The Rise of Facial Recognition Software: Purpose, Implementation, and Policy Responses

Vezio Kittel

November 24th, 2025

Introduction

The development of facial recognition software (FRS) is one of the most debated innovations in recent times. FRS serves to identify individuals based on key features such as "the distance between your eyes, the depth of your eye sockets, the distance from forehead to chin, the shape of your cheekbones, and the contour of the lips, ears, and chin"(Kaspersky, 2024). Due to our diverse application and integration of this technology, we have seen immense transformations in societal areas including public security, retail, authorization, and authentication, sparking controversy regarding the ethics and privacy implications of this technology. This paper will explore the purpose, history, evolution of design, impact, current, and future trends of facial recognition software, as well as providing specific applications to demonstrate its variable nature.

Purpose of Facial Recognition Software

The primary purpose of facial recognition software is, as the name would suggest, to identify (or recognize) individuals by analyzing their facial features to enable automated identification or verification of individuals. The first thing that comes to most people's mind when discussing FRS is most likely the face ID scan on their Iphones which addresses the first of many applications, authentication. Personal devices use FRS to replace the traditional need of a password, allowing quicker and more seamless alternatives that are just as if not more secure. FRS has also quickly found its way into our security and surveillance. Using this technology, coupled with cross referencing to find names and other information, cameras around the world can identify individuals in real time, allowing comprehensive reports to be made and shared with law enforcement to the actions and locations of known offenders, missing people, or people of

interest. This is where controversy sets in as this can easily be abused by governments and infringe on individual civil rights. Modern examples of this would be Russia and China, both countries that actively use facial recognition to identify potential “threats” to their leadership by using their face to find more personal information in areas like social media. It's a double edge sword, the technology that provides security can also take it away from you. Other uses for FRS can be seen in personalization of marketing in that FRS will detect your expressions and determine if you enjoy what you are looking at, allowing markets to tailor to your preferences (essentially a more sophisticated version of cookies). Using the same expression detection, FRS enters healthcare. “Face images are captured by the camera or any other device, and then, the features are extracted by…analyzing the primary curves on the faces that are commonly seen in eyebrows, eye, lips, and nose [10], [12]. Measured movements of these four key features are used to identify the expression”(Torki Altameem, Ayman Altameem, 2020). This allows doctors to better assist patients with disabilities such as autism or mutism to express what they are feeling, leading to a more accurate diagnosis going forward. In fact there was a study conducted at the Research Project of School of Information Management Wuhan University that tested FRS on individuals with autism found that “the accuracy rate of facial expression recognition is 81.4 percent” (Zhao, Lu, 2020), meaning this method of determination has a “diagnostic accuracy of autism higher than that of traditional systems” (Zhao, Lu, 2020). These applications severely underscore the versatility and nuance of FRS because its application potential is endless, but they do point out the need for sanctions and ethical considerations in its use.

History and Evolution of Facial Recognition Software

In the mid 1960s, Woody Bledsoe, Helen Chan Wolf, and Charles Bisson made great strides in technological advancements through their creation of the very first facial recognition

system. This project was funded by an unnamed intelligence agency, though highly implied it was for the US government and military, resulting in most of their work never being published. Later it was revealed to the public that their initial work involved the manual marking of various "landmarks" on the face such as eye centres, mouth etc. These were then mathematically rotated by a computer to compensate for pose variation. Moving on to the 1970s, Goldstein, Harmon and Lesk advanced the initial findings by testing "a set of 22 features [that] was evolved from an initially larger set to provide relevant, distinctive, relatively independent measures which can be judged reliably" (Goldstein, Harmon, Lesk, 1971). These features include characteristics like hair color, lip thickness, and jawline shape. The findings from this study conclude that "approximately 6 of an individual's features are required to isolate him from a population of 255" (Goldstein, Harmon, Lesk, 1971). One of the major reasons behind this group's discoveries compared to the start in the 1960s is due to the creation of complex algorithms involved in computer vision. The advancements continued in the late 1980s to early 1990s with the introduction of linear algebra into the FRS algorithm. Mathematician Sirovich and Kirby created a system "computing an average face from a set of pictures. Then they used that same set of pictures to find the most common ways faces differ from their average. These differences were expressed using a set of images called eigenfaces" (University of Houston, 2023). To further corroborate these findings, neuroscientists found that "once our brain realizes that it's observing a face, cells in certain parts of the cortex seem to respond to deviations of our friend's face from the average. Certain brain cells might respond to her nose being shorter, while others indicate that her eyebrows are more peaked than those on an average face" (University of Houston, 2023). This, along with the National Institute of Standards and Technology (NIST) Face Recognition Vendor Tests (FRVT) in the early 2000s, was the most major turning point in the

softwares evolution because at this point it had become reliable enough for major government agencies such as The Defence Advanced Research Projects Agency (DARPA) and the National Institute of Standards and Technology (NIST) to start using it in an effort to integrate it with law enforcement agencies. Fastforward 17 years we see the introduction of face ID in Iphones and fast forward to now we have face ID in almost every corner of society.

