Committee: Disarmament and International Security Committee

Issue: Addressing the Security Risks and Benefits of Biometric Mass Surveillance Practices in Europe

Student Officer: Marios Katzigkas

Position: Co-Chair

.

PERSONAL INTRODUCTION

Dear delegates,

My name is Marios Katzigkas and I am a Grade 10 student at Pinewood International American School of Thessaloniki. I have attended 3 MUN conferences so far, and I am very excited to be a co-chair for the first time in the 5th DSTMUN.

During the GA1 session we will be discussing two very important topics, namely "The Security Risks and Benefits of Biometric Mass Surveillance Practices in Europe" and "The Question of Nuclear Proliferation on a Global Scale". You may use this document as a guide to your research and as a general overview on the first topic. However, it should not be your only source of information and each delegate should perform their own research in order to get a better understanding of the topic and their country's policy on it. Feel free to use the links provided at the end of the document to further your research.

If you have any questions on the topic don't hesitate to email me at mkatzigkas@pinewood-school.gr.

I look forward to meeting and working with all of you, and having a fruitful debate.

Regards,
Marios Katzigkas

TOPIC INTRODUCTION

Following the rapid pace of technological development of the 21st century, one of the most staggering leaps in innovation is the creation of biometrics technology, which allows computers to identify individuals using features such as their fingerprints, face, gait, voice, DNA, eyes, and more. The most controversial aspect of this development however, has been the development of Facial Recognition Technology.

Facial recognition uses Artificial Intelligence (AI) neural networks to identify an individual just from a picture of their face. This technology works by having an image of an individual stored and then asking the AI to find this person by searching for their face across hundreds of security camera feeds. Facial Recognition is only one form of biometrics but it is the most effective one to be used on a mass scale.

Biometric mass surveillance is the usage of technologies such as Facial Recognition, Voice Recognition, or even Gait Analysis to identify individuals. The difference between mass surveillance and the technology that is mostly in use now is the databases which are used by the government to search for the individuals they seek to find. The ethical discussion about the risks and benefits of this technology arise when discussing mass surveillance and therefore the data collection by the government. Most current systems work by having Law Enforcement give them an already existing image of a known criminal and 'asking' it to find this individual. A biometric mass surveillance system would work differently.

In a Biometric Mass Surveillance system the AI will create the profiles by itself instead of having the law enforcement agents give it a person to track. The system would track every single individual it saw and store information about their location, activity, who they interact with, in a general database. If such a system is combined with a database of every individual using passport or ID photos it makes it possible to find and keep track of anyone with just their name. This is technology that already exists outside of Europe and has been proven to function. Furthermore, multiple countries in Europe are either experimenting or already rolling out this technology.

There are both benefits and drawbacks to a BMS system. The capability to detect and track any individual gives law enforcement the power to identify and locate criminals to a previously impossible extent. This could be the key to a safer, more secure society. A BMS system, however, poses some ethical concerns. The data that such a system is capable of collecting is so extensive that it would be a major violation of privacy to gather and store it without permission. Furthermore, there are also some practical setbacks to the creation of a BMS system. Although it is possible, to implement the vast network of biometric identification devices required would be logistically challenging, and expensive.

DEFINITION OF KEY TERMS

Biometrics

The measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity.[1]

Artificial Intelligence (AI)

"Artificial intelligence leverages computers and machines to mimic the problem-solving and decision-making capabilities of the human mind."[2]. Essentially, artificial intelligence is technology that allows computers to recognize patterns and use logic that traditional, algorithm-based, programs are not capable of doing.

Neural Network

[1] "Biometrics Definition". *Merriam Webster*, https://www.merriam-webster.com/dictionary/biometrics

[2] "What is Artificial Intelligence?". *IBM,* https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

A neural network is an artificial version of the neurological connections of the human brain. Some neural networks simulate millions of neurons in order to perform their function. It is what allows computers to learn. A neural network is designed and trained to perform a specific task. Some neural networks, for example, are capable of recognizing faces. Neural networks are the foundation of AI and machine learning.

