MUNESCO

Forum: GC5: Communication and Information
Issue: The contribution of facial recognition technology to digital trust and hypothetical consequences.
Student Officer: Barışta Harmancı
Position:

Introduction

Facial recognition technology has become one of the most popular and reliable way for identification and verification due to its unique and developed procedure. The main part of the technology is the biometric systems, which recognises the pre-set face as the main user or the owner of the device. With the device recognizing your distinctive facial features, it is almost impossible for someone else to unlock, verify and use the device without the owner's consent. The development and creation of FRT goes all the way back to 1964 and was used primarily for the US military. Woody Bledsoe, Helen Chan, and Charles Bisson lead the research and development of FRT of the present day. This technology was then developed and restructured to fit in and afterwards was used in mugshots, thermal cameras and nowadays across mobile platforms and personal devices.

This report focuses on FRT and elaborates on the possible challenges and concerns that might and will come with the technology. It explains the needed limitations of the technology, the cases where it may be misused and the ethical and economic factors. With ethicality and affordability of the technology being the main issue to tackle, the possible developments and restrictions are also important. With the restrictions and certain laws, FRT may be affordable and may not cause a major threat to countries and its citizens.

Definition of Key Terms

Facial Recognition Technology:

A facial recognition system, is a technology capable of identifying or verifying a person from an image or a video frame that is captured by the device it is featured in. There are multiple methods in which facial recognition systems work, but in general, they work by comparing selected facial features from the given image and biometric systems.

Biometric system:

Biometric systems are the systems that use measurements and statistical analyses of people's unique physical and behavioural characteristics. They are mainly used in facial recognition, mugshots and personal information cards such as identity cards and passports.

Digital Trust:

Digital trust is the trust of users in social media about solving issues and developing the digital world. Digital trust is given to companies who have proven themselves on topics like safety, reliability, security, privacy, and ethicality with their product such as applications and devices.

Face ID:

Face ID is a facial recognition and authentication technology developed by Apple. Face ID allows a user to unlock their device, or make transactions, just by using the devices newly designed front-facing camera.

Identity Verification Service:

The service is used by businesses to assure that users or customers provide information that is associated with the identity of a real person. The service is capable of matching authenticity of physical identity documents such as a driver's license and passports through documentary verification.

Background Information

The argument over privacy and identity theft has been around since the beginning of the usage and development of social media and artificial intelligence. With most social media platforms and devices having facial recognition features in them, many people started discussing the issue of privacy and the threat it can cause over the accounts and the people who own the accounts. The start of facial recognition in social media started with Facebook's feature which recognised the face of the people in the posted photos. The main aim of this feature was to tag people and their accounts to the posted photos. Afterwards, many applications such as Instagram and Snapchat started using facial recognition with filters and tagging features which caused a lot of controversy and suspicion. Within a few years, multi-billion companies like Apple and Samsung started using facial recognition technology as a way of unlocking devices and verifying that it's the owner who is doing transactions and operations.

Many users of social media were suspicious and curious about how their personal information was kept private and secure due to the amount of ethical controversy and issues like identity theft. People were unsure and insecure about the functioning of the feature. The accusations about identity theft and unsafe personal data storage led to many arguments over the usage and purpose of facial recognition technology.

Major companies like Facebook and Apple have talked and addressed publicly that the usage of FRT in their products and social media platforms were safe to use and that no information was being sold or stolen by them. People are still biased about the usage of FRT and have started many campaigns and oppositions. Many users also believe that the FRT can be manipulated and can become a threat with further development. There has been many cases of face-swapping and information selling that have been witnessed by the whole world. Hackers and terrorists have used FRT to act and talk as someone else to create conflict and commotion.

Timeline of Major Events

1964-1965	The first facial recognition technology was developed by Woodie Bledsoe, Helen Chan, and Charles Bisson.
2010	Facebook started using facial recognition to help people with tagging each other on posts and photos.

2011	First major installation of face recognition in an airport. The government of Panama, with the collaboration with the US, authorized a pilot program of facial recognition system (Facefirst) in order to cut down on illicit activity in Panama's Tocumen airport which is known for its drug trades. Shortly after implementation, the system resulted in the apprehension of multiple INTERPOL suspects. The Facefirst system's implementation at Tocumen, is still the largest functioning facial recognition system in an airport
2015	Snapchat published their face filters for the users, which scanned your face and put on effects. These lenses can also change your facial structure and facial features in the pictures and videos.
2017	Apple launched their new phone iPhone X which included the Face ID feature. These phones are able to unlock the device and verify the user with FRT.
2018	Apple Inc. launched IOS 12 which had a new feature where your device could separate and classify the pictures and videos in your gallery. You could search for a phrase or word and the pictures that included the relevant object or person would be presented by the iPhone.
2018	The Facebook–Cambridge Analytica data scandal was a major political scandal in early 2018 when it was revealed that Cambridge Analytica had harvested the personal data of millions of users Facebook profiles without their consent and used it for political advertising purposes.
2019	Instagram launched the new feature of the application. The app now has lenses just like Snapchat that uses FRT and can now put on effects and change your facial structure.