Impact of Facial Recognition Software

It's undeniable the positive impacts facial recognition software has had in the short time the technology has been around. Despite its implications, the existence of FRS has brought security to a new level. From city streets to businesses to airports, practically any place that is monitored by camera can and does use facial recognition software to some degree. The methods of identification have been completely revamped and upgraded in modern day. The increased convenience of FRS in everyday life through fast and contactless means to access smartphones as well as in the workplace environment replacing key cards increasing risk prevention and reducing unauthorized access if one was to lose, misplace, or have their access stolen. Transportation processes, specifically at airports, are becoming increasingly easier on the traveler due to this technology. TSA is implementing FRS “to automate the current manual ID credential checking process”(TSA, 2023) while also easing travelers of any concerns regarding privacy by ensuring it “will not be used for surveillance or any law enforcement purpose. TSA uses facial recognition CAT-2 technology only to verify the identity of the traveler at the podium and make a determination for access into physical security screening” (TSA, 2023). On top of all of this, the previously mentioned benefits in retail spaces creating more personalized experience as well as medical fields being able to be more accurate in their assistance are some more net positives stemming from this technology. Unfortunately, there are negatives to balancing the scales.

Starting with privacy concerns which were touched on briefly earlier, the use of FRS has significant potential privacy violations. The mass monitoring and recording of individuals essentially without their explicit consent raises many red flags because no one besides those behind the scene know what is being done with this information. A very clear and recent example of this can be seen in the lawsuit against Clearview AI, an American facial recognition company, providing software primarily to law enforcement and other government agencies. The lawsuit stems not from what they do with their information because, for the most part, they are giving their information to law enforcement and government agencies but rather how they obtain that information. Clearview AI is being fined for "harvesting billions of photos of people from the internet, which it then converts…into a unique biometric code per face", all of which is done without the consent of the individual"(Hart, 2024). There are also concerns brought up due to potential bias and discrimination in FRS. A study done at MIT found that "a significant gap exists when comparing gender classification accuracies of females vs males (9 - 20%) and darker skin vs lighter skin (10 - 21%)"(Buolamwini, 2017). It was discovered that of their tests, 37-83% of discrepancies in classification resulted from "darker females" while "lighter males" only contributed 0.4-3% of said errors. Lastly, aside from private corporations, there is a lot of concern regarding government misuse of this technology. Already addressed previously, but countries such as China and Russia are very adamant in abusing this technology to maintain authoritarian leadership over its people and that's an issue that can't be allowed to find its way into any other countries.

Current and Future Trends

The current trends of FRS have been touched on quite a bit in previous excerpts of this essay so to briefly cover them we have seen a large focus on the development of emotion

recognition, primarily in the medical field, but also in law enforcement for instances such as interrogations to go hand in hand with polygraph test, adding one more layer of assurance. A large integration into the Internet of Things through smart home applications, such as Ring doorbells, taking steps or at least in talks about adding it. Lastly, large ethical concerns regarding this technology have sparked policy makers to implement regulations for the use of FRS. Looking to the future, there are goals in improving the fundamentals of this technology like increasing its accuracy so as to eliminate any bias, as seen in the MIT study, through a wide range of algorithms and training datasets. Regarding user privacy there are plans to use blockchain technology to create a secure and decentralized way of managing FRS databases. This would provide more security against breaches and transparency in its use. Lastly, the introduction of this software in augmented reality (AR) and self driving vehicles. Adding FRS to AR would allow you to be a playable character by scanning your biometrics and replicating them in the game as well as capturing your mouth movements when talking and facial expressions, creating a massively more immersive experience.In a consumer and retail space you could use AR to simulate what some products or clothes would look like on your body such as makeup and headgear.

Conclusion

Facial recognition software displays a monumental advancement in information technology through its extensive capabilities in security, healthcare, and personalization. However, its implementation invites challenges, including privacy risks, misuse, and algorithmic biases. As this technology and society itself continue to develop and work through these issues, the need for transparent regulations and ethical frameworks are necessary in capturing FRS's

numerous benefits while minimizing its drawbacks. Addressing any and all dynamics of FRS are pivotal to its success in integration with society.

Works Cited

Emerald Publishing. (2019). *Library Hi Tech: Leveraging facial recognition technology in libraries*. *Emerald Insight*. https://www.emerald.com/insight/content/doi/10.1108/lht-08-2019-0176/full/html

Hart, R. (2024, September 3). *Clearview AI: Controversial facial recognition firm fined $33 million for illegal database*. Forbes. Retrieved November 29, 2024, from https://www.forbes.com/sites/roberthart/2024/09/03/clearview-ai-controversial-facial-recognition-firm-fined-33-million-for-illegal-database/

Kaspersky. (n.d.). *What is facial recognition?* Kaspersky. Retrieved November 29, 2024, from https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition

MIT. (2017). *Face recognition technology and its history*. MIT DSpace. Retrieved November 29, 2024, from https://dspace.mit.edu/handle/1721.1/114068

ScienceDirect. (2020). *Facial recognition technology: An application review*. *Elsevier*. https://www.sciencedirect.com/science/article/abs/pii/S0262885620301761

Transportation Security Administration (TSA). (2023, May 22). *Facial recognition technology: TSA factsheet*. Retrieved November 29, 2024, from https://www.tsa.gov/news/press/factsheets/facial-recognition-technology

University of Houston. (2023, October 18). *Facial recognition technology: Emerging applications and ethical considerations*. *Engines of Innovation Podcast*. Retrieved November 29, 2024, from https://engines.egr.uh.edu/episode/2544