Why Facial Recognition Technology is Essential

April 12, 2021

John Wilson

CS 300T

Professor Rekha Gupta

Table of Contents

John Wilson

Professor Rekha Gupta

CS 300T

4/12/2021

Why Facial Recognition Technology is Essential

Introduction

It is 12:00 am on a Saturday night, and you have just been robbed at knife point. You report the incident to the police; but cannot remember details of the criminal. Two days later, the police contact you to return your property and to inform you the thief was Identified and apprehended by the assistance of facial recognition technology. The need to identify a person has been an ongoing enterprise since the wanted posters were first used in the United States in 1874 by the Pinkerton Detective Agency. The Federal Bureau of Investigation (FBI) would later adapt fingerprinting to uniquely identify individuals. Today's progress of computer technology has added another exceptional identifier tool known as facial recognition technology and it is being utilized in concert with police body cameras, drones, official ports of entry, etc. This paper will discuss that even though facial recognition software has the potential to threaten individual privacy, the software is essential because it strengthens security measures and helps law enforcement locate missing persons and criminals.

What is facial recognition software?

Facial recognition is designed identify an individual by scanning their face through two-dimensional (2D) photographs and comparing to photos in a database. However, there are some misconceptions about how simplistic the technology works such as it merely measures the size of your mouth or the distance between the eyes similarly portrayed in science fiction movies like

Marvels “Black Panther – Wakanda Forever”. In fact, the software is a complex mathematical algorithm which selects several specific characteristics of the human face at once, like shape of the chin and nose, location of the eyes, curve of lips, the distance between the forehead and chin, etc., and compares this to an existing facial database.

Strengthens security measures.

On September 11, 2001, the United States (U.S.) was attacked by terrorists commissioned and trained by Osama Bin Ladens Al Qaida terrorist group. From this point forward, the world today seems to be more dangerous with several reports of individuals committing atrocities against governments or communities because of race or religion. The use of facial recognition technology along with additional biometric information can help curb the war against these horrific misdeeds.

In 2019, the U.S. receives received a total of “122,253” international air travel passengers daily (“Air Passenger Travel”). This is a staggering amount of people to screen and without the technology implemented it will result in the increase likeliness of individuals with bad intentions slipping through unnoticed because of human error. If facial recognition were used in 2001, American Airlines Flight 77 terrorists Nawaf bin Muhammad Salim al-Hazmi and Khalid bin Muhammed bin Abdallah al-Mihdhar would have been detained. The Central Intelligence Agency placed al-Hazmi on a watch list when they learned his name and that he departed from Bangkok Thailand “on January 15 on a United Airlines flight to Los Angeles” with al-Mihdhar (9/11). If facial recognition technology were used at the border patrol points at the major debarkation points, they would have been apprehended which would have ended the plan to use flight 77 as a terrorist weapon. In addition, this could have had other far-reaching implications as it could have foiled the other planned attacks on that day as well.

U.S. airports are currently using this technology in the baggage areas, ticket counters, security areas, embarking and debarking of planes to better protect the passengers and employees passing through. In addition, the software has assisted the Transportation Security Administration “intercept six imposters” using false passports at U.S. airports (Buege).

Assists in locating missing children.

One of the most important reasons for the use of facial technology is to locate missing persons especially children and the elderly. Imagine your child had gone missing or abducted from a store or even your front yard. How about your grandmother with dementia walks off in the middle of the night in her nightgown and you cannot locate her? These scenarios are very much real and facial recognition software has been used to successfully locate these loved ones.

In 2019, Chinese law enforcement used facial recognition in identifying and reuniting a child with his parents after missing for thirty years. The child was abducted and sold to a childless family for approximately $840 U.S. Dollars. This worked because the software analyzed a 30-year-old picture and searched through their database. Eventually, they found the missing person and confirmed his real identity through DNA testing.

In 2020, India, used facial recognition technology through an application that helped locate missing children. The police developed the application themselves and the program uses up to “80 different points on the face” to match with photographs in their database (Nagaraj). Currently this app is responsible for the rescue of approximately 3,000 children used in illegal child slavery and other illicit practices.

According to a 2017 article by Trackimo.com, approximately eight million children are abducted annually worldwide and usually forced to fulfill all forms of abhorrent duties.

Hopefully with allowing the use of this technology can make a positive difference in helping to stop children gone missing.

Supports locating and identifying criminals and prisoners.

Another reason to allow facial recognition to be used is to assist constabulary agencies to identify and locate criminals and prisoners. Currently, law enforcements resources throughout the U.S. are at an all-time low with a limited or even low manpower pool and monetary budget constraints from either the COVID-19 pandemic or other political reasons. Facial recognition software with the use of additional investigative tools like fingerprinting and DNA, has been effective.

In August 2019, New York City police used facial recognition software to help identify and catch a 27-year-old rapist in the Bronx. The tech used high-definition video stills and comparted them to their criminal database to find the positive match.

In 2020, Las Vegas Police used facial technology to identify a wanted murder. The police used the suspects Facebook profile to match with images of criminals previously arrested. Las Vegas has continued to use the software to successfully locate and identify kidnappers, sex traffickers, child abusers, and the conducting of aggravated assaults and bring them to justice.