Major Countries and Organizations Involved

Facebook:

Established in 2004, from the college dorm room of Mark Zuckerberg, a Harvard student, the website is now worth billions of dollars and is one of the world's most recognisable brands. The website allows its users to connect with friends, family or people they don't know, online and for free. It allows users to share pictures, music, videos, and articles, as well as their own thoughts and opinions to the people all over the platform. The company has a net worth greater than $605 billion.

There has been multiple court cases and allegations Facebook has faced due to privacy and identity security. The most recent scandal took place in 2018 when Facebook allowed Cambridge Analytica to use user information and profiles without the user's consent. After the scandal, Cambridge out a statement saying that the amount was 30, but Facebook confirmed that the real number of harvested users were over 85 million.

Apple Inc.:

Apple Inc. is an American multinational technology company headquartered in the USA, that designs, develops, and sells consumer electronics, computer software, and online services. It is considered as one of the greatest companies. The corporation shares the Big Four with Facebook, Google and Amazon. The net worth of Apple Inc. is around $1.3 trillion.

Apple Inc. is also the innovator of Face ID. The idea behind the feature was to use the persons face to unlock the device and verify transactions and operations. The company's devices take many information from the user such as credit card number and many passwords of websites and accounts. This brought up the controversy of Apple Inc. harvesting its user's identity and information to proceed with transactions. The other theory was that the cameras were used for watching and examining the user for governmental or corporate reasons. The trillion-dollar company has put out multiple letters and informative posts stating that the Face ID in their devices are no more than a simple technological feature that uses your face to get verification and unlocking commands. They have stated that no information was being used in other places nor being sold to other companies.

United States of America:

The Unites States of America alone, has more than 243 million social media users within its borders. This means that one third of the country has a social media account. The United States operates one of the largest face recognition systems in the world with a database of 117 million American adults, with photos mainly taken from driver's license photos and mugshots. The country also has many multinational and multi-million social media and FRT companies that are United States originated. With Facebook, Google and Apple being originated form the United States, the country has a dominant soft power in the virtual field. They also can access many FRT's with the help of the US based companies and the FBI. The country has started the trend of using FRT in airports to identify criminals and suspects. With some states going against the FRT, many states have agreed on using it for security. In the US, the police are allowed to use FRT for further investigation or identification of a suspect.

China:

With 1.3 Billion people currently living in China, the country is undoubtfully one of the hardest places to apply facial recognition technology. The government had trouble tracking down the suspects and the criminals due to the mass population. With the newest guidelines, China now has a way of using FRT's successfully. The guidelines, first issued in September, require telecom companies to include "artificial intelligence and other technical methods" in their devices to check the identities of people registering the SIM cards. China has already made mobile phone users register to their SIM cards with their identity cards or passports and many telecoms had begun scanning customers' faces since last year. Many social media platforms also require users to sign up with their real names. To assure that, the user information is taken from the device and the phone number.

China's Ministry of Education stated in September that they would "curb and regulate" the use of facial recognition after the parents of the students were angry when facial recognition software was installed without their knowledge or consent at a university in Nanjing. The reasoning was given as "to monitor students' attendance and focus during class."

France:

France is poised to become the first European country to use facial recognition technology to give citizens a secure digital identity no matter what the citizens want or prefer. The reasoning behind using FRT is to make the state more efficient. President Emmanuel Macron's government is pushing hard to speed the release of the ID program, named Alicem The country's data regulator says the program breaches the European rule of consent and a privacy group is challenging it in France's highest administrative court. A published newspaper has stated that it took a hacker just over an hour to break into a "secure" government messaging app this year, raising concerns about the state's security standards.

According to the ministry, the app and the passport communicate in a secure manner. The designers of the project also have promised that the photos will not be stored in a central database but kept securely in private databases. When Alicem is being used, the system will connect to the national population register managed by ANTS (National agency for secure documents). Alicem creates a connection between biographic and biometric data. Next to that, the programme will synchronize with phone numbers, emails, and transaction logs.

Previous Attempts to Solve the Issue

The Office of Information and Communications Technology (OICT) was tasked with establishing an information risk management regime and supporting policies for the Secretariat. In 2013, OICT developed an action plan to address the most urgent shortcomings and mitigate specific risks. That action plan is now moving to maintenance mode and OICT continues to proactively implement effective measures to address both short- and long-term information security concerns.

"Progress on the implementation of recommendations related to strengthening information and systems security across the Secretariat"
(General Assembly, 25 October 2013)

"PERSONAL DATA PROTECTION AND PRIVACY PRINCIPLES"

There has been an alleged agreement on facial recognition technologies between China and the UN. The alleged agreement has been found out due to certain leaked documents. The agreement is about China's telecommunications equipment maker ZTE, security camera maker Dahua Technology and the state-owned Chinese telecommunication company China Telecom are proposing new international standards in the UN's International Telecommunication Union (ITU) for facial recognition. (Although the evidence is present, until an official word is put out, the news should not be used as a prime example in the resolutions. However, the news can be used in debates since accusations are okay in debates.)