Database

A database is a large collection of data. Computers use databases to store and organize information. A database can contain millions of records of anything.

Facial Recognition

The use of AI Neural Networks to identify and match faces from images. Facial recognition software can take an image of a person and match it to another image of the same person.

Forensics

The use of science to assist in police investigations. Forensics can be used to identify cause of death, locate a victim, identify a criminal, etc.

BACKGROUND INFORMATION

The history of technology assisting in Peacekeeping

The use of science to assist with peacekeeping operations was developed back in the times of ancient civilizations. The first autopsy was conducted back in 44 BC by the Roman physician Antistius, who analyzed the body of emperor Julius Caesar to conclude his cause of death. The field of using science and technology to help in solving crimes has been called forensics, which advanced along with scientific knowledge and technology. Physicians became able to study bodies more accurately to determine the cause of death, and by extension, identify the killer. It became possible to chemically analyze bodies to see if they had been poisoned or died naturally. In the 1800s the biggest leap in forensics occurred when it became possible to conduct fingerprint analysis. Forensic scientists were now able to identify criminals based on their fingerprints. This was perhaps the biggest leap in forensics to date.

Fingerprinting has allowed forensic scientists to identify criminals using the fingerprint traces they leave behind at the crime scene. Fingerprinting has proved to be instrumental in the modern police investigation, contributing to thousands of arrests. Following the development of fingerprinting forensics, the next step was DNA forensics. DNA analysis allows forensic scientists to identify individuals based on the genetic code of artifacts left behind in a crime scene. For example, it is possible to extract the DNA sequence of an individual from a hair or a blood sample at the crime scene. The sequence can then be matched with an existing sample to identify the individual that left the DNA sample behind. This works similarly to regular

fingerprinting. These technologies have helped law enforcement agencies to capture and bring thousands of criminals to justice. The effectiveness of forensics in capturing criminals is unparalleled and the development in the field has ultimately made society a safer place.

Biometric Technology

Both Fingerprinting and DNA are biometric identifiers. This means that it is possible to identify a unique individual using just the data from these identifiers. Fingerprint and DNA analysis, however, are not the only biometric identifiers that exist. Facial recognition, gait analysis, iris recognition, and voice recognition are the most common biometric identifiers that are used. The major step in biometric analysis is the fact that computers now have the ability to identify people using these features. This makes it possible for analysis to be done faster, more efficiently, and on a larger scale. Biometrics technology is commonly used today. Most smartphones currently have the ability to use a person's biometric features, such as their face or fingerprint to identify them. These features make the user experience more convenient and secure.

Benefits of Biometric Technology

There are many benefits to the use of biometric technology. As mentioned before, biometric technology has become invaluable in the creation of secure computer systems. Due to the unique nature of biometric identifiers, they offer incredibly secure identification. The use of biometrics to verify bank transactions, information handling, and secure messaging has been useful to both organizations and individuals. Furthermore biometrics can be used to protect sensitive government systems, such as defense infrastructure.

Drawbacks of Biometric Technology

While there are many benefits to the use of Biometric technology, it also poses some potential dangers to the privacy of individuals. Even though biometrics offer a unique way to identify individuals, they are also unalterable. Unlike a password, a person's biometrics identifiers will remain the same throughout their whole life. For this reason they can be considered personal information and the storage and tracking of said information without the individual's permission could violate privacy. Biometric identifiers could also be used to track multiple aspects of an individual’s life with enough data.

Databases and AI

In order to identify a person through their biometrics a computer must already have an existing copy of that person’s identifiers in order to be able to match the new data with the already existing one. This means that if law enforcement has collected biometric data and they want to find out who it belongs to they will need the computer to have something to match them to, meaning that a database with such data must already exist. This is the principle of how AI can recognize an individual from their biometrics. An existing database with that person's biometric data in it is searched by the AI to find the closest match to the data it has been given.

