense of individual privacy.

Technical Discussion

The aforementioned discussion of Clearview AI, the data they collect and the power they wield is very loosely coupled with my Computer Engineering Capstone. Regardless, there are several implications that are shared. My capstone project is a reworking of the original video game, pong. This game is basic by today's standards and for those unfamiliar, features two paddles on either end of the screen that allow users to bounce a ball between them, with the goal being to score points by getting the ball past the opponent's paddle. Our novel spin on this game is that instead of controlling the paddles with a joystick or other physical input system, we utilize the user's vocal pitch to control the panel. It is this system of input that shares an inherent biasing with facial recognition. Just as deep learning based facial recognition algorithms are known to "incorrectly identify people of color," (Marks, 2021) human vocal input varies widely along racial and cultural lines. I recognize that a misrepresented input to a video game does not hold the same weight as a wrongly identified person of interest from a facial recognition algorithm. However, the method of vocal recognition in its entirety has significantly more profound implications and is subject to these biases. Voice recognition has applications in translation software, voice prompt creation such as telephone prompts, and even voice-based biometry security. These applications all have the potential to inequitably serve underrepresented groups through embedded bias.

Specific to my group's project, we have taken steps to provide an equal playing field for all individuals through carefully considering the calibration steps taken before commencing a game. It is our hope that the simple system we create remains unbiased and equitable to all players.

STS Discussion

Returning to the implications of facial recognition and large data collection it incurs, Clearview AI has amassed "2.8-billion face photos…creating a search engine for any face image hosted on the public Internet" (Marks, 2021). In comparison, the FBI has access to 411 million face images. The FBI has amassed its database through government-provided images, such as mug shots and driver's license photos. In contrast, Clearwater AI has taken to collecting images from every corner of the internet; this approach has landed them in a difficult situation. Google, Twitter, and LinkedIn have all issued cease and desist letters regarding the information taken from their websites. The American Civil Liberties Union filed legal complaints in Illinois and California. Clearwater's operations in Canada ceased after privacy concerns were raised. NGOs from the UK, France, Austria, Italy, and Greece filed legal complaints against Clearview, spurring investigations into their practices and immediately ending usage in the European Union. These investigations and litigations have limited Clearview AI's potential customer base and have opened their doors to more sweeping legislation.

Clearview AI uses a process called web scraping to gather data from across the internet. Unlike their proprietary facial recognition algorithm, web scraping is not a novel practice. Social Media Companies (SMC), such as Facebook (Meta), Twitter, LinkedIn have been deeply invested in this technology for years. The business model of most SMCs revolves around leveraging data they gather from customers to develop new, innovative products and effective advertising strategies to market those products. This results in a large collection of data from their users, thus

making them valuable targets for web scraping. This targeting has led to SMCs to "employ increasingly sophisticated artificial intelligence (AI) based software to prevent automated bots and web crawlers from accessing and scraping customer data." (Johnston, 2020) Preventing the automated collection of data from a website or application is even more sophisticated as the process of collecting said data – both of which are technically beyond this paper. Regardless, SMCs use more than technological means to limit and deter anyone who tries to utilize the data they have collected. Under the auspices of enforcing their own proprietary rights and their customers' privacy rights, "SMCs have asserted a variety of legal claims – ranging from common law trespass and breach of contract theories to federal copyright and Computer Fraud and Abuse Action (CFAA) claims – in an effort to shut down, or at least deter, their competitors' efforts to access and 'scrape' SMC customer data" (Johnston, 2020) The most notable of recent cases to have been heard was "*hiQ Labs, Inc v. LinkedIn Corp*." This decision by the U.S. Court of Appeals for the Ninth District Circuit, set the precedent in favor of web scraping. HiQ, a company that scrapes publicly available data to yield insight into business' personnel, was issued a cease-and-desist stating that they "violated LinkedIn's terms of use agreement, and that any future access of LinkedIn data would subject hiQ to liability under the CFAA, the Digital Millennium Copyright Act (DMCA), California Penal Code Section 502(c), and the California common law of trespass." (Johnston, 2020) HiQ subsequently filed an injunction that was ruled in their favor, effectively prohibiting LinkedIn from erecting technological barriers to hiQ's automated bots. This case was reaffirmed in 2022 cementing it as a cornerstone precedent in the right to automate gathering of publicly accessible data. This case has massive implications regarding facial recognition as Clearview AI's massive face databases and associated data comes from these automated web scraping techniques. As their business model, similarly to hiQ's, revolves around the usage of this

publicly accessible data, Clearview AI could potentially use this precedent if ever challenged regarding their data collection techniques.

Conclusion

There is no doubt that facial recognition technology will continue to improve in accuracy and pervasiveness. However, 'brain' of this technology is no more than complex mathematics behind powerful digital computational tools. The real power of this technology is derived from the data being fed into these algorithms. This data is at the center of the fight for individual privacy in the digital age. As continued development into more complex, AI based, autonomous web scraping programs and the legal precedent protecting organizations that employ these entities for their own monetary gain, an individual's right to digital privacy is under attack.

References

Hill, K. (2020, January 18). The Secretive Company That Might End Privacy as We Know It. *The New York Times*. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Hill, K. (2022, September 18). Clearview AI, Used by Police to Find Criminals, Is Now in Public Defenders' Hands. *The New York Times*. https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html

Marks, P. (2021). Can the Biases in Facial Recognition Be Fixed; Also, Should They? *Communications of the ACM*, *64*(3), 20–22. https://doi.org/10.1145/3446877

Johnston, L. (2020). Ninth Circuit Rejects LinkedIn's Efforts to Block Web-Scraping of Member Public Profiles. *Computer & Internet Lawyer*, *37*(4), 5–7.

Walsh, T. (2022). The Troubling Future for Facial Recognition Software: Considering the myriad perspectives of facial recognition technology. *Communications of the ACM*, *65*(3), 35–36. https://doi.org/10.1145/3474096

Word Count: 1492