Possible Solutions

In order to solve this issue completely and clearly, every citizen of each delegation must consent in to having their information and identity in the companies and/or governments hands. Since this is very unlikely, what can be done is to put restrictions and penalties to the FRT producers and users. The technology should not violate the human rights and disrupt the peace with discomfort. The issue in hand should be approached by two angles. The first one is being citizen safety and user consent, and the second one being about restrictions and limitations on where and why FRT is being used. Although FRT is easy to use and functional, it is very open to manipulation and it may cause threat for citizens. Hacking of accounts and devices can lead to many transactions and information leakage which holds risks for the citizens. Hence, new implementations on hackers and identity thefts should be created and presented to the house. The penalties of identity theft should be reconsidered and further specified due to the lack of attention given. To assure a safe and peaceful environment for the citizens, the policies of companies and countries should be looked over to see if there are any unspoken and unadded topics. There aren't enough judicial NGO's or unbiased organisations to control and inspect the governments and the companies. The UN has yet to further develop a solution on facial recognition technologies. The technology is slowly becoming a huge part of our lives and without knowing, we also are putting ourselves in risk. The technology is not monitored strict and well enough.

In addition, the affordability of the technology is still a question waiting to be answered. Although the issue in hand seems to have an easy solution, for many countries, it means that they will have to spend more than what they can afford. The resolutions should most definitely talk about funding and support for the LEDC's. as known, most drug and illicit arms trades are done in underdeveloped cities and countries to avoid the advanced security. With support from the UN, the amount of trades will decrease. Many countries lose track of their criminals due to them fleeing to the underdeveloped countries.

Useful Links For Further Research

- https://nissenbaum.tech.cornell.edu/papers/facial_recognition_report.pdf
- https://www.facefirst.com/blog/brief-history-of-face-recognition-software/
- https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

- https://www.scmp.com/tech/policy/article/3040164/chinese-tech-companies-are-shaping-un-facial-recognition-standards

- https://unite.un.org/services/information-security

- https://www.unsceb.org/CEBPublicFiles/UN-Principles-on-Personal-Data-Protection-Privacy-2018.pdf

- https://www.lawfareblog.com/facial-recognition-software-costs-and-benefits

- https://facex.io/blog/facial-recognition-applications/

- https://www.nytimes.com/news-event/apple-fbi-case

- https://techcrunch.com/2019/10/18/facebook-35-billion-lawsuit/

Bibliography

- "4 Major Applications of Facial Recognition: History: Data Used." *FaceX*, 6 Mar. 2019, facex.io/blog/facial-recognition-applications/.

- "History of Face Recognition & Facial Recognition Software." *FaceFirst Face Recognition Software*, 9 May 2019, www.facefirst.com/blog/brief-history-of-face-recognition-software/.

- *Bloomberg.com*, Bloomberg, www.bloomberg.com/news/articles/2019-10-03/french-liberte-tested-by-nationwide-facial-recognition-id-plan.

- "Cybersecurity." *United Nations*, United Nations, unite.un.org/services/information-security.

- "Technology." *The New York Times*, The New York Times, www.nytimes.com/news-event/apple-fbi-case.

- Constine, Josh. "$35B Face Data Lawsuit against Facebook Will Proceed." *TechCrunch*, TechCrunch, 18 Oct. 2019, techcrunch.com/2019/10/18/facebook-35-billion-lawsuit/.

- "Chinese Tech Companies Said to Be Shaping UN Facial Recognition Rules." *South China Morning Post*, 2 Dec. 2019, www.scmp.com/tech/policy/article/3040164/chinese-tech-companies-are-shaping-un-facial-recognition-standards.

- Deutsche Welle. “France Embraces Facial Recognition Tech: DW: 10.11.2019.” *DW.COM*, www.dw.com/en/france-embraces-facial-recognition-tech/a-51106489.

- l'Intérieur, Ministère de. “Alicem, La Première Solution D'identité Numérique Régalienne Sécurisée.” *Http://Www.interieur.gouv.fr/Actualites/L-Actu-Du-Ministere/Alicem-La-Premiere-Solution-d-Identite-Numerique-Regalienne-Securisee*, www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee.

- Griffiths, James. “China Is Rolling out Facial Recognition for All New Mobile Phone Numbers.” *CNN*, Cable News Network, 2 Dec. 2019, edition.cnn.com/2019/12/02/tech/china-facial-recognition-mobile-intl-hnk-scli/index.html.

- Ghaffary, Shirin, and Rani Molla. “Here's Where the US Government Is Using Facial Recognition Technology to Surveil Americans.” *Vox*, Vox, 10 Dec. 2019, www.vox.com/recode/2019/7/18/20698307/facial-recognition-technology-us-government-fight-for-the-future.

- “Facial Recognition Technology: Ensuring Transparency in Government Use.” *FBI*, FBI, 4 June 2019, www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use.

- *Facebook Loses Court Battle To Keep Internal Privacy ...* www.forbes.com/sites/zakdoffman/2019/05/31/facebook-loses-in-court-over-privacy-emails-as-zuckerberg-votes-to-keep-full-control/.

- “Cybersecurity.” *United Nations*, United Nations, unite.un.org/services/information-security.