After the closest match is found, the AI presents it to the law enforcement officers. The database must also have other information about the individual who's biometric data was just located. If the database contains personal information such as an individual's name or address in combination with their biometric data it makes it possible for the computer and law enforcement to identify the individual.

Such databases already exist. The US Department of Homeland Security already has a database with over 260 million stored identities and their biometric identifiers such as fingerprints or faces. Furthermore multiple countries both in Europe and outside have biometric databases of known criminals. If a criminal is in the database, it makes it possible for them to be identified with their biometrics. The goal of these databases is to make it easier for government and law enforcement officials to identify criminals, terrorists, immigration violators, etc. Computer systems and AI have been developed to the point where it takes a few seconds to find a match for a biometric search.

Biometric Mass Surveillance (BMS)

The concept of Biometric Mass Surveillance is essentially the enlargement of some already existing biometric identification technologies to a massive scale. Biometric Mass Surveillance is essentially the use of biometric identifiers being used to track and collect data on large populations without their consent, a major human rights violation. Such a system would be able to collect data about a person's daily activities, location, who they meet with, etc. and file this information into a massive database containing similar information about every citizen. The technology to implement a system like this exists and has already been experimented with in multiple European countries. Furthermore, a biometric mass surveillance system is already in place in China.

The most common biometric feature that can be used for biometric mass surveillance is facial recognition. Facial recognition technology can function even if the person is not directly interacting with a sensor or computer. In order to massively identify biometric features it is necessary to be able to quickly identify many individuals from a distance. For this reason Facial recognition is the most commonly used biometric and with the use of security cameras in public places it is possible to identify multiple individuals at a time through this feature. With a large enough number of cameras a system would be able to identify individuals wherever they went and then use the data of this individual's location to add to their database, essentially allowing the system to track the location of thousands or even millions of people. This data can also then be used in conjunction with the data of other people to see with which individuals a person has been meeting with.

A search isn't possible, however, without an already existing record for the AI to match against. For this reason, for a biometric mass surveillance system to be the most effective it needs to already have a database of every existing citizen to add all the data it collects to. This can be achieved by using already existing records of citizens and simply making them digital. To set up this initial database that the system will use to create profiles of citizens, official documents like ID cards or

driving licenses can be used. The government already has access to these documents, making it easy to create the foundation for a BMS system.

The difference between a Mass Surveillance system and a facial recognition system is essentially the size of the database that is used for searches. If the database contains only known criminals and wanted persons then it is hard to consider the use of facial recognition technology mass surveillance. If the database, however, contains data on all citizens and stores their personal data using biometrics, then it is a mass surveillance system.

Biometric Mass Surveillance in Europe

While there are no active uses of BMS in Europe there have been multiple pilot programs, led by multiple countries, that have experimented with the technology. Both Interpol in France and Europol in the Netherlands have their own facial recognition and database systems with profiles of known criminals and wanted persons.

A lot of European Countries, however, do have their own facial recognition implementations, which mostly use criminal or mugshot databases for recognition. Systems like Hungary's civil database, however, use data from civilians for facial recognition. More information about EU member state facial recognition implementations is available in the TELEFI report[3]. This report includes a detailed description of every current FR implementation in Europe. Further information about both current facial recognition implementations but also pilot, experimental systems in Europe can be found in the Greens/EFA report on Biometric Mass Surveillance in Europe[4].

Due to Europe's relatively strong economy, technological advancements often develop within its borders. These advancements include faster, more accurate biometric identification technology, and also more advanced AI. This makes Europe the perfect location for the development and testing of BMS technology. While this development happens all over Europe, a main hub is the Netherlands, which has experimented with many types of technologies that could be used in a BMS system. More details about these pilot programs can be found in the Major Countries and Organizations involved section of this study guide and the aforementioned Greens/EFA report. While these developments are taking place in Europe, the EU is attempting to create a legal basis for the implementation of such technology. The Artificial Intelligence Act[5] is a still developing legal basis for all uses of AI within the EU. This includes BMS systems.

