Committee: Youth Assembly (YA)

Issue: The issue of human facial recognition and its relation to data breaches

Student Officer: Vasileios Georgantidis

Position: Co-Head

PERSONAL INTRODUCTION

Dear Delegates,

My name is Vasileios Georgantidis, I am an 11th grade student at Pierce – The American College of Greece and it is my great honour to serve as Co-Head in the Youth Assembly (YA) of the 7th ACG Model United Nations conference.

I'd like to start by congratulating all of you for choosing to participate in this conference. While it may present some challenges, I'm certain that this enjoyable experience will help you improve your public speaking and critical thinking skills. I'm excited to chair for the first time, having previously participated in MUN as a delegate. I recommend that each of you make the most of this experience, as Model United Nations (MUN) not only broadens your understanding of politics but also provides the opportunity to form new friendships and gain greater confidence in various aspects of life.

I am equally pleased that ACGMUN has chosen to include the Youth Assembly as one of its committees this year, a departure from previous sessions. Regarding the Youth Assembly, I must express my admiration for this committee. The topics under consideration are undeniably captivating. Serving as a chair for the first time is the realization of a long-held dream, and I eagerly anticipate the upcoming conference. I hope you are as excited as I am, and I am looking forward to meeting you all! Should you have any questions as far as the topic is concerned, please do not hesitate to contact me via email: v.georgantidis@acg.edu

TOPIC INTRODUCTION

In the digital age, where information flows rapidly through the vast networks of cyberspace, the issue of human facial recognition technology and its complex interrelation with data breaches has become a serious matter of privacy and security. It is essential that we all understand the weight of this phenomenon and how it could expand if human facial recognition technologies are not used ethically. The consequences affect society as a whole as private personal information is used by people wishing to share it for unethical purposes.

From unlocking smartphones to protecting critical facilities, facial recognition technology has advanced quickly and become ingrained in many facets of modern society. But this technology's extensive use also brings up serious issues referring not only to morals but also to the legal framework of each country. When facial recognition technology is used without proper regulation, there are significant concerns about civil liberties, human autonomy, and privacy. Simultaneously, incorrect implementation of these technologies may result in data breaches, endangering the security of states, businesses, and individuals.

Likewise, the abuse of facial recognition data presents essential issues for society at large. The gathering and storehouse of vast datasets of facial images, frequently without individualities' consent can result in unwarranted surveillance, profiling, and breaches of information. Data breaches can lead to severe consequences, including identity theft, fiscal fraud, and indeed concession of public security. It's essential for us, as global citizens, to grapple with these multifaceted challenges and seek transnational cooperation to address them.

In this era of rapid technological advancement, the ethical and responsible use of facial recognition technology is paramount to safeguard our privacy, civil liberties, and security. Nations, non-government organizations and investors should work together to establish frameworks which strike a balance between technological progress and basic human rights and liberties. If these challenges are dealt with solemnity and facial recognition technologies become more transparent, our society will benefit while having our core values and freedoms uncompromised.

DEFINITION OF KEY TERMS

Facial Recognition

Facial recognition is a technology that automatically identifies and verifies individuals based on their unique facial features. It uses algorithms to analyze facial patterns and matches them against a database, commonly applied in security, authentication, and surveillance.

Data breaches

Data breaches are incidents where information is stolen or taken from a system without the knowledge or authorization of the system's owner. Stolen data may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, trade secrets, or matters of national security. [1]

Cyber space

Cyber Space is a "virtual" world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet's infrastructure. [2]

Biometric Data

Biometric Data are personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. [3]

Eigenface

Eigenface is a term referring to a specific method in facial recognition technology that involves using linear algebra to represent facial features in a lower-dimensional space.

[1] TREND MICRO. "Data Breach - Definition - Trend Micro USA." Trendmicro.com, 2015, www.trendmicro.com/vinfo/us/security/definition/data-breach.
[2] Abdoullaev, Azamat. "Cyber AI: Machine Intelligence and Cyberspace." Www.bbntimes.com, www.bbntimes.com/science/cyber-ai-machine-intelligence-and-cyberspace.
[3]UCL. "GDPR - Glossary of Terms and Definitions." Legal Services, 23 Jan. 2018, www.ucl.ac.uk/legal-services/gdpr-glossary-terms-and-definitions.