Another reason for law enforcement to use facial recognition is within the prison systems. Prisons possess significant challenges from prisoner and guard safety, accountability, and especially prisoner management. Prisoner management within a facility is the overseeing of accountability and movement within a facility. Using this software could make sure prisoners are not within unauthorized areas, slow down criminal activity and will also make sure the prisoners released are the correct individuals.

Facial recognition threatens individual privacy.

It is of major concern facial recognition technology will threaten the privacy of its citizens. In May 2019, the city of San Francisco, California joined other cities, like Boston, Massachusetts to ban city led law enforcement and other agencies from using facial recognition technology because of the perceived threat. Speaking in support of the ruling, Matt Cagle, a representative of the American Civil Liberties Union of California stated the use of facial recognition technology "provides the government with unprecedented power to track people going about their daily lives" and wants to stop the "unleashing of this dangerous technology" (Conger, Kate, et al.).

The statement above is not factual pointing to software being used without oversight or regulations. In fact, local and federal government agencies cannot use this technology without guidelines. The FBI's authority falls under statutes Title 18 U.S.C. 3052 – Powers of FBI Title 28 United States Code (U.S.C) 533 – Investigative and other officials, and Title 28 U.S.C. 534 – Acquisition, preservation, and exchange of identification records and information; Electronic code of federal regulation Title 28 CFR 0.85 – Criminal justice policy coordination; Memorandum of understanding – Implemented between state and federal agencies on the use of facial recognition technology.[1] And depending on the state you are in they possess something similar policies and procedures. Arbitrarily making statements the government has the power to surveil private citizens without oversight is simply preposterous.

[1] See FBI's Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Phase II System, page 10 for regulations and authorities.

Another safeguard against this technology being used wrongly is given by the Fourth Amendment to the U.S. Constitution. The amendment protects “the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures …. “ (Congress). Boiled down, this means an individual should expect a reasonable right to privacy from local and federal government agencies. But what is privacy in the digital age? If you volunteer the information, you cannot expect the right to privacy especially when posting on a social media platform. This was proven in the case of United States v. Miller where the supreme court ruled that, “a person cannot have a protected privacy interest in information voluntarily turned over to a third party” (Carthew). This means if you voluntarily give up the information then you cannot expect the information to be private. The fourth amendment is a fundamental safeguard put in place to make sure governments and law enforcement do not violate our rights to privacy.

Conclusion

In this paper I have defined facial recognition as a technology that identifies an individual using a 2D photograph and matching it through a database. In addition, the technology needs to use more at airports or other ports of entry to assist in screening against bad actors and to help in the identification and location of missing children and criminals. Although facial recognition is believed by some to threaten individual privacy, the technology is an essential tool to our overall safety and security from finding missing persons to locating and detaining criminals.

Works Cited

United States Department of Transportation. "Air Passenger Travel Arrivals in the United States from Selected Foreign Countries." *Bureau of Transportation Statistics*, United States Department of Transportation, 23 July 2021, www.bts.gov/content/air-passenger-travel-arrivals-united-states-selected-foreign-countries-thousands-passengers.

Kim, Soo. "Who Were the 9/11 Hijackers? The 19 Al-Qaeda Members Who Carried Out Terrorist Attack." *Newsweek*, Newsweek, 11 Sept. 2020, www.newsweek.com/united-states-911-attacks-september-11-terrorists-al-qaeda-plane-hijackers-1531041.

National Commission on Terrorist Attacks. The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. Authorized, vol. 1, W. W. Norton & Company, 2004, govinfo.library.unt.edu/911/report/911Report.pdf.

Buege, Jenna. "Evaluating the Pros and Cons of Facial Recognition in Travel." *The Compass*, The Compass, 2 Dec. 2019, www.vaxvacationaccess.com/the-compass/evaluating-the-pros-and-cons-of-facial-recognition-in-travel.

Weiss, Eric. "Police Use Facial Recognition to Find Child Abducted 30 Years Ago." *FindBiometrics*, 21 May 2020, findbiometrics.com/chinese-police-use-facial-recognition-find-child-abducted-30-years-ago-052107.

Nagaraj, Anuradha. "Indian Police Use Facial Recognition App to Reunite Families with Lost Children." *U.S.*, 14 Feb. 2020, www.reuters.com/article/us-india-crime-children/indian-

police-use-facial-recognition-app-to-reunite-families-with-lost-children-idUSKBN2081CU.

Turner, Allan. “Biometrics: Applying an Emerging Technology to Jails.” *American Correctional Association, Corrections Today*, vol. 62, no. 6, 2000. *United States Department of Justice, Office of Justice Programs*, www.ojp.gov/pdffiles1/nij/10_00.pdf.

Conger, Kate, et al. “San Francisco Bans Facial Recognition Technology.” The New York Times, 16 May 2019, www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

Carthew, Alexandra. “SEARCHES AND SEIZURES - FOURTH AMENDMENT AND REASONABLENESS IN GENERAL: PROTECTION OF PRIVACY INTERESTS IN THE DIGITAL AGE.” North Dakota Law Review, vol. 94, no. 1, 2019, p. 197.

Continental Congress. “The Bill of Rights: A Transcription.” *National Archives*, Continental Congress, 25 Mar. 2021, www.archives.gov/founding-docs/bill-of-rights-transcript#toc-amendment-iv.