---

[3] "Summary Report of the project "Towards the European Level Exchange of Facial Images"". TELEFI, 2021, https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf

[4] "BIOMETRIC & BEHAVIOURAL MASS SURVEILLANCE IN EU MEMBER STATES". *Greens/EFA,* 2021, http://extranet.greens-efa.eu/public/media/file/1/7297

[5] "The Artificial Intelligence Act". *European Union,* https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

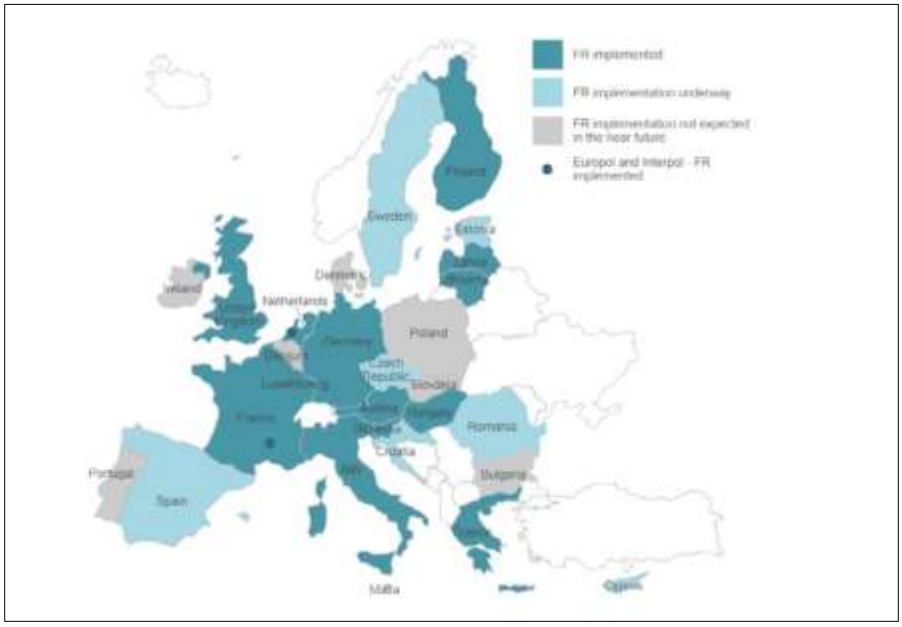

Figure 1: Use of Facial Recognition Technology in EU member states for Forensics Applications [6]

Potential Benefits of Biometric Mass Surveillance

Advancements in Forensics

Biometric Mass Surveillance gives police and other law enforcement agencies an extremely powerful tool to assist in the identification and capture of criminals. With the abilities provided to them by a BMS system, police will be able to find criminals with just trace biometric samples. A picture of the criminal's face will be enough to identify who they are, and collect their personal information, as well as their current location. With such a powerful system law enforcement will become much easier and faster. A BMS system would be the next massive leap in the field of forensics. With it the government and police would be able to use the incredible potential of AI to their advantage.

Safer International Society

Organizations like Europol or Interpol could share their BMS databases with other countries to help them with the identification and capture of known international criminals and wanted persons. The main advantage of such a system, however, is that it can identify anyone. A person must not have committed a crime before to be identified. If someone with no criminal record commits a crime they will still be traceable because of the incredibly large database that the system uses. This ability will help police and law enforcement create a more safe and secure society with minimized crime. In addition to this, people will know that they can be traced easily, deterring them from committing any crimes.

[6] "BIOMETRIC & BEHAVIOURAL MASS SURVEILLANCE IN EU MEMBER STATES" pg 38. *Greens/EFA,* 2021, http://extranet.greens-efa.eu/public/media/file/1/7297

Downsides of Biometric Mass Surveillance System

Violations of Privacy

While a Biometric Mass Surveillance system gives law enforcement the ability to easily track criminals and potentially create a safer society it could also violate multiple human rights and privacy treaties. Collecting so much personal data about an individual's location, behavior, contacts, routine, etc. without their permission could be considered a violation of Article 17 of the International Covenant on Civil and Political Rights. Should a system like this be used in the EU it would also be against Article 8 of the European Convention on Human Rights and Fundamental Freedoms. The privacy concerns of such a system are justified, as the amount of data that can be collected about a person without their knowledge is immense.