Data sets

Data sets are a collection of related sets of information that are composed of separate elements but can be manipulated as a unit by a computer. [4]

BACKGROUND INFORMATION

Technological Advancements in Facial Recognition

The dawn of facial recognition occurred in the 1960's when three scientists, called Woody Bledsoe, Helen Chan Wolf and Charles Bisson attempted to use computers to detect human faces. A big part of their work was never published as the unnamed intelligence agency which funded the project chose to not publish it. Years later, it was shown that their initial work was based on marking landmarks of individual's faces, such as the eye centers, the mouth etc. Furthermore, the distance between the landmarks was computed for facial recognition to be more precise.

The baton was passed through several hands in the intriguing history of facial recognition technology, beginning with Bledsoe's early work and picking up steam in the 1970s with Goldstein, Harmon, and Lesk. In an effort to automate facial identification, these innovators broadened the field by including 21 subjective criteria, such as lip thickness and hair color. Despite the increased precision, the procedure still required manual measurement computation, which was labour-intensive.

When Sirovich and Kirby became the first to apply linear algebra to the problem in the late 1980s, the field of facial recognition experienced a dramatic shift. Their system, known as Eigenface, demonstrated that feature analysis on a collection of facial images could yield a set of basic features, requiring less than one hundred values to accurately code a normalized facial image. This laid the groundwork for advancements in the 1990s.

Turk and Pentland built on this work in 1991, creating techniques for face detection within photos, which resulted in the first automatic facial recognition cases. Notwithstanding obstacles related to technology and the environment, this discovery paved the way for further advancements.

The Face Recognition Technology (FERET) program was introduced in the 1990s by the National Institute of Standards and Technology (NIST) and the Defense Advanced Research Projects Agency (DARPA). By building an extensive database of face photos for testing, FERET sought to boost the commercial facial recognition business. This project stimulated creativity and set the stage for later developments.

[4] Gordon, Linda. "Subject Guides: Data Sets for Business & Management Topics: Home." Laverne.libguides.com, www.laverne.libguides.com/c.php?g=846318.

The National Institute of Standards and Technology launched the Face Recognition Vendor Tests (FRVT) in the early 2000s. Expanding upon FERET, FRVT sought to deliver impartial assessments of face recognition software that is sold commercially, providing vital intelligence to the federal government and law enforcement.

The facial Recognition Grand Challenge (FRGC), which sought to improve facial recognition technology to support ongoing U.S. government initiatives, marked a turning point in 2006. The astounding advancement was demonstrated by the FRGC, which found that new algorithms were 100 times more accurate in 1995 than in 2002 and ten times more accurate in 2002.

The decade of the 2010s saw the widespread adoption of facial recognition technology on popular platforms, such as Facebook, which introduced facial recognition features in 2010. The feature was widely embraced by users, despite discussion around privacy concerns. By 2017, FaceID—a major advancement in the integration of facial recognition into common consumer electronics—was unveiled with Apple's iPhone X.

In summary, the development of facial recognition technology has been an amazing journey, starting with its early conception and ending with a wide range of applications across multiple industries. Leading companies in the field, research initiatives, and pioneers have all been essential in influencing developments, reshaping the environment, and striking a careful balance between privacy and security. Fostering responsible development and implementation of face recognition technology in accordance with international principles of freedom, justice, privacy rights, openness, and continual improvement is crucial as we continue to watch developments in this field.

Applications and Uses of Facial Recognition

A sector in which human facial recognition technology is considered essential is security. First of all, it is widely used in access systems which are used to allow or prevent people from entering buildings or other restricted areas based on their facial characteristics. When it comes to national security, facial recognition softwares are used to protect nations against illegal immigration. Specifically, at border crossings, these kinds of systems can verify travellers' identities and cross check their biometrics with their passports. For instance, Georgia was one of the very first countries, which implemented facial recognition to upgrade border control.

Nations, however, have started using facial recognition systems in many aspects of their citizens lives. Educational institutions, consisting one of the most important sectors of each country have started implementing facial recognition

systems to establish security, especially in regions where serious incidents had taken place in the past. Another really interesting usage of facial id technology is in taxation systems. Specifically, new tax credit portals have been developed, where individuals can sign in using their biometric data and handle tax related obligations. Moving into something much simpler, social media use user's biometric data in the login portals, protecting user's personal information.

Governments have also started using facial recognition technology in healthcare settings. By accurately identifying patients, medical records can be processed easily so that patients are treated sufficiently with right medications based on their records. That obviously acquires patient's consent before hand so that they fully understand in which ways will their data be used.

Ethical and Legal Considerations

There have been many cases where it was questioned by the international community whether human facial recognition technology violates human rights and privacy. Several data breaches have created serious concerns over the ethical and legal implications of deploying facial recognition systems on a widespread scale. One major concern resolves around the potential misuse of biometric data, which is often collected without explicit consent from individuals and results in data breaches.

It is true that facial recognition allows the continuous monitoring of individuals and that is something that obviously raises serious concerns about unwanted surveillance. Having the ability to track individuals across different locations, clearly creates an awkward sense of constant observation. Hence, except of privacy, also the ability of engaging in activities without having the fear of being constantly monitored, is violated. Finally, as it was shown in the past, there is also a possibility that governments or institutions with access to this technology, use people's biometric data to manipulate or control the populace.

As facial recognition is a new technology, there is an absence of legal framework in many nations. The rapid pace of technological innovation has outstripped the development of comprehensive legislation, emphasizing the pressing need for lawmakers to address this gap and establish clear, enforceable regulations that strike a delicate balance between fostering innovation and protecting fundamental human rights. That's why many aspects of this technology remain untransparent and there are constantly new ethical and legal dilemmas of whether civil liberties are not being secretly violated.

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

United States

The issue of human facial recognition has caused some serious concerns over privacy and civil rights in the United States. That's why bans and restrictions have been imposed in several states, including Massachusetts and San Francisco, by government agencies. At the same time, there is federal involvement, with calls for comprehensive legislation to address the issue of data breaches related with facial recognition technology.

China

China was one of the very first countries to invest in facial recognition technology development. It is widely used in public services, and it is also used by the government for social credit programs. The country has faced several accusations concerning potential violations of human rights and citizens' privacy by the international community. China keeps using facial recognition technology for many aspects of not only public life but also for national security, such as border crossing control.

Japan

Japan has succeeded in establishing a balance between facial recognition systems and people’s privacy. Even if many aspects of Japan’s public surveillance are based on human facial recognition, such as the collection of information by the government, so that criminal activity is prevented, serious measures have been taken in order to protect citizens' rights. As Japan was one of the first countries to use facial recognition technologies, had much more time to establish a sustainable legal framework.

European Union (EU)

The General Data Protection Regulation (GDPR) provides a comprehensive framework for data privacy and protection, demonstrating the European Union's proactive approach to the issue. Facial recognition worries are related to more general privacy concerns, which is why the EU is assessing the moral implications of this technology.

Russian Federation

Particularly in public areas and major transit hubs, Russia has demonstrated interest in using facial recognition technology for security purposes. The administration has investigated how it may improve public safety and keep an eye on illegal activity. The political climate in Russia is still discussing how to strike a balance between security and privacy concerns, even though restrictions are not as extensive as they are in certain Western nations.

Amnesty International

Amnesty International keeps questioning the legal implications of facial recognition technology, while raising global awareness about human rights. The organisation has expressed serious concerns over the potential misuse of facial biometrics, because of many data breaches which took place in the past decade and could seriously harm people's privacy rights. The organisation urges nations to take strict measures in order to prevent future data breaches related with facial recognition systems.