Potential for Government Oppression

Another use for a BMS system would be to assist a social scoring system. This system would monitor the daily activities of citizens and apply a score to them depending on their behavior. This score would affect the daily lives of citizens in multiple ways. The score would be an indication of how this person is expected to behave. This system would allow the government to control aspects of a person's life such as access to public infrastructure like hospitals or transport, ability to travel, ability to get loans, job opportunities, internet access and much more. The system would reduce the points of someone acting in an "untrustworthy" manner against the government. Naturally such a system is in violation with human rights such as the freedom of expression, the freedom of peaceful assembly, the right to equal access to public services, the right to leave a country, the right to move freely within a country, the right to healthcare, and much more according to the Universal Declaration of Human Rights[7]. Of course, Biometric Mass Surveillance would not be the only thing necessary to create such a system. The data needed to classify an individual is much more extensive. A BMS system would, however, greatly assist in the creation of a social score system. China has already started using such a system and are planning to expand it to collect more data, and influence more aspects of citizens' lives.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

Hungary

Hungary already has a facial recognition system in place. The facial recognition system is used to assist the police with identifying, locating, and prosecuting criminals. The database used for facial recognition searches is the Facial Imagery Registry. This database takes images from other databases as sources to be

[7] "The Universal Declaration of Human Rights". *United Nations*, 1948, https://www.un.org/en/about-us/universal-declaration-of-human-rights

used in FR scans. The sources that the images are taken from are ID-Card databases, Passport databases, Road Traffic databases, and Asylum seeker databases. While these databases contain the images with other data about an individual like name, address, gender, age, etc, this data is not included in the Facial Imagery Registry. The Registry does, however, include a reference to where the image came from, making detailed information about an individual still accessible. The system does not have the ability to trace movements back in time and can only be used for tracing criminals and other wanted persons. Following some illegal entrances into the country the Hungarian government decided to massively upgrade its security camera network[8]. Project Dragonfly plans to expand Hungary's surveillance infrastructure. Keeping in mind Prime Minister Orban's firm rule so far Hungary has the potential to develop a functioning Biometric Mass Surveillance system with the combination of their project Dragonfly expansion and their Facial Recognition infrastructure.

China

China has been developing Biometric Mass Surveillance technologies for a long time. With an estimate of over 340 million surveillance cameras installed, China has the largest surveillance network on the planet. The cameras are used in conjunction with facial recognition to capture criminals. The databases used for the FR matching contain images of every single citizen with an ID card. This gives the Chinese government the ability to trace whoever they want. Following the COVID-19 pandemic China used the opportunity presented by a mandatory quarantine to install even more surveillance cameras. The vast grid allows China to trace anyone in populated areas. It took just 7 minutes for their facial recognition system to locate a BBC reporter in 2017[9].

Aside from using the system to track criminals or other persons of interest, China also uses the data collected by their BMS system to adjust their citizens' social credit score. The CCP has implemented a system similar to the aforementioned one. The government monitors citizens' activity both online and in the real world and uses the data to assign them a score. This score affects their life in all of the aforementioned ways and restricts the freedom of Chinese citizens. China is an example of the effects a BMS system can have on society.

The Netherlands

The Netherlands is a country that has already implemented FR technology for police use. The system is called CATCH and it uses two databases for facial recognition searches. One contains images and information about known criminals and suspects. The second database contains images and information on people who have applied for a visa or people who have requested asylum. The police are permitted to use these databases for facial recognition searches. The dutch

[8] Sarkadi Nagy, Márton. "After terrorists crossed Hungary, surveillance cameras connected through Project Dragonfly". *Atlatszo*, https://english.atlatszo.hu/2021/12/09/after-terrorists-crossed-hungary-surveillance-cameras-connected-through-project-dragonfly/

[9] Liu, Joyce. "In Your Face: China's all-seeing state". *BBC,* https://www.bbc.com/news/av/world-asia-china-42248056

government also currently has several civil databases that contain images about the general population through driver licenses, IDs, etc. The databases are incompatible with a facial recognition system however.

The Netherlands has also been a pilot for multiple other computer vision technologies. The Netherlands has experimented with both behavior recognition and object recognition systems. The systems used however, were not designed to collect personal identifying marks of a person. They merely monitored people and objects and didn't collect any data. For behavior recognition the project "A Burglary Free Neighborhood" was created. The goal was for the researchers to be able to train an AI to recognize suspicious behavior and warn the operator. For object detection cameras around a stadium in Amsterdam were used to detect if people were holding guns, fireworks or drones. In addition to these two tests the Netherlands has also experimented with live facial recognition multiple times. None of these systems is still in use, however, except from the forensic CATCH system.

Europol

Europol has an in-house developed FR and facial image database called FACE. This database allows for FR searches to be done automatically from surveillance sources. The FACE database contains information submitted to Europol from all of its member states as well as third parties. The information is usually about wanted criminals, suspects, witnesses, or victims that the member states have submitted to the database. The FACE database is not connected to Europol's other information databases. This allows for a FR search to be completed but the results are then handed back to the requesting member state for further investigation.

Interpol

Interpol uses its own facial recognition system called the Interpol Face Recognition System. The system works in a similar way to Europol's. Images are submitted to the general database by 179 member countries. Interpol can perform FR searches using this database and report the results back to the member state in question.

The Greens/EFA

The Greens/EFA is a group within the EU Parliament that performs various studies to present to the Parliament in order to inspire change. They believe in and support democratic ideals including freedom of speech and the right to privacy. One of their studies was on Biometric Mass Surveillance in Europe. This report included a detailed analysis of various biometric developments within the EU as well as information of various experiments or pilot programs that could potentially lead to BMS. In addition to providing information on developments of biometric systems within Europe, the Greens/EFA also explain how these developments could lead to a biometric mass surveillance system.

BLOCS EXPECTED

Bloc 1: In favor of Biometric Mass Surveillance

This Bloc will be composed of countries who support the use of BMS and are looking to develop it within their borders. Such countries will want stricter control of their population and want to increase the power of their law enforcement. (Hungary, Poland, etc.)

Bloc 2: Against Biometric Mass Surveillance

This Bloc will be made from countries that are against the use of BMS and want to forbid its use. These countries will likely have a very privacy-focused government that wants to give more power to its citizens. (Denmark, Belgium, Sweden, etc.)

TIMELINE OF EVENTS

Date	Description of event
1880	Sir Francis Galton developed the first technique for fingerprint matching and became the first man to use biometrics in forensics.
1896	The Henry Classification System was developed by Edward Henry to identify criminals using fingerprints. This system is still in use today and is what it used to run many of our fingerprint identification systems.
1950	First Neural Network was developed with the ability to classify simple images.
1965	The first facial recognition algorithms were born.
2010s	Artificial Intelligence research expanded rapidly. AI became a focus of many institutes and universities.
2005	China developed its Skynet system, a live BMS system with over 20 million cameras.
2015-2018	Various European countries began implementing FR technology to capture criminals.
April 15, 2019	The TELEFI project was funded to study the uses of Facial Recognition in the EU.
April 24, 2021	The EU proposed the AI act, which aimed to set a legal basis for the operation of AI in the EU.
2021	Hungary began developing project dragonfly, a live FR system to track down criminals and monitor suspicious behavior.

October, 2021	The Greens/EFA published their report on biometric mass surveillance across Europe.

RELEVANT RESOLUTIONS, TREATIES AND EVENTS

Article 17 of the International Covenant on Civil and Political Rights 16/12/1996 2200A

Article 17 states that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation." and that "Everyone has the right to the protection of the law against such interference or attacks."[10]. This is a very relevant resolution because a BMS system could infringe on the privacy of individuals and therefore be in violation of this Article.