The Centre for Democracy and Technology (CDT)

The Centre for Democracy & Technology (CDT), based in the United States, focuses on the intersection of technology and civil liberties. CDT has been actively involved in discussions around facial recognition, emphasizing the need for clear regulations to safeguard privacy and prevent discrimination. The organization engages in policy advocacy and provides expertise to policymakers to ensure that technology respects democratic values and individual rights.

TIMELINE OF EVENTS

Date	Description of event
1987	Linear algebra applied for facial feature representation in Eigenface method.
1991	Techniques developed for automatic face detection in photos.
2006	Facial Recognition Grand Challenge (FRGC) highlights significant algorithmic improvements.
2010	Facebook introduces facial recognition features.
2017	Apple's iPhone X unveils FaceID, a major advancement in consumer electronics.

25 May 2018	The General Data Protection Regulation (GDPR) was adopted.

RELEVANT UN RESOLUTIONS, TREATIES AND EVENTS

- Universal Declaration of Human Rights, Article 12, 10 December 1948[5]
- Resolution on guidelines for the Regulation of Computerized Personnel Data Files, A/RES/45/95, 29 January 1991[6]
- HRC resolution on the promotion, protection and enjoyment of human rights on the Internet, A/HRC/RES/38/7, 17 July 2018[7]
- GA Resolution on the right to privacy in the digital age, A/RES/75/176, 16 December 2020[8]

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a regulation implemented by the European Union on 25 May 2018 in order to protect the privacy rights of EU citizens. GDPR covers a wide variety of different aspects of data protection, including facial recognition technology. Organizations deploying facial recognition technology must be really cautious, as the processing of people's data must be done lawfully and transparently. That also means that individuals should be informed about the usage of their data and their consent should be obtained by the organization. Organizations should clearly define the purposes for which facial data is collected and processed, and they should not use the data for purposes unrelated to the original intent. (Articles 5 and 6)

Japan Act on the Protection of Personal Information

The Act on the Protection of Personal Information (APPI) was drafted as part of Japan's data protection laws and put into force in the year 2003. When APPI was implemented, it aimed to protect the rights and interests of individuals by regulating the handling of personal information. When it comes to facial recognition technology or any other type of collecting data, APPI requires organizations to obtain individuals' consent before collecting them, especially if the information is sensitive, e.g. biometric data. An amended version of the APPI came into force on April 1, 2022.

[5] https://www.un.org/en/about-us/universal-declaration-of-human-rights.
[6] https://digitallibrary.un.org/record/105299?ln=en.
[7] https://digitallibrary.un.org/record/1639840?ln=en
[8] https://digitallibrary.un.org/record/3896430?ln=en.

Biometric Information Privacy Act (BIPA)

Illinois' Biometric Information Privacy Act (BIPA) is one of the strictest biometric privacy laws in the United States, which was enacted in 2008. BIPA broadly defines biometric information to include data derived from measurements or analysis of physical characteristics, such as facial features, fingerprints, voiceprints, and retina scans. BIPA's mandate that businesses get consumers' written agreement before gathering, utilizing, or retaining their biometric data is one of its key features. Data on facial recognition is part of this. The precise reason and length of time for which the biometric data is being gathered must be specified in the consent.

POSSIBLE SOLUTIONS

Implementing stricter regulations on the use of facial recognition technology

More strict laws controlling the use of face recognition technology must be put in place in order to solve the ethical and privacy issues that surround it. Tighter laws would clearly define the parameters within which this technology can be used, guaranteeing that its application is consistent with moral principles and does not violate people's right to privacy. In order to prevent potential abuses and promote a safer and more private environment, governments and regulatory agencies can offer guidance on the appropriate and transparent use of facial recognition technology by establishing thorough legislative frameworks.

Raising awareness about the dangers of facial recognition technology

In order to enable the public to express their rights and comprehend the risks linked with facial recognition technologies, education and awareness are essential. There should be campaigns to educate people on the uses of their facial data, the risks associated with uncontrolled deployment, and the value of protecting their privacy. Communities can participate in educated debates, stand up for their rights, and help shape moral standards and legal frameworks pertaining to facial recognition technology by raising public knowledge. In order to build a more aware and watchful society that can defend its privacy in the face of technological progress, this education is crucial.