Article 8 of the European Convention on Human Rights and Fundamental Freedoms 1950

Article 8 ensures that "Everyone has the right to respect for his private and family life, his home and his correspondence."[11]. This convention, which is still valid today, states that EU citizens have the right to remain private without interference from the government. BMS technology could be in violation of this article since it would allow for the collection of private data about a person without their permission. The data gathered by a BMS system is so extensive that it can be used to learn a great deal about an individual's private life. As such the collection of this data is a direct violation of Article 8.

The Artificial Intelligence Act by the EU 21/4/2021

The AI Act which was created by the EU aims to lay down some fundamental guidelines about the use of AI in Europe. It recognizes both the opportunities and dangers presented by the widespread use of artificial intelligence technologies. This also includes the issue of biometric mass surveillance. The act sets down some guidelines that would prevent the use of AI technology for mass surveillance within EU borders. It is important to note that the Act is still not in effect. It is a draft that is actively changing until it becomes in depth enough to pass as a law.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

[10] "International Covenant on Civil and Political Rights". *UN General Assembly,* https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[11] "European Convention on Human Rights and Fundamental Freedoms". *European Union,* https://www.echr.coe.int/Documents/Convention_ENG.pdf

Seeing as this is an issue that has arisen from the development of AI it is still very new. There have been almost no attempts to solve the issue of biometric mass surveillance specifically. The closest relevant solutions attempted by any body are the Artificial Intelligence Act proposed by the EU, as well as the TELEFI project.

The Artificial Intelligence Act

The proposed law recognizes the potential dangers that mass surveillance can have on society. It states that biometric mass surveillance can impede several fundamental rights of citizens like freedom of privacy, freedom of expression or freedom of assembly. The Act further prohibits the use of such technology with the exception of 3 extremely narrow situations. "Those situations involve the search for potential victims of crime, including missing children; certain threats to the life or physical safety of natural persons or of a terrorist attack; and the detection, localisation, identification or prosecution of perpetrators or suspects of the criminal offences referred to in Council Framework Decision 2002/584/JHA"[12]. This essentially means that the EU is proposing the complete prohibition of live FR systems except for certain crimes mentioned in Council Framework Decision 2002/584/JHA. This means that the Act only allows the use of live biometric surveillance for criminal identification, something that a lot of EU countries are already doing. This is in an effort to stop the development of a mass surveillance system.

The TELEFI project

The Telefi project is an EU funded project that aims to research and understand how Facial Recognition technology is used across EU member states. It stands for "Towards the European Level Exchange of Facial Images". The report published by the TELEFI project includes an analysis of every facial recognition implementation within EU borders. This information is invaluable to identify potential BMS systems under development and to trace the progress of FR technology within Europe.

POSSIBLE SOLUTIONS

Complete Prohibition of Facial Recognition by the Government

This is an extreme solution that will completely forbid the use of facial recognition technology. It will completely stop governments or police departments from using this technology to identify criminals or from developing a biometric mass surveillance system. Such a solution would also entail the proposition and implementation of a policy to prevent the development of such technology. For example, prohibiting companies inside Europe from developing or using facial recognition would make it significantly harder for countries to use biometric

[12] "The Artificial Intelligence Act". *European Union,* https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

identification for law enforcement. Seeing as most EU countries already use, or plan to use facial recognition for law enforcement purposes, it would be hard to implement such a solution.

Prohibition of Live Monitoring Systems

By prohibiting the use of live monitoring systems it would be impossible to develop biometric mass surveillance systems because they require constant surveillance of live video feeds. This would also allow police to still use facial recognition technology on recovered footage from closed-circuit television (CCTV) for investigations. This solution is essentially what is currently the case within Europe. It allows for some of the benefits of a BMS system, such as the safer society, and easier tracking of criminals, but it sacrifices speed and efficiency since it is impossible for a system to monitor live footage. This suggestion, if implemented, makes it impossible for a system to gather information about the general population on a mass scale, however, removing privacy concerns.