BIBLIOGRAPHY

"America Is Turning against Facial-Recognition Software." *The Economist*, The Economist Newspaper, www.economist.com/united-states/2019/05/25/america-is-turning-against-facial-recognition-software?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18151738051&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gad_source=1&gclid=CjwKCAiA-bmsBhAGEiwAoaQNmvwVf-iNw5aMLVdGnRTY0K95YKNdAWuhKr-dJOV6iNXZ-Ee9T5ZsdBoCgZwQAvD_BwE&gclsrc=aw.ds. Accessed 5 Dec. 2023.

"Biometric Data." *Migration and Home Affairs*, home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/biometric-data_en#:~:text=Definition(s),facial%20images%20or%20dactyloscopic%20data. Accessed 25 Dec. 2023.

"Facial Recognition and Data Protection: New Guidelines in the European Union." *Osborne Clarke*, 23 June 2023, www.osborneclarke.com/insights/facial-recognition-and-data-protection-new-guidelines-european-union.

"Facial Recognition Technology and Privacy Concerns." *ISACA*, www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-51/facial-recognition-technology-and-privacy-concerns. Accessed 22 Nov. 2023.

Ban Dangerous Facial Recognition Technology That Amplifies Racist Policing, Amnesty International, 26 Jan. 2021, www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/?ref=static.internetfreedom.in.

Gavin. "A Brief History of Facial Recognition - NEC New Zealand." *NEC*, 9 Mar. 2023, www.nec.co.nz/market-leadership/publications-media/a-brief-history-of-facial-recognition/.

Home | Bureau of Justice Assistance, bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf. Accessed 5 Dec. 2023.

Kumar, Vivek. "What Will Happen When a Facial Recognition Firm Is Hacked?" *Analytics Insight*, 11 Mar. 2021, www.analyticsinsight.net/what-will-happen-when-a-facial-recognition-firm-is-hacked/.

Madiega, Tambiama, and Hendrik Mildebrath. "Regulating Facial Recognition in the EU - European Parliament." *Regulating Facial Recognition in the EU*, European Parliament, Sept. 2021, www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf.

McGowan, Iverna, et al. “Brief – Human Rights Risks of Facial Recognition AI Tech in Policing and Immigration Must Be Properly Recognised in the EU AI Act.” *Center for Democracy and Technology*, CDT, 10 Feb. 2023, cdt.org/insights/brief-human-rights-risks-of-facial-recognition-ai-tech-in-policing-and-immigration-must-be-properly-recognised-in-the-eu-ai-act/#:~:text=As%20a%20result%2C%20CDT%20has,effective%20limitations%20are%20in%20place.

Noyan, Oliver. “New German Government to Ban Facial Recognition and Mass Surveillance.” *Www.Euractiv.Com*, 26 Nov. 2021, www.euractiv.com/section/data-protection/news/new-german-government-to-ban-facial-recognition-and-mass-surveillance/.

Rudakov, Andrey. “Russia: Broad Facial Recognition Use Undermines Rights.” *Human Rights Watch*, 2 Nov. 2019, www.hrw.org/news/2021/09/15/russia-broad-facial-recognition-use-undermines-rights.

Schwartz, Mathew J., and Ron Ross. “Hackers Claim to Defeat Iphone X ‘face ID’ Authentication.” *Bank Information Security*, www.bankinfosecurity.com/hackers-claim-to-defeat-iphone-x-face-id-authentication-a-10452. Accessed 24 Nov. 2023.

Smith, Marcus, and Seumas Miller. “The Ethical Application of Biometric Facial Recognition Technology - AI & Society.” *SpringerLink*, Springer London, 7 July 2021, link.springer.com/article/10.1007/s00146-021-01199-9.

Wakae, Masako. “Rules Needed to Use Facial Recognition Technology.” *The Japan News by The Yomiuri Shimbun*, The Japan News, 14 June 2022, japannews.yomiuri.co.jp/society/general-news/20210831-37417/.

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.