Heavy Restrictions on Live Monitoring

This solution would still permit the use of live monitoring systems using biometric systems. Their use would, however, be heavily restricted to “extreme use” cases. This means that the police could use live biometric surveillance only in circumstances where it poses a huge threat to general public safety. This is essentially what is proposed in the Artificial Intelligence Act. This solution leaves the decision to use live surveillance up to the country in question. What classifies as an “extreme case” can vary wildly and is not a concrete identification. It would be possible to exploit such legislation to use live monitoring all the time, creating a BMS system.

Restricting Databases to Known Criminals

By restricting the databases that the AI can use it is still possible to use live monitoring without infringing on the privacy of the general public. These databases would contain data only on known criminals. The system would also be required to not collect data on the general public and only be used for the identification of wanted persons. This solution ensures the further development of forensic technology without violating human rights. It would be difficult, however, to ensure that countries do not violate this rule, because the technology for a BMS system would already be implemented. The only element needed to transition to a mass surveillance system would be a software update. Certain checks by a governing body could be performed on countries in order to ensure that this does not happen.

BIBLIOGRAPHY

“Biometrics Definition”. Merriam Webster, https://www.merriam-webster.com/dictionary/biometrics

"What is Artificial Intelligence?". IBM, https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

"Biometric Surveillance and the Right to Privacy." IEEE Technology and Society, 5 Oct. 2017, https://www.technologyandsociety.org/biometric-surveillance-and-the-right-to-privacy/

"Biometric and Behavioural Mass Surveillance in EU Member States." www.greens-Efa.eu, https://www.greens-efa.eu/biometricsurveillance/.

"Summary Report of the Project "towards the European Level Exchange of Facial Images."". *TELEFI,* 2021, https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf

Eu, I. "Report for the Greens/EFA in the European Parliament BIOMETRIC BEHAVIOURAL MASS SURVEILLANCE". 2021, http://extranet.greens-efa.eu/public/media/file/1/7297

Fritsvold, Erik. "The Cutting-Edge Technologies Transforming 21st Century Policing." University of San Diego, 10 May 2019, https://onlinedegrees.sandiego.edu/10-innovative-police-technologies/.

"White Paper on Artificial Intelligence a European Approach to Excellence and Trust", 2021, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Incognito Forensic Foundation. "The History of Forensic Science and It's Evolution - IFF Lab." IFF Lab, 29 Dec. 2017, https://ifflab.org/history-of-forensic-science/.

Biometrics Institute. "Types of Biometrics - Biometrics Institute." Biometrics Institute, 2018, https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/.

Department of Homeland Security. "Biometrics." Department of Homeland Security, 6 Feb. 2017, https://www.dhs.gov/biometrics.

"In Your Face: China's All-Seeing State." Www.bbc.com, https://www.bbc.com/news/av/world-asia-china-42248056.

United Nations. "Universal Declaration of Human Rights." United Nations, 10 Dec. 1948, https://www.un.org/en/about-us/universal-declaration-of-human-rights.

"After Terrorists Crossed Hungary, Surveillance Cameras Connected through Project Dragonfly." Atlatszo, https://english.atlatszo.hu/2021/12/09/after-terrorists-crossed-hungary-surveillance-cameras-connected-through-project-dragonfly/.

"Coming into Focus: China's Facial Recognition Regulations." Www.csis.org, https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations.

Business, Nectar Gan, CNN. “China Is Installing Surveillance Cameras Outside People’s Front Doors ... And Sometimes inside Their Homes.” CNN, 28 Apr. 2020, https://edition.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html.

European Court of Human Rights. “European Convention on Human Rights”. 1950, https://www.echr.coe.int/Documents/Convention_ENG.pdf.

“In China, Beware: A Camera May Be Watching You.” NPR.org, https://www.npr.org/2013/01/29/170469038/in-china-beware-a-camera-may-be-watching-you.

IBM Cloud Education. “What Are Neural Networks?” Www.ibm.com, IBM, 17 Aug. 2020, https://www.ibm.com/cloud/learn/neural-networks.